International Journal of Information Management 36 (2016) 25–34

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

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/

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 combination of equipment and actions required to obtain data for the purposes of the study. These authors conclude that event trees are usually constructed horizontally, starting on the left with the initiating event.

ETA has been used for this purpose in many different contexts, including animal behaviour (Bidder et al., 2014), natural disasters (Rosqvist et al., 2013), gas accidents (Brito & Almeida, 2009; Ferdous, Khan, Sadiq, Amyotte, & Veitch, 2009), underwater tunnel excavation (Hong, Lee, Shin, Nam, & Kong, 2009) and the release of hazardous materials (Vílchez, Espejo, & Casal, 2011), among others.

In this study, ETA is applied to prevent a system failure owing to the invasion of a data center, through the analysis of results propagated from the risk associated with critical events. Eventually, ETA is used as a guide to guarantee system data center safety by superimposing additional safety measures that correspond to risk components identified during analysis.

In an information security context, users may understand how to protect the system against potential security threats, thus providing the foundation to determine information security policy (Chen & Zhao, 2013). One way to solve this problem is using ETA, which is a very powerful tool for identifying and evaluating all system consequence paths that are possible after an initiating event occurs and identifies the consequences that may result following the occurrence of a potentially dangerous event (Andrews & Dunnet, 2000).

Also, the definition of risk by NIST (2002) – "risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization" – emphasizes the importance of characterization of events, which are responsible for accidents related to IT security. Thus, the use of ETA, a methodology already established and traditionally used in different contexts for identifying and evaluating the sequence of events in a potential accident scenario, is justified.

Table 1 show the steps to develop an ETA.

Table 1
Steps to develop an event tree analysis.

Activities	Description
1st step—identify the accident scenarios	Perform hazard analysis on the data center to identify existing system hazards and accident scenarios.
2nd step—identify the initiating events	Refine the hazard analysis to identify the significant initiating event in the data center accident. The initiating event includes invasion through internal or external access.
3rd step—identify the pivotal events	Identify the source of the fault occurrence in the invasion of the data center.
4th step—build the event tree diagram	Construct the logical event tree diagrams, starting with the initial events, then the pivotal events and ending with the outcome of each path.
5th step—identify the outcome risk	Assess the risk for each outcome path in the event tree diagram.

2.3. *Fuzzy decision theory*

Risk quantification and assessment models predominantly use probability models, which are the fundamental basis for informed decision making related to risk in many areas. However, a probability model built upon classic set theory may not be able to describe some risks in a meaningful and practical way (Shang & Zakir, 2013). In this sense, many authors (Mokhtari, Ren, Roberts, & Wang, 2012) propose the application of fuzzy logic and fuzzy set theory, introduced by mathematician Lotfi A. Zadeh in 1965, to risk management. Rommelfanger (2003) also argues that the acceptance of decision models can be increased by using fuzzy utilities and fuzzy probabilities because normative decision theory is hardly used in practice to solve real life problems.

With the publication of the paper "fuzzy sets" by Zadeh in 1965, fuzzy sets theory started to be considered as a new way for modelling more realistic decision models, making it feasible to model vague data as precisely as possible. Consequently, some fuzzy elements have been proposed for use in decision models: fuzzy acts, fuzzy events, fuzzy probabilities, fuzzy utilities values, and others. However, many of these fuzzy elements are not applied in practice, either because they are not known to the public or because they are of little use for real problems (Rommelfanger, 2003).

In this paper, the use of fuzzy expected values (FEV), as discussed by Rommelfanger (2003), is proposed to define the risk expected of each act-event associated to information security management. In this sense, the applicability of two fuzzy elements is recognized:

Fuzzy probabilities: $\tilde{P}_j = \tilde{P}(s_j) = \left\{(p, \mu_{P_j}(p)) | p \in [0, 1]\right\}$, Watson, Weiss, & Donell (1979); Dubois & Prade (1982); Whalen (1984).

Fuzzy utility vales (consequences): $\tilde{U}_{ij} = \tilde{U}\left(a_i, s_j\right) = \left\{u, \mu_{U_{ij}}(u) | u \in U\right\}$, Jain (1976), Watson et al. (1979); Yager (1979); Rommelfanger (1984), Whalen (1984).

Where a_i represents the actions and s_j represents the possible nature states (possible scenarios). As in Rommelfanger (2003), how to obtain (fuzzy) utility functions is not discussed. It is assumed that the decision maker or an expert knows the utility function

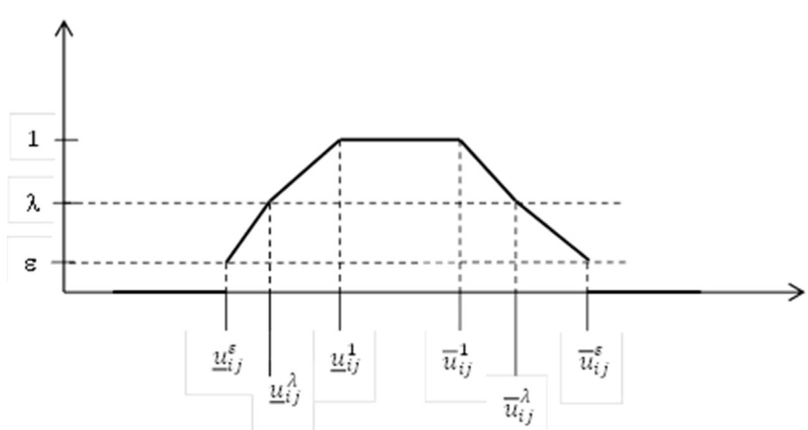

Fig. 1. Membership function of $\tilde{U}_{ij}$.

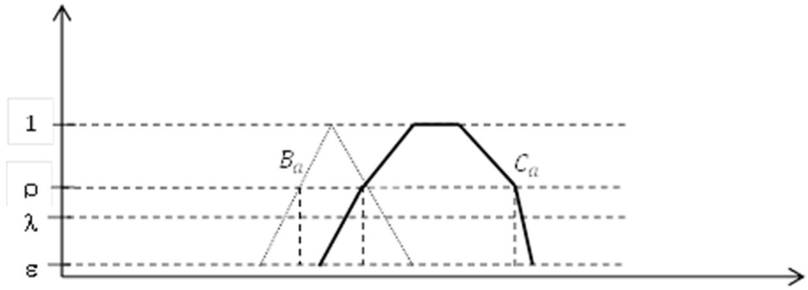

Fig. 2. Membership function of the sets $\tilde{\boldsymbol{B}}$ e $\tilde{\boldsymbol{C}}$; ρ-preference.

$u = u(g_{ij})$. Then, the fuzzy results are mapped in the fuzzy utilities $\tilde{U}_{ij} = \left\{u(g), \mu_{\tilde{G}_{ij}}(g) | g \in G\right\}$ or alternatively the expert specifies directly utility values $\tilde{U}_{ij} = \left\{u, \mu_{\tilde{U}_{ij}}(u) | u \in U\right\}$, where U is the possible set of crisp utility values.

2.3.1. Fuzzy expected values (FEV)

As discussed in Rommelfanger (2003), assuming that each real number a can be modelled as a fuzzy number like:

$$\hat{A} = \left\{\left(x, \mu_{\hat{A}}(x)\right) | x \in R\right\} \text{with} \mu_{\hat{A}}(x) = \begin{cases} 1 \text{if} x = a \\ 0 \text{else} \end{cases} \tag{1}$$

Each act-event combination (a_i, s_j) is valued by a fuzzy interval:

$$\tilde{U}_{ij} = \left(\underline{u}_{ij}^{\varepsilon};\ \underline{u}_{ij}^{\lambda};\ \underline{u}_{ij}^{1};\ \overline{u}_{ij}^{1};\ \overline{u}_{ij}^{\lambda};\ \overline{u}_{ij}^{\varepsilon}\right)^{\lambda,\varepsilon},\ i = 1, \ldots, m;\ \ j = 1, \ldots, n. \tag{2}$$

The membership function of $\tilde{U}_{ij}$ is a polygon presented in Fig. 1.

This membership is proposed considering that an approximation of a fuzzy set can be constructed by using few α-cuts. And so, for:

$\alpha = 1 : \mu_{\tilde{U}_{ij}}(u) = 1$, u has the highest chance of belonging to the set of utility values associated with the act-event combination (a_i, s_j).

$\alpha = \lambda : \mu_{\tilde{U}_{ij}}(u) \geq \lambda$, the decision maker or the expert is willing to accept u as an available value for the time being. A value u with $\mu_{\tilde{U}_{ij}}(u) \geq \lambda$ has a good chance of belonging to the set of utility values associated with the act-event combination (a_i, s_j). Corresponding values of u are relevant for the decision.

$\alpha = \epsilon : \mu_{\tilde{U}_{ij}}(u) < \epsilon$, u has only a very little chance of belonging to the set of utility values associated with the act-event combination (a_i, s_j). The expert is willing to neglect the values u with $\mu_{\tilde{U}_{ij}}(u) < \epsilon$.

Then, considering that the expert specifies the priori probabilities $p(s_j), j = 1, 2, \ldots, n$, the expected value of each alternative a_i can be calculated as:

$$\tilde{E}(a_i) = \tilde{U}_{il} \otimes p(s_1) \oplus \quad \ldots \oplus \quad \tilde{U}_{in} \otimes p(s_n) = \left(\underline{E}_i^{\varepsilon};\ \underline{E}_i^{\lambda};\ \underline{E}_i^{1};\ \overline{E}_i^{1};\ \overline{E}_i^{\lambda};\ \overline{E}_i^{\varepsilon}\right)^{\varepsilon,\lambda} \tag{3}$$

where

$$\underline{E}_i^{\alpha} = \sum\nolimits_{j=1}^{n} \underline{u}_{ij}^{\alpha} \times p\left(s_j\right), \alpha = \epsilon, \lambda, 1 \tag{4}$$

$$\bar{E}_i^{\alpha} = \sum\nolimits_{j=1}^{n} \bar{u}_{ij}^{\alpha} \times p\left(s_j\right), \alpha = 1, \lambda, \epsilon \tag{5}$$

2.3.2. Ordering of fuzzy preferences

The expert must identify each act-event combination that generates the best result. After calculating the expected values, the expert must compare the fuzzy sets and construct preference ordering. This identification step gains significance when fuzzy sets are used in the classical model.

Different concepts for comparing fuzzy sets and for constructing preference orderings have been proposed and can be divided into old proposals (Jain, 1976; Dubois & Prade, 1980, 1983; Dubois & Prade, 1983; Adamo, 1980) and recent proposals (Abbasbandy & Hajjari, 2009; Chen & Sanguansat, 2011; Nejad & Mashinchi, 2011; Nesseri et al., 2013; Destercke & Couso, 2014). To illustrate the increasing interest on the issue, Bortolan and Degani (1985) present a literature review and test the indexes of nine proposals; sixteen years later Wang and Kerre (2001a,b) counted thirty five methods.

Most of the concepts are based on defuzzification, meaning that each fuzzy set is compressed into a single, crisp, real number. In other words, Ekel and Schuffner Neto (2006) pointed out that the ordering of fuzzy quantities is about converting a fuzzy quantity into a real number and then basing the comparison of fuzzy quantities on that of real numbers.

Some shortcomings can be cited regarding these methods: the spreads of the fuzzy sets are neglected in the defuzzification process (Rommelfanger, 2003); each individual conversion approach

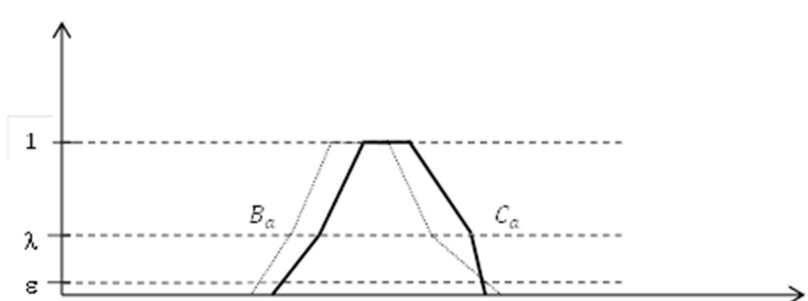

Fig. 3. Membership function of the sets $\tilde{\boldsymbol{B}}$ e $\tilde{\boldsymbol{C}}$; ϵ-preference.

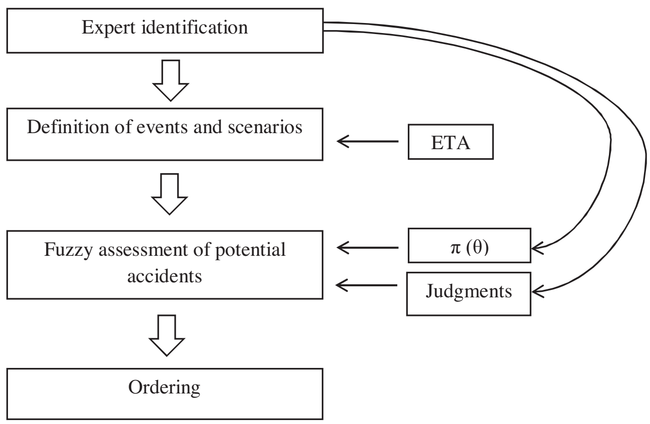

Fig. 4. Steps of the proposed model.

pays attention to one unique special aspect of fuzzy quantity (Ekel & Schuffner Neto, 2006), the defuzzification methods may produce different rankings for the same problem (Cheng, 1998), and choices that appear inconsistent with intuition can occasionally result (Ekel, Pedrycz, & Schinzinger, 1998); finally the majority of the methods assume an obligatory distinction among the alternatives, which is not natural because the uncertainty of information leads to decision uncertainty regions (Ekel & Schuffner Neto, 2006).

In order to avoid these shortcomings, Rommelfanger (2003) suggested the use of ρ-preference and ϵ-preference as alternatives for constructing preference orderings using the following concepts.

A fuzzy set $\tilde{B}$ is preferred to a fuzzy set $\tilde{C}$ on the ρ-level, $\rho \in [0, 1]$, written as $\tilde{B}_\rho\tilde{C}$, if:

- ρ is the least real number, such that: Inf $B_\alpha \geq$ SupC_a for all $\alpha \in [\rho, 1]$ (6)
- and for at least one $\alpha \in [\rho, 1]$the inequality (6) holds in the strict sense.

where the ρ-level-sets of $\tilde{B}$ and $\tilde{C}$ are defined as:

$$B_\alpha = \left\{ x \in X \dot{:} \mu_{\tilde{B}}(x) \geq a \right\}$$

$$C_\alpha = \left\{ x \in X \dot{:} \mu_{\tilde{C}}(x) \geq a \right\}$$

Fig. 2 presents an example where $\tilde{B}_\rho\tilde{C}$.

In cases where the ρ-preference relation does not lead to a preference ordering of the given alternatives, the ϵ-preference relation is more appropriate and suitable because ϵ-preference is weaker than the ρ-preference. For more details, see Rommelfanger (2003).

On the ϵ-level, $\epsilon \in [0, 1]$, a fuzzy set $\tilde{B}$ is preferred to a fuzzy set $\tilde{C}$, written as $\tilde{B}_\epsilon\tilde{C}$, if:

- ϵ is the least real number, such that: Sup $B_\alpha \geq$ SupC_a and Inf $B_\alpha \geq$ InfC_a for all $\alpha \in [\epsilon, 1]$ (7)
- and for at least one $\alpha \in [\epsilon, 1]$ one of these inequalities holds in the strict sense.

Fig. 3 presents an example where $\tilde{B}_\epsilon\tilde{C}$.

3. Information security risk assessment proposed model

The proposed information security model includes four phases (Fig. 4): expert identification, determination of scenarios and events, fuzzy evaluation and ordering.

The aim of the proposed model is to evaluate the consequence of each alternative in terms of financial loss, an easily perceived variable, considering the different possible scenarios (possible nature states). As outlined in Section 2, the alternatives detailed below represent a potential accident regarding information security in the proposal.

3.1. Expert identification

The first step consists of expert identification. The expert is the person, or group of people, who, based on experience, is able to identify: the vulnerabilities of the organization, and consequently the potential accidents; possible scenarios; the chances of occurrence, and judgments about each of these elements.

According to Purba (2014), an expert is someone with multiple skills who understands the working environment and has substantial training in and knowledge of the system being evaluated. The question to be answered is how to select an expert with these aforementioned skills.

Three indicators recommended by Cooke et al. (2008), namely: the number of scientific publications, recommendations from a wide range of experts, and experiences of previous similar studies, can be used to properly select the experts who have the expertise, which is most relevant to the system being evaluated. Similarly, Ramzali, Malasani, and Ghoudousi (2015) take into consideration professional position, length of experience, education level, and age in order to select an expert.

In line with the previous recommendations, the expert selected for this study is a senior academic, with more than 20 years of experience time. She holds a Ph.D. degree in Information Systems, has published eleven papers in this field and her age is between 40 and 49 years. She also has experience as a consultant on IS to companies in the private sector.

3.2. Definition of events and scenarios

The development of a taxonomy of events and scenarios is done using the ETA methodology presented in the previous section. The methodology ETA is developed to represent the issues related to assessing the information security risk, their vulnerability and consequences (see Fig. 5).

For the construction of the ETA, this paper considers several characteristics identified in different papers. According to Feng et al. (2014), in information systems, security risks are caused by various interrelated internal and external factors and could be derived from viruses, worms, hackers, and crackers (Grant, Edgar, Sukumar, & Meyer, 2014). Insider threats include inappropriate usage of devices, network data breaches, laptop loss/theft, lack of education (Sarkar, 2010), lack of experience, deliberate damage, spam, hoaxes, and phishing (Grant et al., 2014). External security threats are represented as accidental damages (Grant et al., 2014)

Once the information security ETA is constructed, it serves as a tool for risk evaluation based on decision theory and fuzzy logic.

3.3. Fuzzy assessment of potential accidents and ordering

The starting point for use of the fuzzy decision theory approach to the assessment of potential accidents is the construction of a matrix, where the rows represent the alternatives (e.g., potential accident regarding information security in data center services) and the columns the possible scenarios. For each cell of the matrix, the expert uses fuzzy logic to define the financial losses stemming from combinations of these variables (alternatives × scenarios). The expert also provides the probability of each scenario considering the different means of occurrence. These a priori probabilities ($p(s_j)$), are represented by $\pi(q)$ in the application.

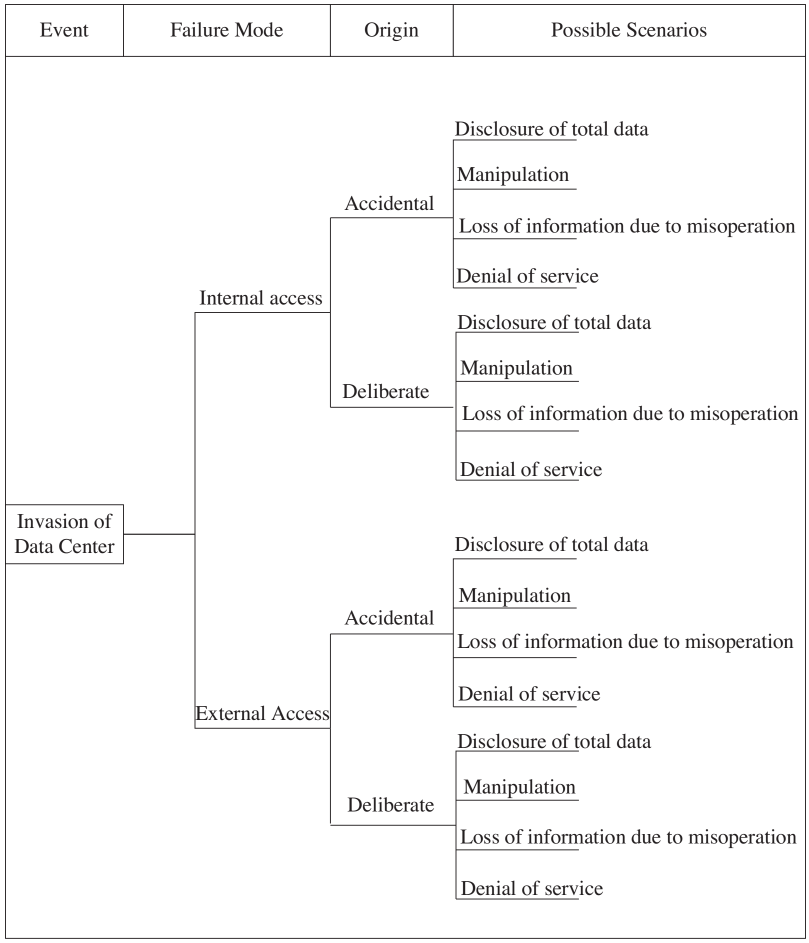

Fig. 5. Event tree analysis for the data center invasion (attack).

It is then possible to calculate the FEV, using the Eq. (3), and ordering the potential accidents in accordance with the procedure presented by Rommelfanger (2003) as discussed earlier.

4. Illustrative example

This section presents an example that illustrates the applicability of the proposed model. This application is based on a real context. Although real data, regarding the information required, have not been used, the data, which used to give an overview of the model, are nevertheless realistic.

Following the steps of the proposed model (Fig. 4), explained in Section 3, the information required (realistic data) was provided by an expert in the security risk to information area, based on his judgment and expertise. She focused on the risks of using a data center as measured against her perception of the vulnerabilities of its services. This encompasses a growing number of managed nodes in heterogeneous environments scattered over many locations.

In this application, the expert also provided a preliminary summary of the main characteristics of the data center's services, as shown in Table 2.

In the following step of the proposed model, an ETA analysis was developed, based on the expert's knowledge, as described in the Fig. 5, to provide definition of events and scenarios regarding the data center's invasion.

Given the difficulty of attributing a numerical value to potential accidents, and the uncertainties involved, we propose the use of fuzzy numbers, more specifically of triangular fuzzy numbers. The triangular fuzzy numbers, presented in Table 3, are determined according to a five-point linguistic scale (very low, low, moderate, high and very high) to represent the financial consequences of each alternative concerning each state of nature.

The use of triangular membership functions in this paper is justified because of its simplicity and applicability to the present context (Pedrycz, 1994). In the literature, triangular fuzzy numbers are rep-

Table 2
Data center services.

Services	Description
Website	A hosting service that allows people or companies to store their information, pictures, videos or any other content on online systems accessible via the web.
E-commerce	A service providing a technical platform with secure payment methods, purchasing and large database backend, supporting the sale of products and services through the Internet.
Database-as-a-service	A service that hosts databases in the cloud, and a viable option for businesses developing bespoke web based applications.

Table 3
Verbal scale regarding monetary range.

Linguistic terms	Fuzzy number	Values	Unit
Very low	Triangular	(100;150;200)	Thousands U$
Low	Triangular	(250;350;450)	Thousands U$
Moderate	Triangular	(350;600;800)	Thousands U$
High	Triangular	(650;1000;1300)	Thousands U$
Very high	Triangular	(1000;1600;2000)	Thousands U$

Table 4
Expert's elicitation evaluation.

Alternatives (A_i)	θ_1	θ_2	θ_3	θ_4
W/I/A(A_1)	H	VH	M	L
W/I/D (A_2)	L	M	M	H
W/E/A(A_3)	L	VL	VL	VL
W/E/D(A_4)	M	M	VH	VH
EC/I/A(A_5)	M	L	VL	L
EC/I/D(A_6)	VL	VL	L	L
EC/E/A(A_7)	M	L	M	M
EC/E/D(A_8)	L	H	M	VH
DB/I/A(A_9)	H	VH	VH	M
DB/I/D(A_{10})	VH	M	H	VH
DB/E/A(A_{11})	L	M	M	L
DB/E/D(A_{12})	H	VH	H	VH

resented by a triple (a; m; b), where a and b mean the lower and upper bounds of a fuzzy set and the parameter m means a modal (typical) value of this set (Kaufmann and Gupta, 1988).

According to information obtained from the expert, the financial loss, resulting from a data center invasion, may range from US$ 100,000.00 to US$ 2000,000.00. Thus, the verbal scale covers this range. However, it should be noted that the proposed model allows variations in the magnitude of values in line with the context to be analysed.

To proceed to a fuzzy assessment of potential accidents, it is necessary to calculate the expected value of each alternative with regard to risk. To do this, it is necessary to first define the nature states and the alternatives (act-event combinations). Then, the evaluation of alternatives from the expert must be obtained using fuzzy logic and the priori probabilities ($p(s_j)$), represented by $\pi(\theta)$ in this illustrative example because nature states are represented by θ and priori probability by π in decision theory.

Thus, the nature states (θ), which are the possible result scenarios (nature state) of a data center's invasion (shown in Fig. 5), were defined as: data dissemination (θ_1), data modification (θ_2), data loss or destruction θ_3 and service interruption (θ_4).

The alternatives (act-event combinations) were constructed grouping each data center service (website (W), e-commerce (EC) and database (DB) with two failure modes (internal (I) and external (E) access) and the two possible origins (accidental (A) and deliberate (D)), resulting in twelve alternatives (Table 4).

Table 4 shows the expert's evaluation concerning each pair of alternatives and state of nature. This evaluation was performed by means of a 5-point linguistic scale ranging from very low (VL) to very high (VH).

The expert's judgments about the financial losses of the alternatives (potential accidents: act-event combination) for each nature state (possible scenario) are presented in Table 5.

The definition of prior probability, $\pi(\theta)$, takes into account expert experience or past data regarding data centre attacks. It was assumed that the expert is risk neutral regarding financial aspects.

Table 6
Fuzzy expected value (FEV).

Alternatives (A_i)	FEV (laplace criteria)	FEV (expert's elicitation)
W/I/A(A_1)	(562.5; 887.5; 1137.5)	(541; 842; 1078)
W/I/D (A_2)	(400; 637.5; 837.5)	(430; 674; 882)
W/E/A(A_3)	(137.5; 200; 262.5)	(142; 206; 270)
W/E/D(A_4)	(674; 1100; 1400)	(675; 1100; 1400)
EC/I/A(A_5)	(237.5; 362.5; 475)	(257; 392; 513)
EC/I/D(A_6)	(175; 250; 325)	(175; 250; 325)
EC/E/A(A_7)	(325; 537.5; 712.5)	(328; 545; 723)
EC/E/D(A_8)	(562.5; 887.5; 1137.5)	(622; 978; 1244)
DB/I/A(A_9)	(750; 1200; 1525)	(668; 1072; 1372)
DB/I/D(A_{10})	(750; 1200; 1525)	(808; 1296; 1638)
DB/E/A(A_{11})	(300; 475; 625)	(286; 440; 576)
DB/E/D(A_{12})	(825; 1300; 1650)	(853; 1348; 1706)

Table 7
Alternatives ranking.

Alternatives (A_i)	Ranking (laplace criteria)	Ranking (expert's elicitation)
W/I/A(A_1)	4th	6th
W/I/D (A_2)	5th	7th
W/E/A(A_3)	10th	12th
W/E/D(A_4)	3rd	3rd
EC/I/A(A_5)	8th	10th
EC/I/D(A_6)	9th	11th
EC/E/A(A_7)	6th	8th
EC/E/D(A_8)	4th	5th
DB/I/A(A_9)	2nd	4th
DB/I/D(A_{10})	2nd	2nd
DB/E/A(A_{11})	7th	9th
DB/E/D(A_{12})	1st	1st

To assess the robustness of the proposed model, we analyze two methods of setting $\pi(\theta)$: the first method uses laplace criteria and the second uses an expert's experience.

According to Eq. (3), the fuzzy expected value (FEV), presented in Table 6, were calculated using these different methods. In the first column, the probabilities were defined using the laplace criteria, considering $\pi(\theta_1) = \pi(\theta_2) = \pi(\theta_3) = \pi(\theta_4) = 0.25$ and in the second column the probabilities were elicited from the expert, $\pi(\theta_1) = 0.28$, $\pi(\theta_2) = 0.22$, $\pi(\theta_3) = 0.14$, $\pi(\theta_4) = 0.36$. The correspondent triangular fuzzy numbers are shown on Figs. 6 and 7.

Table 7 summarizes the rankings provided by the two methods. These rankings were defined in accordance with the procedure presented by Rommelfanger (2003).

Thus, as a result of the application of the model, alternative A12 (Deliberate External Database Attack) represent the need for increased levels of awareness for both scenarios. Using the laplace criteria, alternatives A9 and A10 have a similar risk. On the other hand, it is important to say that alternative A10 was the second most risky using the expert elicitation, as well as for laplace criteria. Another important result is that alternative A3—accidental external website attack was the least risky alternative for both methods.

Table 5
Decision matrix.

Alternatives (A_i)	θ_1	θ_2	θ_3	θ_4
W/I/A(A_1)	(650;1000;1300)	(1000;1600;2000)	(350;600;800)	(250;350;450)
W/I/D (A_2)	(250;350;450)	(350;600;800)	(350;600;800)	(650;1000;1300)
W/E/A(A_3)	(250;350;450)	(100;150;200)	(100;150;200)	(100;150;200)
W/E/D(A_4)	(350;600;800)	(350;600;800)	(1000;1600;2000)	(1000;1600;2000)
EC/I/A(A_5)	(350;600;800)	(250;350;450)	(100;150;200)	(250;350;450)
EC/I/D(A_6)	(100;150;200)	(100;150;200)	(250;350;450)	(250;350;450)
EC/E/A(A_7)	(350;600;800)	(250;350;450)	(350;600;800)	(350;600;800)
EC/E/D(A_8)	(250;350;450)	(650;1000;1300)	(350;600;800)	(1000;1600;2000)
DB/I/A(A_9)	(650;1000;1300)	(1000;1600;2000)	(1000;1600;2000)	(350;600;800)
DB/I/D(A_{10})	(1000;1600;2000)	(350;600;800)	(650;1000;1300)	(1000;1600;2000)
DB/E/A(A_{11})	(250;350;450)	(350;600;800)	(350;600;800)	(250;350;450)
DB/E/D(A_{12})	(650;1000;1300)	(1000;1600;2000)	(650;1000;1300)	(1000;1600;2000)

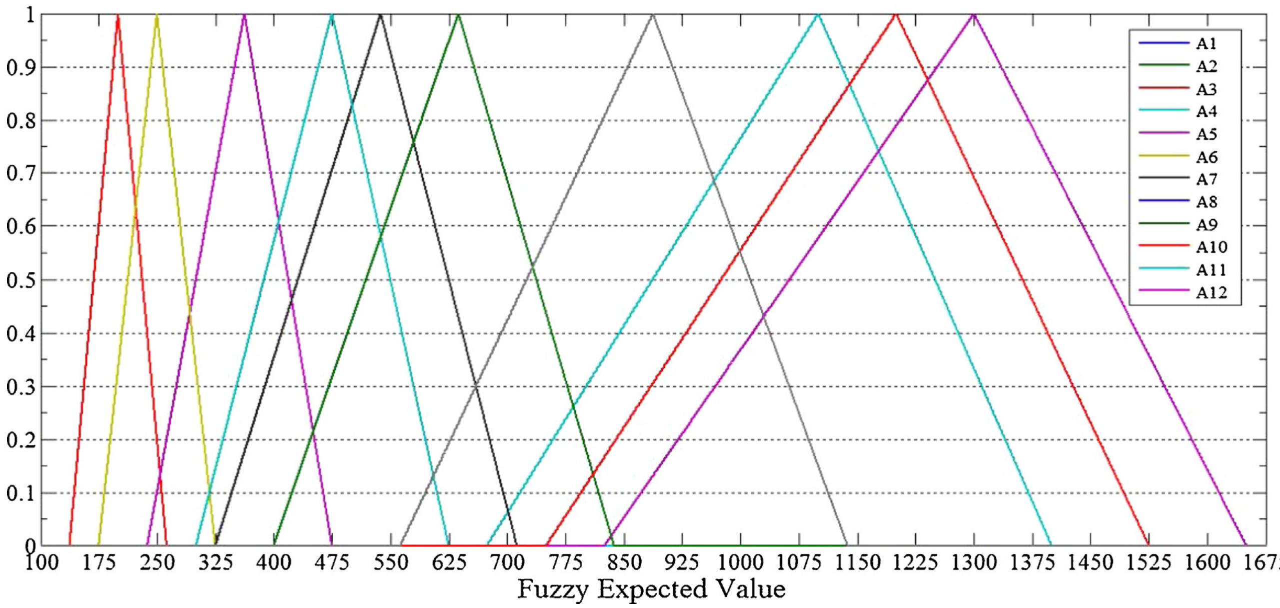

Fig. 6. Triangular fuzzy numbers of alternatives—laplace criteria.

5. Discussion

In this study, a model for information security risk management was formulated and illustrated by means of an illustrative example developed in a data center. This model makes a contribution to information security practices by addressing some critical aspects; evaluation and analysis of possible scenarios, origins and potential failure modes.

The ETA methodology was used to identify the alternatives of interest, which were defined from the taxonomy of events and scenarios and thereafter, a risk assessment analysis was conducted.

It is well known that the knowledge of a single expert is often used when the ETA methodology is used because, in most cases, data collection is either difficult or very expensive. Although, multiple expert knowledge can provide more reliable information for an observation (e.g., the probability of an event) than the knowledge a single expert, expert judgments are qualitative/linguistic in nature and may suffer from inconsistency if a lack of consensus among various experts arises. Moreover, Ferdous et al. (2009) claim that the classical probabilistic framework is not very effective at dealing with vague or incomplete/inconsistent concepts.

Similar papers have used only one expert's knowledge to provide value judgments that represent the expert's perceptions and/or preferences. For instance, the aforementioned study by Ferdous et al. (2009) provides evidence obtained from two unbiased and independent experts, resulting in two different evaluations. Taking into consideration this work, we performed two evaluations in our application as well: one using Laplace criteria, and the other using an expert's judgment. Furthermore, Garcez and Almeida (2014a,b) explore a risk measure of underground vaults

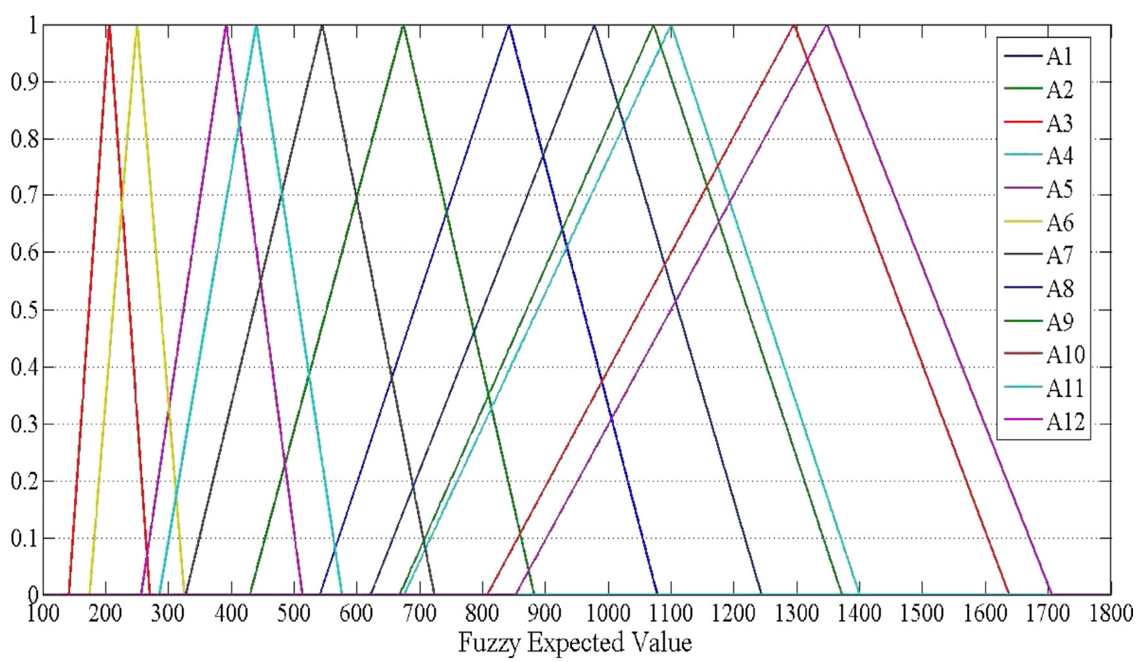

Fig. 7. Triangular fuzzy numbers—experts' elicitation.

that considers the consequences of arc faults using a single expertís a priori knowledge.

Accordingly, it is worth stating that the probabilities of the events of the ETA are not defined in this paper. Thus, less information is required from the expert. On the contrary, the expert provided the evaluations concerning each pair of alternatives (potential accidents: act-event combination) for each state of nature (possible scenario). This evaluation was performed by the expert who used a 5-point linguistic scale ranging from very low (VL) to very high (VH) regarding monetary range.

Still, by means of elicitation procedures, the expert also provided the prior probability $\pi(\theta)$ of each state of nature (and not the probability of an event). It is worth saying that these prior probabilities, which are defined by the expert and those deriving from Laplace criteria, were used with a view to illustrating the model and its accuracy.

The illustrative example, which considers financial aspects, shows that although there are differences between the probabilities for both methods of analysis, the importance of the alternatives remains basically the same, which demonstrates the robustness of the proposal and context. A reason for this difference; however, may be because the four states of nature are very common as information security issues.

Moreover, the top two potential problems arise from deliberate actions, instead of accidental actions, which justifies increased efforts in the internal monitoring of the activities of the organization, since the consequences derived from these deliberate actions are usually more damaging.

Also, it should be noted that according to Dzazali, Sulaiman and Zolait (2009) twenty-five percent of information security incidents originated from within organizations, 15% originated from the outside, and 11% were from a mixture of internal and external sources. However, according to Magklaras and Furnell (2002), the great majority of abuse originates from external factors. Therefore, the aim of the proposed model is not to establish the origins of incidents, but to provide a general assessment of the organization regarding information security, thereby enabling information security policies to be prioritized.

6. Conclusions

This paper proposes an information security risk model using fuzzy decision theory, which encompasses four phases: expert identification, determination of scenarios and events, fuzzy evaluation, and ordering. The paper aims to evaluate the consequence of each alternative in terms of an easily perceived variable – financial loss – considering the different possible states of nature (scenarios). To achieve this goal, this work described a taxonomy of events and scenarios using the ETA methodology, which served as the basis for the risk analysis and led to awareness concerning the threat level of deliberate and external data center attacks. Then, this paper ordered each alternative based on the criticality of the risk.

Despite its conceptual nature, the main contribution of this paper is the ability to provide an organization with information regarding the causes of information system attacks of highest managerial relevance. Although this paper focuses on the application of the model to assess the risk of information security in a data center, it is not restricted to this area. The model could be used in other areas where information security policies must be prioritized and also be applied in a private or public organization.

For future work, application of the model to a private/public organization and the use of a multicriteria approach in order to include other criteria such as service availability are recommended. This can be done using the method proposed in , which is based on constructing and analyzing payoff matrices reflecting effects that can be obtained for different combinations of solution alternatives and states of nature or scenarios and allows one to speak about the evaluation of the particular mono-criteria as well as aggregated multi-criteria risks. Another subject for future research is to provide solutions to minimize potential losses.

For future work, the use of a multidimensional risk analysis (de Almeida et al., 2015) in order to include other criteria and to obtain a broader view, is recommended. Ekel, Martini, and Palhares (2008), for example, propose a method which is based on constructing and analyzing payoff matrices reflecting effects that can be obtained for different combinations of solution alternatives and states of nature or scenarios and allows one to speak about the evaluation of the particular mono-criteria as well as aggregated multi-criteria risks. Another subject for future research is to provide solutions to minimize potential losses.

Finally, another perspective is the analysis of risk in the view of multiple experts. The context of information security is complex. Thus to be able to draw on the combined knowledge of multiple experts is appropriate in order to harness as much human expertise as possible and increase the robustness of how estimates are made.

Acknowledgements

This research was partially supported by the Universidade Federal de Pernambuco and GPSID—Decision and Information Systems Research Group.

References

Abbasbandy, S., & Hajjari, T. (2009). A new approach for ranking of trapezoidal fuzzy numbers. *Computers & Mathematics with Applications*, *57*, 413–419.

Adamo, J. M. (1980). Fuzzy decision trees. *Fuzzy Sets and Systems*, *4*(3), 207–219.

Alter, S., & Sherer, S. (2004). A general, but readily adaptable model of information system risk. *Communications of the AIS*, *14*(1), 1–28.

Anderson, R. (2001). Why information security is hard: An economic perspective. *ACSAC '01: Proceedings of the seventeenth annual computer security applications conference* (vol. 358) Los Alamitos, CA: IEEE Computer Society, (p. 2001).

Anderson, R., & Schneier, B. (2005). *Economics of information security*. IEEE Security and Privacy.

Andrews, J. D., & Dunnet, S. J. (2000). Event-tree analysis using binary decision diagrams. *IEEE Transactions on Relialability*, *49*(2).

Bidder, O. R., Arandjelović, O., Almutairi, F., Shepard, E. L. C., Lambertucci, S. A., Qasem, L. A., et al. (2014). A risky business or a safe BET? A fuzzy set event tree for estimating hazard in biotelemetry studies. *Animal Behavior*, *93*, 143–150.

Bojanc, R., & Jerman-Blazic, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*, 413–422.

Bortolan, S. G., & Degani, R. (1985). A review of some methods for ranking fuzzy numbers. *Fuzzy Sets Systems*, *15*, 1–19.

Brender, N., & Markov, I. (2013). Risk perception and risk management in cloud computing: results from a case study of Swiss companies. *International Journal of Information Management*, *33*, 726–733.

Brito, A. J., & de Almeida, A. T. (2009). Multi-attribute risk assessment for risk ranking of natural gas pipelines. *Reliability Engineering and Systems Safety*, *94*, 187–198.

Chen, S. M., & Sanguansat, K. (2011). Analyzing fuzzy risk based on a new fuzzy ranking method between generalized fuzzy numbers. *Expert Systems with Applications*, *38*, 2163–2171.

Chen, G., & Zhao, D. (2013). Model of information security risk assessment based on improved wavelet neural network. *Journal of Networks*, *8*(9).

Cheng, C. H. (1998). A new approach for ranking fuzzy numbers by distance method. *Fuzzy Sets Systems*, *95*, 307–317.

Lo, C.-C., & Chen, W.-J. (2012). A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems with Applications*, *39*, 247–257.

Clifton, A., & Ericson, I. I. (2005). *Hazard analysis techniques for system safety*. New York: John Wiley & Sons.

Cooke, R. M., ElSaadany, S., & Huang, X. (2008). On the performance of social network and likelihood-based expert weighting schemes. *Reliability Engineering & System Safety*, *93*(5), 745–756.

de Almeida, A. T., Cavalcante, C. A. V., Alencar, M. H., Ferreira, R. J. P., Almeida-Filho, A. T., & Garcez, T. V. (2015). Multicriteria and multiobjective models for risk, reliability and maintenance decision analysis. In *International series in operations research & management science*. New York: Springer.

Destercke, S., & Couso, I. (2014). Ranking of fuzzy intervals seen through the imprecise probabilistic lens. *Fuzzy Sets and Systems* (accessed 24.12.14.).

Dubois, D., & Prade, H. (1980). *Fuzzy sets systems: theory and applications*. New York: Academic Press.
Dubois, D., & Prade, H. (1983). Ranking of fuzzy numbers in the setting of possibility theory. *Information Sciences*, *30*, 183–224.
Dubois, D., & Prade, H. (1982). The use of fuzzy numbers in decision analysis. In M. M. Gupta, & E. Sanchez Hrsg (Eds.), *Fuzzy information and decision processes* (pp. 309–321). Amsterdam, New York: Oxford.
Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape and maturity level: case study of Malaysian public service (MPS) organizations. *Government Information Quarterly*, *26*, 584–593.
Ekel, P. Ya., & Schuffner Neto, F. H. (2006). Algorithms of discrete optimization and their application to problems with fuzzy coefficients. *Information Sciences*, *176*, 2846–2868.
Ekel, P. Ya., Pedrycz, W., & Schinzinger, R. (1998). A general approach to solving a wide class of fuzzy optimization problems. *Fuzzy Sets and Systems*, *97*, 49–66.
Ekel, P. Ya., Martini, J. S. C., & Palhares, R. M. (2008). Multicriteria analysis in decision making under information uncertainty. *Applied Mathematics and Computation*, *200*, 501–516.
Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences*, *256*, 57–73.
Feng, N., & Li, V. (2011). An information systems security risk assessment model under uncertain environment. *Applied Software in Computetrs*, *11*(7), 4332–4340.
Ferdous, R., Khan, F., Sadiq, R., Amyotte, P., & Veitch, B. (2009). Handling data uncertainties in event tree analysis. *Process Safety and Environmental Protection*, *87*(5), 283–292.
Garcez, T. V., & Almeida, D. E. A. T. (2014a). A risk measurement tool for an underground electricity distribution system considering the consequences and uncertainties of manhole events. *Reliability Engineering & Systems Safety*, *124*, 68–80.
Garcez, T. V., & Almeida, D. E. A. T. (2014b). Multidimensional risk assessment of manhole events as a decision tool for ranking the vaults of an underground electricity distribution system. *IEEE Transactions on Power Delivery*, *29*, 624–632.
Grant, K., Edgar, D., Sukumar, A., & Meyer, M. (2014). Risky business: perceptions of e-business risk by UK small and medium sized enterprises (SMEs). *International Journal of Information Management*, *34*, 99–122.
Hong, E.-S., Lee, I.-M., Shin, H.-S., Nam, S.-W., & Kong, J.-S. (2009). Quantitative risk evaluation based on event-tree analysis technique: application to the design of shield TBM. *Tunnelling and Underground Space Technology*, *24*(3), 269–277.
Jain, R. (1976). Decision making in the presence of variables. *IEEE Transactions on Systems Man and Cybernetics*, *6*, 698–703.
Kaufmann, A., & Gupta, M. M. (1988). *Fuzzy mathematical models in engineering and management science*. North-Holland, Amsterdam, N.Y: Elsevier Science Publishers.
Kiyomoto, S., Fukushima, K., & Miyake, Y. (2014). Security issues on IT systems during disasters: a survey. *Journal of Ambient Intelligence and Humanized Computing*, *5*, 173–185.
Liu, F., Dai, K., Wang, Z., & Ma, J. (2005). Research on fuzzy group decision making in security risk assessment. *In Networking—ICN*, *2005*, 1114–1121.
Magklaras, G. B., & Furnell, S. M. (2002). Insider threat prediction tool: evaluating the probability of IT misuse. *Computers & Security*, *21*(1), 62–73.
Mokhtari, K., Ren, J., Roberts, C., & Wang, J. (2012). Decision support framework for risk management on sea ports and terminals using fuzzy set theory and evidential reasoning approach. *Expert Systems with Applications*, *39*, 5087–5103.
Nejad, A. M., & Mashinchi, M. (2011). Ranking fuzzy numbers based on the areas on the left and right sides of fuzzy number. *Computers & Mathematics with Applications*, *61*(2), 431–442.
Nesseri, S. H., Zadeh, M. M., Kardoost, M., & Behmanesh, E. (2013). Ranking fuzzy quantities based on the angle of the reference functions. *Applied Mathematical Modelling*, *37*, 9230–9241.
Paula, S., & Vignon-Davillierb, R. (2014). Unifying traditional risk assessment approaches with attack trees. *Journal of Information Security and Applications*, *19*, 165–181.
NIST, (2002). Risk management guide for information technology systems, National Institute of Standards and Technology (NIST) Special Publication 800–30.
Pedrycz, W. (1994). Why triangular membership functions? *Fuzzy Sets and Systems*, *64*(1), 21–30.
Power, R., 2001. '2001CSI/FBI Computer Crime and Security Survey', Volume VII—No. 1, Computer.
Purba, J. H. (2014). A fuzzy-based reliability approach to evaluate basic events of fault tree analysis for nuclear power plant probabilistic safety assessment. *Annals of Nuclear Energy*, *70*, 21–29.
Ramzali, N., Lavasani, M. R. M., & Ghodousi, J. (2015). Safety barriers analysis of offshore drilling system by employing fuzzy event tree analysis. *Safety Science*, *78*, 49–59.
Rasheed, H. (2014). Data infrastructure security auditing in cloud computing environments. *International Journal of Information Management*, *34*, 364–368.
Rommelfanger, H. J. (2003). Fuzzy decision theory intelligent ways for solving real-world decision problems and for solving information costs. In G. Della Riccia, R. Kruse, D. Dubois, & H.-J. Lenz (Eds.), *Planning based on decision theory* (Vol. 472). CISM International Centre for Mechanical Sciences.
Rommelfanger, H. J. (1984). Entscheidungsmodelle mit fuzzy-nutzen. *In Operations Research Proceedings*, 559–567.
Rosqvist, T., Molarius, R., Virta, H., & Perrels, A. (2013). Event tree analysis for flood protection-an exploratory study in Finland. *Reliability Engineering & System Safety*, *112*, 1–7.
Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*, *15*, 112–133.
Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), 526–531.
Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications*, *18*, 45–52.
Shang, K., & Zakir, H. (2013). Applying fuzzy logic to risk assessment and decision-making. *Joint Risk Management Section of the CAS, the CIA, and the SOA, 2013, 3–4 and 32–40*.
Schneier, B. (2004). *Secrets & lies, digital security in a networked world*. Wiley Publishing.
Silva, M. M., Gusmão de, A. P. H., Poleto, T., Silva, L. C., & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management*, *34*, 733–740.
Sun, L., Srivastava, R. P., & Mock, T. J. (2006). An information systems security risk assessment model under the Dempster–Shafer theory of belief functions. *Journal of Management Information Systems*, *22*(4), 109–142.
Theoharidou, M., Kokolakis, S., Karyda, K., & Kiountouzis, M. E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*(6), 472–484.
Vílchez, J. A., Espejo, V., & Casal, J. (2011). Generic event trees and probabilities for the release of different types of hazardous materials. *Journal of Loss Prevention in the Process Industries*, *24*(3), 281–287.
Wang, P., Chao, K.-M., Lo, C.-C., Huang, C.-L., & Younas, M. (2007). A fuzzy outranking approach in risk analysis of web service security. *Cluster Computing*, *10*, 47–55.
Wang, X., & Kerre, E. E. (2001a). Reasonable properties for the ordering of fuzzy quantities (I), (2001). *Fuzzy Sets and Systems*, *118*(3), 375–385.
Wang, X., & Kerre, E. E. (2001b). Reasonable properties for the ordering of fuzzy quantities (II). *Fuzzy Sets and Systems*, *118*(3), 387–405.
Watson, S. R., Weiss, J. J., & Donell, M. L. (1979). Fuzzy decision analysis. *IEEE Transactions on Systems Man and Cybernetics*, *9*, 1–9.
Whalen, T. (1984). Decision making under uncertainty with various assumptions about available information. *IEEE Transactions on Systems Man and Cybernetics*, *14*, 888–900.
Yager, R. R. (1979). *Possibilistic decision making. IEEE, transactions on systems*. Man and Cybernetics.
Zadeh, L. A. (1965). Fuzzy sets. *Information Control*, *8*, 338–353.