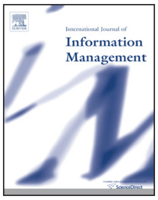
International Journal of Information Management 34 (2014) 733–740

Contents lists available at ScienceDirect

International Journal of Information Management

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



A multidimensional approach to information security risk management using FMEA and fuzzy theory

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

School of Engineering, Centre for Technology and Geosciences, Department of Production Engineering, Universidade Federal de Pernambuco, Recife PE, Caixa Postal 5125, CEP: 52.070-970, Brazil

ARTICLE INFO

Article history:
Available online 9 August 2014

Keywords:
Information security
Risk management
FMEA
Fuzzy theory

ABSTRACT

Because of the evolution and widespread use of the Internet, organisations are becoming more susceptible to attacks on Information Technology Systems. These attacks result in data losses and alterations, and impact services and business operations. Therefore, to minimise these potential failures, this paper presents an approach to information security risk management, encompassing Failure Mode and Effects Analysis (FMEA) and fuzzy theory. This approach analyses five dimensions of information security: access to information and systems, communication security, infrastructure, security management and secure information systems development. To illustrate the proposed model, it was applied to a University Research Group project. The results show that the most important aspects of information security risk are communication security, followed by infrastructure.

1. Introduction

In an information society, information is considered to be the primary asset of an organisation. It is also at constant risk, at more risk than ever before. This is, in part, a result of the Internet's evolution, which has lead organisations to share information (Bojanc & Blazic, 2008). Organisations are relying on Internet services as well as information systems (IS) to enhance business operations, facilitate management decision-making, and deploy business strategies (Kankanhalli, Teo, Tan, and Wei, 2003). As attacks on information systems become more dangerous, this dependence on IS leads to a corresponding increase in the impact of IS security abuses.

Security abuses, according to Bojanc and Blazic (2008), are related to technical failures, system vulnerabilities, human failures, fraud, and external events. Therefore, information security has become crucial to the survival of institutions to minimising risks that endanger organisations' operations, and to maintaining the confidentiality, integrity, and availability of information.

As stated in Yildrim, Akalp, Aytac, and Bayram (2011), information security policies are rules, instructions, and actions that provide information security to enterprises and define acceptable security levels in enterprises and associations. Because information security is not only a technical issue, but also a behavioural issue involving users (Bang, Lee, Bae, and Ahnc, 2012), it is essential that all employees and other collaborating enterprises comply with these policies. These policies are covered by the ISO 27001 standard, which is not a technical standard but rather a business standard that establishes the infrastructure for continuously improving information security in an organisation (Ozkan & Karabacak, 2010). According to these authors, organisational culture must change and executives must participate in the information security process to provide information security.

Conversely, prevention of the losses from attacks and other information system failures in an organisation is usually associated with continuous analyses and management of different information security measures. Therefore, realizing information security risk management in an organisation involves identifying and analysing risks to the organisation, identifying and assessing damage that may be caused by a successful attack on the business, and deciding to mitigate or reduce risk (Bojanc & Blazic, 2008).

However, as shown in Straub and Nance (1990), there are low level management concerns about IS security, e.g., managers assume the risk if the IS security abuse is low and decide to invest little in IS security; barriers to evaluating the benefits of information security exist; and some managers lack knowledge of the range of controls available to reduce IS security abuses.

Therefore, it is essential that an organisation define an information security procedure that enables an organisation to implement

* Corresponding author. Tel.: +55 81 21268728; fax: +55 81 21268728.
E-mail address: maisa.ufpe@yahoo.com.br (M.M. Silva).

http://dx.doi.org/10.1016/j.ijinfomgt.2014.07.005
0268-4012/© 2014 Elsevier Ltd. All rights reserved.

security risk management. Linking steps established by Bojanc and Blazic (2008) and Hoo (2000), this procedure encompasses identifying and evaluating business assets, consequences of security incidents, likelihood of a successful attack to the ICT systems, measures to minimise the risk of implementation of appropriate controls, and monitoring the effectiveness of implemented controls.

Following these steps to minimise these potential failures, this paper presents an approach to information security risk management based on FMEA and fuzzy theory. This approach analyses five dimensions of information security: access to information and systems, communication security, infrastructure, security management, and secure information systems development. Because these dimensions of information security are assessed using fuzzy numbers, one contribution of this paper is the way that fuzzy sets are compared to construct a preference ordering – risk priority. Much of the literature (Abbasbandy, 2009; Brunelli & Mezei, 2013) proposes a procedure based on defuzzification, which means that each fuzzy set is compressed into a single crisp real number, and the preference ordering is based on these crisp numbers. This procedure, however, neglects the spreads of fuzzy sets (Rommelfanger, 2003). This paper applies the procedure suggested by Adamo (1980), with the objective of preserving the information derived to evaluate the dimensions.

First we will briefly outline some information security risk management methodologies and directions to provide a brief background on our methodology. Then we will introduce the methodology and present a real case illustrating how the methodology is used to validate the proposed approach. Finally, we present discussions and concluding remarks.

2. Background

2.1. Information security risk management methodologies

According to Ozkan and Karabacak (2010), the preliminary step of risk management is risk analysis, which is defined as the systematic use of information to identify sources and to estimate the risk. Therefore, if it is not well performed, the selection of countermeasures will fail, and the risk management process cannot be successful. In terms of risk assessment, the basic steps for evaluation are determining the potential impact of an individual risk by assessing the likelihood that it will occur and the resulting impact if it should occur (Bojanc & Blazic, 2008).

There are several methodologies for evaluating information security risks. Generally, they are based on two types of risk analysis methods. The first type is based on qualitative risk analysis methods, in which many non-technical issues are easily accounted for and managers consider the risk-assessment calculations to be simple; it is unnecessary to quantify threat frequency (Patel, Graham, and Ralston, 2008). The second type, based on quantitative risk analysis methods, contains mathematical instruments to evaluate risk and, in this case, mathematical procedures, such as fuzzy logic, fault trees, and multi-criteria methods (Ozkan & Karabacak, 2010).

Bojanc and Blazic (2008) analysed several approaches enabling the assessment of the necessary investment in security technology from the economic point of view. They introduced methods for identifying the assets, the threats, and the vulnerabilities of the ICT systems. They proposed a procedure to select the optimal investment in the necessary security technology, based on quantifying the values of the protected systems.

The work by Patel et al. (2008) suggests a method to quantify risk in terms of a numeric value, presenting the threat-impact index and the cyber-vulnerability index, based on vulnerability trees. By qualifying information security quantitatively and comparing the indices for various possible security enhancements, managers can prioritise their security enhancement choices according to their relative effectiveness, select the best choice and statistically justify spending resources on the selected choice. In Ozkan and Karabacak (2010), a collaborative risk method for information security management was analysed. The analysis considered the common problems encountered during the implementation of ISO standards.

Table 1
FMEA system elements.

System element	Description
Potential failure modes and causes	The failure of information security should be defined clearly. In the current work, experts in security information were asked to explain the failure modes of each system
Potential effects of failure	The consequence of each failure mode should be carefully examined and recorded
Failure detections and compensation	All of the detected failures should be corrected to eliminate the cause and to maximise reliability
Assigning severity, occurrence, and detection	The current work's severity ranking is developed.

Deursen, Buchanan, and Duff (2013) proposed a methodology using a mixed methods approach, including a quantitative analysis of historical security incident data and expert elicitation through a Delphi study for monitoring information security risks within health care services.

Based on the works described, it should be noted that an effective risk management method is necessary for organisations willing to implement information security management practices. Therefore, this paper puts forward a multidimensional approach that uses fuzzy logic and FMEA for information security risk management.

2.2. A review of the FMEA methodology

Failure Mode and Effects Analysis (FMEA) is a complex engineering analysis methodology used to identify potential failure modes, failure causes, failure effects, and problem areas affecting the system's or product's mission success, hardware, and software reliability, maintainability, and safety. It also provides a structured process for assessing failure modes and mitigating the effects of those failure modes through corrective actions (McDemortt, Mikulak, and Beauregard, 2008).

Furthermore, the FMEA procedure starts by analysing all of the systems step by step; that is, by examining the system and subsystem functions. Table 1 shows system elements.

The FMEA method has been applied to many engineering areas. Offshore structures are popular applications. Wall, Pugh, Reay, and Krol (2002) explained how to utilise FMEA for Floating Production, Storage, and Offloading (FPSO) of vessels and other Floating Storage Units (FSUs).

Vinnem, Seljelid, Haugen, Sklet, and Aven (2007), after classifying FMEA as a qualitative risk assessment, gave many examples of offshore accidents lessons learned from past experiences. FMEA combined with fuzzy sets and Fuzzy Multi-attribute Decision Making (FMADM) methods have been applied to marine and offshore engineering subjects such as ballast water (Pam, Li, Wall, Yang, and Wang, 2013).

Geum, Cho, and Park (2011) proposed a systematic approach for identifying and evaluating potential failures using a service-specific FMEA and grey relational analysis. First, the service-specific FMEA was provided to reflect the service-specific characteristics, incorporating three dimensions and nineteen sub-dimensions to represent the service characteristics. As the second step under this

Table 2
Severity rating scale.

Rating	Description	Definition
10	Extremely dangerous	Failure could cause the death of a customer (patient, visitor, employee, staff member, business partner) and/or total system breakdown, without any prior warning.
9 8	Very dangerous	Failure could cause a major or permanent injury and/or serious system disruption with interruption in service, with prior warning.
7 6	Dangerous	Failure could cause a minor to moderate injury with a high degree of customer dissatisfaction and/or major system problems requiring major repairs or significant re-work.
5	Moderate danger	Failure could cause a minor injury with some customer dissatisfaction and/or major system problems.
4 3	Low to moderate danger	Failure could cause a very minor or no injury but annoys customers and/or results in minor system problems that can be overcome with minor modifications to the system or process.
2	Slight danger	Failure could cause no injury and the customer is unaware of the problem; however, the potential for minor injury exists. There is little or no effect on the system.
1	No danger	Failure causes no injury and has no impact on the system.

Table 4
Detection rating scale.

Rating	Description	Definition
10	No chance of detection	There is no known mechanism for detecting the failure.
9 8	Very remote/unreliable chance of detection	The failure can be detected only with a thorough inspection, and this is not feasible or cannot be readily performed.
7 6	Remote chance of detection	The error can be detected with a manual inspection, but no process is in place, so that detection left to chance.
5	Moderate chance of detection	There is a process for double-checks or inspections, but it is not automated and/or is applied only to a sample and/or relies on vigilance.
4 3	High chance of detection	There is 100% inspection or review of the process, but it is not automated.
2	Very High chance of detection	There is 100% inspection of the process, and it is automated.
1	Almost certain chance of detection	There are automatic "shut-offs" or constraints that prevent failure.

framework of service-specific FMEA, the risk priority of each failure mode was calculated using grey relational analysis.

Liu, Liu, Liu, and Mao (2012) applied the VIKOR method, which was developed for the multi-criteria optimisation of complex systems, to find the compromise priority ranking of failure modes according to the risk factors in FMEA. In the methodology, linguistic variables, expressed in trapezoidal or triangular fuzzy numbers, were used to assess the ratings and weights for the risk factors. The extended VIKOR method was used to determine the risk priorities of the failure modes that were identified.

According to FMEA, the risk priorities of failure modes are generally determined through the Risk Priority Number (RPN), which assesses three factors of risk: occurrence (O), severity (S), and detection (D). Then, the RPN is defined in Eq. (1).

$$\mathrm{RPN} = O_X S_X D \tag{1}$$

The occurrence factor measures the likelihood of a failure mode occurring. The severity is the expected consequence of the failure. The ability to realise the error before its consequences affect the costumers is measured by the detection factor. Considering the subjective aspect of these risk factors, the decision maker (DM) provides a fuzzy assessment of these values using a specific scale for each factor. Various scoring guidelines exist, and, in this paper, the proposed model uses the 10-point linguist scale for evaluating the O, S and D factors, as suggested by Goodman (1996), that are used in many applications of FMEA (Lin, Wand, Lin, and Liu, 2014; Liu et al., 2012). These scales are described in Tables 2–4.

2.3. Fuzzy theory

According to Pedrycz, Ekel, and Parreiras (2011), the fuzzy set theory, designed by Zadeh (1965), is one of the most fundamental concepts of science and engineering, because it can manage inaccurate information by manipulating mathematical terms. The notion of fuzzy sets is quite intuitive and transparent as it captures the essence of how things are perceived and described in everyday life.

The concept of a fuzzy set manages the representation of classes/categories that has boundaries that are ill-defined or flexible by means of characteristic functions taking values in an ordered set of membership values (Dubois & Prade, 1998). Therefore, fuzzy set A is, by definition, the membership function that maps the elements of the universe X to the unit interval [0, 1], as follows (Zadeh, 1965, 1975):

$$A : X \rightarrow [0, 1] \tag{2}$$

A fuzzy set A in X is therefore characterised by a membership function $f_A(x)$, which associates each point X with a real number in the interval [0, 1] with a value of $f_A(x)$ representing the association level of x with the set A. Therefore, the closer to one the value of $f_A(x)$ is assumed to be, the greater the membership of the element x is to the set A (Zadeh, 1965).

Assuming that A reflects a preference for the values of a variable x in X and because x is a decision variable and the fuzzy set A is an elastic constraint characterising the feasible values and the decision maker's preferences, $f_A(v)$ denotes the degree of preference in favour of v as the value of x. This interpretation prevails in fuzzy optimisation and decision analysis (Pedrycz et al., 2011).

Table 3
Occurrence rating scale.

Rating	Description	Potential failure rate
10	Certain probability of occurrence	Failure occurs at least once a day, or failure occurs almost every time.
9	Failure is almost inevitable	Failure occurs predictably, or failure occurs every 3–4 days
8	Very high probability of occurrence	Failure occurs frequently, or failure occurs about once per week.
7		
6	Moderately high probability of occurrence	Failure occurs approximately once per month.
5		
4	Moderate probability of occurrence	Failure occurs occasionally, or failure occurs once every 3 months.
3		
2	Low probability of occurrence	Failure occurs rarely, or failure occurs about once per year.
1	Remote probability of occurrence	Failure almost never occurs; no one remembers the last failure.

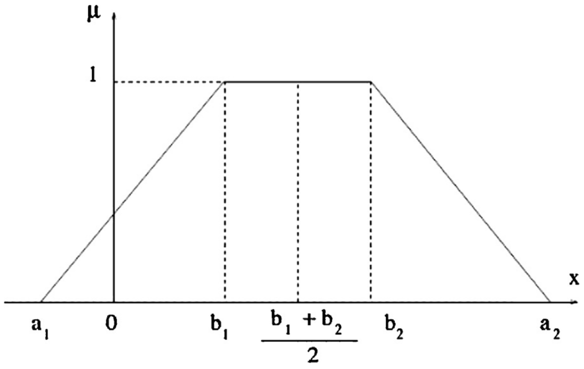


Fig. 1. Trapezoidal fuzzy number.
Adapted from Bojadziev and Bojadziev (2007).

The form of the membership functions reflects the problem at hand for which the fuzzy sets are constructed. It is also essential to assess the type of fuzzy set from the standpoint of its suitability for managing the ensuing optimisation procedures (Pedrycz et al., 2011). The most commonly used categories of membership functions—all defined in the universe of real numbers—are: triangular, trapezoidal, Gaussian, and Exponential-like membership functions.

A trapezoidal fuzzy number A, which is used in this paper, can be described according to its membership function as follows:

$$\mu_A(x) = \begin{cases} 0 & \text{if } \; x < a_1, \\ \dfrac{x - a_1}{b_1 - a_1} & \text{if } \; a_1 \leq x \leq b_1, \\ 1 & \text{if } \; b_1 \leq x \leq b_2, \\ \dfrac{x - a_2}{b_2 - a_2} & \text{if } \; b_2 \leq x \leq a_2, \\ 0 & \text{if } \; x > a_2, \end{cases} \tag{3}$$

where A can also be represented by $A = (a_1, b_1, b_2, a_2)$ (Fig. 1).

If $b_1 = b_2 = a_M$, A is a triangular fuzzy number: $A = (a_1, a_M, a_M, a_2) = (a_1, a_m, a_2)$.

Basic operations of fuzzy set theory can be reviewed here. They are extensions of the corresponding crisp numbers, supporting the determination of the fuzzy number. For more details, see Zadeh (1965), Bellman and Zadeh (1970), Bojadziev and Bojadziev (2007) and Belohlavek and Klir (2011).

Let $A_1 = (a_1, b_1, b_2, a_2)$ and $A_2 = (a_3, b_3, b_4, a_4)$ be two non-negative trapezoidal fuzzy numbers then:

$$\begin{aligned} A_1 + A_2 &= (a_1, b_1, b_2, a_2) + (a_3, b_3, b_4, a_4) \\ &= (a_1 + a_3, b_1 + b_3, b_2 + b_4, a_2 + a_4) \end{aligned}$$

$$\begin{aligned} A_1 - A_2 &= (a_1, b_1, b_2, a_2) - (a_3, b_3, b_4, a_4) \\ &= (a_1 - a_3, b_1 - b_3, b_2 - b_4, a_2 - a_4) \end{aligned}$$

$$-A_1 = -(a_1, b_1, b_2, a_2) = (-a_2, -b_2, -b_1, -a_1)$$

$$\begin{aligned} A_1 \otimes A_2 &= (a_1, b_1, b_2, a_2) \otimes (a_3, b_3, b_4, a_4) \\ &\cong (a_1 a_3, b_1 b_3, b_2 b_4, a_2 a_4) \end{aligned}$$

As presented in the previous subsection, the model proposed in this paper uses the 10-point linguist scale for evaluating the O, S, and D factors. Considering the difficulty of precisely evaluating the three risk factors, they are evaluated by experts using linguistic variables. According to Pedrycz et al. (2011), the notion of linguistic variables can be regarded as variables that have values that are fuzzy sets and assume values consisting of words or sentences expressed in a certain language, or in Zadeh's words (1975), "variables whose values are not numbers but words or sentences in a natural or artificial language".

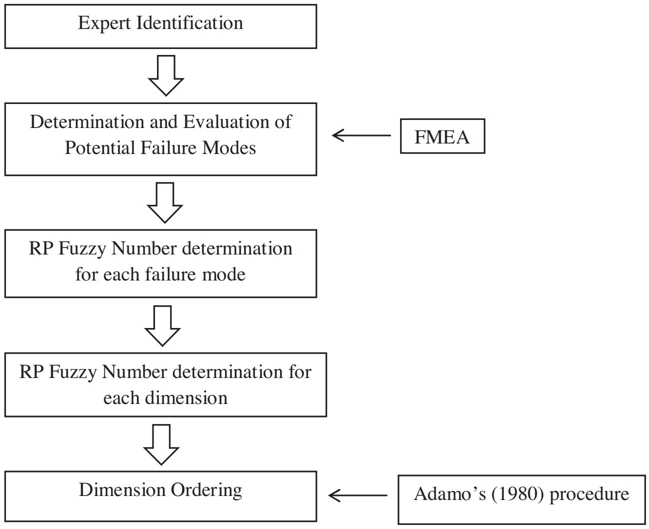

Expert Identification
Determination and Evaluation of Potential Failure Modes
FMEA
RP Fuzzy Number determination for each failure mode
RP Fuzzy Number determination for each dimension
Dimension Ordering
Adamo's (1980) procedure

Fig. 2. Steps of the proposed approach.

Further, Zadeh (1996) notes that the main contribution of fuzzy logic is a methodology for computing with words, which is a necessity when the available information is too imprecise to justify the use of numbers and is useful when there is a tolerance for imprecision that can be exploited to achieve tractability, robustness, a low solution cost, and a better rapport with reality.

For the reasons presented, the use of fuzzy theory and, more precisely, the use of linguistic variables can be justified.

3. The proposed information security risk management model

Because the problem addressed in this paper is to assess the risk to an organisation with respect to multiple dimensions of information security, the construction of a decision model is necessary in accordance with the vision of Belton and Stewart (2002). In this paper, an approach to information security risk management has been developed to analyse the five dimensions presented in the previous section based on FMEA and fuzzy linguistic theory. The approach proposed is presented in Fig. 2 and is detailed in next sections.

3.1. *Expert identification*

The first step of the approach consists of expert identification. The expert is the person who knows the enterprise systems and their vulnerabilities and is able to assess the information security risk to the organisation regarding the five dimensions. This step could also identify a group of experts and accomplish the analysis by considering their judgement.

3.2. *Determination and evaluation of potential failure modes*

This step determines the failure modes that are associated with five dimensions regarding information security. These five dimensions are based on Chen and Zhao (2013), who considered influencing factors in assessing information security risks, and Li and Tang (2013), who proposed an Information Security Engineering

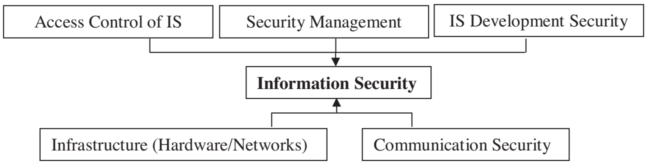


Fig. 3. Information security dimensions.

Table 5
Dimension descriptions.

Dimension element	Description
Access control of IS	Refers to the measures that control people's access to information and systems
IS development security	Refers to the methods, policies and procedures that lead to developing a secure information system
Infrastructure (hardware/networks)	Refers to the information security infrastructure that comprises the hardware and network resources
Security management	Refers to the planning and evaluation of information systems and maintaining secure information systems with the organisation based on principles of: confidentiality, integrity and availability (backup, recovery, and contingency between people)
Communication security	Refers to the measures adopted to ensure secure communication between people is achieved

Adapted from Li and Tang (2013).

(ISE) framework, based on four main issues of information security: definition, basic theory, methodology, and application. At the methodology level, they suggested different techniques for analysis and evaluation. In this paper, we combine FMEA and fuzzy logic to improve information security risk management. The failure modes associated with each dimension reflect the vulnerability of the company. The consequences of failure could be devastating.

Based on the four main issues associated with information security considered by Li and Tang (2013), and Chen and Zhao (2013), this paper presents a structure that encompasses the five dimensions associated with potential information security failures.

Each dimension in Fig. 3 is described in detail in Table 5.

These dimensions can be damaged by various activities, resulting in immediate or eventual serious failures modes in an IS (Table 6).

These failure modes are evaluated according to three risk factors suggested by the FMEA: occurrence, severity, and detection. In our representation, five intangible linguist terms are defined according to the following corresponding trapezoidal fuzzy numbers, from the 10-point linguist scale. Additionally, five-scale fuzzy linguistics are also used to assign the impact of each failure mode in each dimension. Table 7 describes both the linguistics scale and the trapezoidal fuzzy numbers for evaluating performance and impact.

Figs. 4 and 5 show detailed the membership values of the risk factors (performance) and the impact of each failure mode in each dimension, respectively.

3.3. RP fuzzy number determination

This step determines the RP fuzzy number for each failure mode using the trapezoidal fuzzy numbers that were used to evaluate the failure modes regarding the risk factors: occurrence, severity, and detection.

Let O_{ij}, S_{ij}, and D_{ij} be the trapezoidal fuzzy numbers that represent the occurrence, severity, and detection evaluations for dimension i and failure mode j. Then, the RP fuzzy number is the product of these risk factors:

$$RP \quad fuzzy \quad number_{ij} \cong O_{ij} \otimes S_{ij} \otimes D_{ij} \tag{4}$$

Table 6
Failures modes associated with each dimension of an IS.

Dimension	Failures modes
D1 – access of information and systems	D1.1: lack of management of removable computer media D1.2: lack of user password control (information system and network passwords) D1.3: lack of user register D1.4: lack of automatic terminal recognition D1.5: lack of user id authentication D1.6: lack of management of external access
D2 – communication security	D2.1: lack of safety of electronic mail D2.2: lack of safety of electronic office systems D2.3: lack of encryption control management D2.4: lack of limited content access to the Internet D2.5: lack of information safety education and training
D3 – infrastructure	D3.1: lack of information back-up D3.2: lack of network node certification D3.3: lack of software origination D3.4: lack of software safety defence D3.5: lack of a *cluster server* D3.6: lack of a back-up electric generator
D4 – security management	D4.1: lack of an information security audit D4.2: lack of a policy paper for information safety D4.3: lack of responsibility for information safety D4.4: lack of maintenance of hardware and software D4.5: lack of review of information security policies implemented
D5 – secure information systems development	D5.1: lack of standardisation and documentation of the software development process D5.2: failure to test against vulnerabilities and software conflicts D5.3: lack of a change monitoring log

Table 7
Linguistics scale and trapezoidal fuzzy numbers for evaluation of performance and impact.

Performance	Impact
Very low (VL): (0; 0; 1.5; 2)	Absolutely little influence (LI): (0; 0; 0.15; 0.2)
Low (L): (1.5; 2; 3.5; 4)	Little influence (LI): (0.15; 0.2; 0.35; 0.4)
Moderate (M): (3.5; 4; 5.5; 6)	Moderately influential (MI): (0.35; 0.4; 0.55; 0.6)
High (H): (5.5; 6; 7.5; 8)	Influential (I): (0.55; 0.6; 0.75; 0.8)
Very high (VH): (7.5; 8; 9.5; 10)	Very influential (VI): (0.75; 0.8; 0.9; 1)

3.4. Dimension evaluation

We can now calculate the total RP fuzzy numbers for the dimensions to compare and rank them with respect to the risks. They are evaluated by the expert for dimension i and failure mode j, with respect to economic and operational consequences. Finally, let I_{ij} be the influence (or impact) of each failure mode j on each dimension i.

$$RP \quad fuzzy \quad number_i = \sum_{j=1}^{m} RP \quad fuzzy \quad number_{ij} \quad j = 1, 2, \ldots, m. \tag{5}$$

where $RP\,fuzzy\,number_i$ is the total RP fuzzy score of the mth dimension and denotes the RP fuzzy score of the jth failure mode in the ith dimension, and j is the number of failure modes in each dimension.

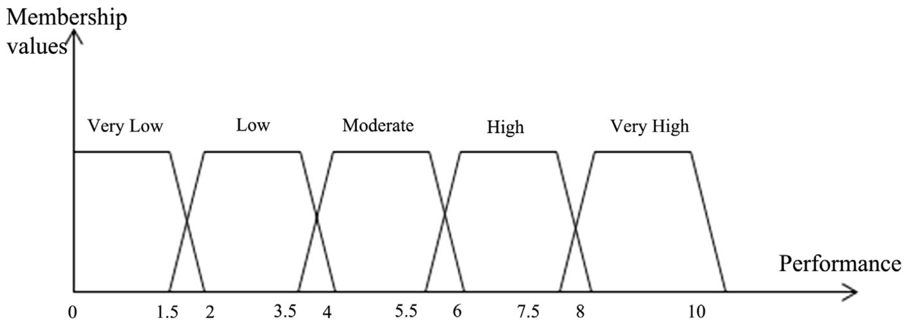


Fig. 4. Membership function of performance.

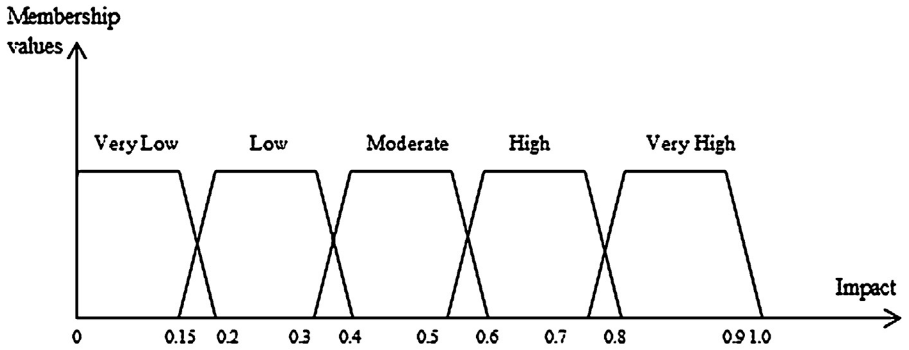


Fig. 5. Membership function of impact.

Table 8
Potential failure modes evaluations.

Dimension	Potential failure modes	Occurrence (O)	Severity (S)	Detection (D)
D1 – access of information and systems	D1.1: lack of management of removable computer media	(VL)	(VH)	(H)
	D1.2: lack of user password control (information system and network passwords)	(M)	(H)	(M)
	D1.3: lack of user register	(L)	(M)	(L)
	D1.4: lack of automatic terminal recognition	(M)	(H)	(M)
	D1.5: lack of user ID authentication	(L)	(M)	(M)
	D1.6: lack of management of external access	(H)	(VH)	(L)
D2 – communication security	D2.1: lack of safety of electronic mail	(VH)	(H)	(H)
	D2.2: lack of safety of electronic office system	(L)	(H)	(M)
	D2.3: lack of encryption control management	(L)	(M)	(L)
	D2.4: lack of limited content access to Internet	(VH)	(M)	(H)
	D2.5: lack of information safety education and training	(M)	(H)	(L)
D3 – infrastructure	D3.1: lack of information back-up	(L)	(VH)	(L)
	D3.2: lack of network node certification	(H)	(M)	(M)
	D3.3: lack of software origination	(M)	(H)	(H)
	D3.4: lack of software safety defence	(H)	(H)	(M)
	D3.5: lack of cluster server	(M)	(H)	(L)
	D3.6: lack of back-up electric generator	(VL)	(VH)	(M)
D4 – security management	D4.1: lack of information security audit	(L)	(M)	(M)
	D4.2: lack of policy paper for information safety	(L)	(L)	(L)
	D4.3: lack of responsibility for information safety	(M)	(M)	(M)
	D4.4: lack of maintenance of hardware and software	(H)	(VH)	(M)
	D4.5: lack of a review of the implemented information security policies	(M)	(H)	(L)
D5 – secure information systems development	D5.1: lack of standardisation and documentation of the software development process	(H)	(L)	(M)
	D5.2: failure to test against vulnerabilities and software conflicts	(VH)	(M)	(H)
	D5.3: lack of a change monitoring log	(H)	(H)	(M)

3.5. *Dimension ordering*

Different concepts for comparing fuzzy sets and for constructing preference orderings have been proposed (Abbasbandy, 2009; Brunelli & Mezei, 2013). Most of the concepts are based on defuzzification, meaning that each fuzzy set is compressed into a single crisp real number. The spreads of the fuzzy sets are neglected in the defuzzification process (Rommelfanger, 2003).

In this work, we will use the method suggested by Adamo (1980), which satisfies all of the properties proposed by Wang and Kerre (2001) and simply evaluates the fuzzy number on the rightmost point of the α-cut for a given α:

$$AD_{\alpha}(A) = a_{\alpha}^{+} \tag{6}$$

Table 9
RP fuzzy number for each failure mode.

Dimension	Potential failure modes	RP fuzzy number
D1 – access of information and systems	D1.1: lack of management of removable computer media	(0; 0; 85.5; 160)
	D1.2: lack of user password control (information system and network passwords)	(67.375; 96; 165; 288)
	D1.3: lack of user register	(7.875; 16; 38.5; 96)
	D1.4: lack of automatic terminal recognition	(67.375; 96; 165; 288)
	D1.5: lack of user ID authentication	(18.375; 32; 77; 144)
	D1.6: lack of management of external access	(61.875; 96; 142.5; 320)
D2 – communication security	D2.1: lack of safety of electronic mail	(226.875; 288; 427.5; 640)
	D2.2: lack of safety of electronic office system	(28.875; 48; 105; 192)
	D2.3: lack of encryption control management	(7.875; 16; 38.5; 96)
	D2.4: lack of limited content access to Internet	(144.375; 192; 313.5; 480)
	D2.5: lack of information safety education and training	(28.875; 48; 82.5; 192)
D3 – infrastructure	D3.1: lack of information back-up	(16.875; 32; 66.5; 160)
	D3.2: lack of network node certification	(67.375; 96; 165; 288)
	D3.3: lack of software origination	(105.875; 144; 247.5; 384)
	D3.4: lack of software safety defence	(105.875; 144; 225; 384)
	D3.5: lack of cluster server	(28.875; 48; 82.5; 192)
	D3.6: lack of back-up electric generator	(0; 0; 57; 120)
D4 – security management	D4.1: lack of information security audit	(18.375; 32; 77; 144)
	D4.2: lack of policy paper for information safety	(3.375; 8; 24.5; 64)
	D4.3: lack of responsibility for information safety	(42.875; 64; 121; 216)
	D4.4: lack of maintenance of the hardware and software	(144.375; 192; 285; 480)
	D4.5: lack of a review of the implemented information security policies	(28.875; 48; 82.5; 192)
D5 – secure information systems development	D5.1: lack of standardisation and documentation of the software development process	(28.875; 48; 105; 192)
	D5.2: failure to test against vulnerabilities and software conflicts	(144.375; 192; 313.5; 480)
	D5.3: lack of a change monitoring log	(105.875; 144; 225; 384)

4. Numerical application

The method proposed was applied in a university lab. There was an expert involved. The steps performed are the same as shown in Fig. 2 and are given below:

4.1. Step 1: expert identification

Evaluations were obtained from experienced experts in information security using their judgements, which is based on their knowledge and expertise in each risk factor. The expert can provide a precise numerical value, a range of numerical values, a linguistic term, or a fuzzy number. In many circumstances, if adequate information is obtained and the risk factor is quantitatively measurable, an expert is likely to provide a precise numerical value or a range of possible numerical values. However, the experts sometimes find that it is hard to give numerical values because of the uncertainties involved or because the risk factor is quantitatively immeasurable. Under those circumstances, a linguistic term or fuzzy number can then be used in the proposed model.

4.2. Step 2: potential failure modes determination and evaluation

Table 8 shows the potential failure mode evaluations for occurrence, severity, and detection.

4.3. Step 3: RP fuzzy number determination

Table 9 shows the RP fuzzy number for each failure mode. In the next step, we will evaluate each dimension.

4.4. Step 4: dimension evaluation

Based on the RP fuzzy number for each failure mode, we can now calculate the total RP fuzzy number for each dimension to compare and rank them with respect to risks, according to Eq. (5). The RP fuzzy numbers are presented in Table 10.

Table 10
RP fuzzy number for each dimension.

Dimension	RP fuzzy number
D1 – access of information and systems	(222.875; 336; 673.5; 1296)
D2 – communication security	(436.875; 592; 967; 1600)
D3 – Infrastructure	(324.875; 464; 777; 1528)
D4 – security management	(237.875; 344; 590; 1096)
D5 – secure information systems development	(279.125; 384; 643.5; 1056)

Table 11
Ranking of dimensions.

Interface ordering	Dimension	Value
1°	D2 – communication security	1283.5
2°	D3 – infrastructure	1152.5
3°	D1 – access of information and systems	984.75
4°	D5 – secure information systems development	849.75
5°	D4 – security management	843

4.5. Step 5: dimension ordering

Finally, for $\alpha = 0.5$, we present the ordered dimensions in Table 11, according to Adamo's value.

5. Results and discussion

In this study, a model of IS security risk management was formulated and tested on an academic group research project in a public organisation, examining the five dimensions. Applying the model to the project reveals the need for increased levels of awareness of dimensions D2 and D3. Further, to maintain and sustain dimensions D1, D5 and D4 at a high level of development, it is necessary to invest in infrastructure and communication.

Therefore, specific basic activities should receive more attention to improve those dimensions, such as: investing in information safety education and training, limiting access to Internet content, developing electronic mail safety, and realizing information backup. There is also value in defining information security policies that minimise the vulnerabilities of those activities and dimensions.

6. Conclusion

With the rise of potential risks, investments in security services are becoming a serious issue to many organisations, and various methodologies of information security risk management have been developed. Although there are many studies about IS security management in the literature, few of them are focused on combining FMEA and information security. Based on this, in this paper, we fill this void by creating a multi-dimensional model that addresses the five dimensions of information security and combines fuzzy logic with FMEA. The model provides guidelines and directions to researchers in the information security areas. It proposes five dimensions that cover a large section of existing information security risks. It then prioritises each area based on the criticality of the risk.

Although this paper focuses on the causes of system attacks, it should be noted that important effects/consequences could appear in different perspectives, such as: performance degradation in servers, work stations, or networks; network and system damage; information leakage or information loss (breach of commercial confidentiality); financial loss (cost of information recovery); reputation loss (impairment of business performance); and service interruption (disruption of business activities).

Finally, the main contribution of this paper is the ability to provide an organisation with information regarding the critical aspects and failures of their information security programmes that produce vulnerabilities in their systems. Additionally, the model measures these critical aspects of information security programmes.

As suggestions for future work, we recommend applying the model to a private organisation. We propose using an expert group decision approach, as there should be more than one expert for an IT department. We suggest defining the maturity levels of an organisation according to its perceptions of risks.

Acknowledgments

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

References

Abbasbandy, S. (2009). Ranking of fuzzy numbers, some recent and new formulas. In *Proceedings of IFSA-EUSFLAT 2009* (pp. 642–646).

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

Bang, Y., Lee, D.-Y., Bae, Y.-S., & Ahnc, J.-H. (2012). Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. *International Journal of Information Management*, *32*, 409–418.

Bellman, R. E., & Zadeh, L. A. (1970). Decision making in a fuzzy environment. *Management Science*, *17*, 4.

Belohlavek, R., & Klir, G. J. (2011). *Concepts and fuzzy logic*. Cambridge MA: The MIT Press.

Belton, V., & Stewart, T. J. (2002). *Multiple criteria decision analysis: An integrated approach*. Dordrecht, Netherlands: Kluwer Academic Publishers.

Bojadziev, G., & Bojadziev, M. (2007). *Fuzzy logic for business, finance and management* (2nd ed.). Inc. River Edge, NJ, USA: World Scientific Publishing Company.

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

Brunelli, M., & Mezei, J. (2013). How different are ranking methods for fuzzy numbers? A numerical study. *International Journal of Approximate Reasoning*, *54*, 627–639.

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

Deursen, N. V., Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within health care. *Computers & Security*, *37*, 31–45.

Dubois, D., & Prade, H. (1998). An introduction to fuzzy sets. *Clinica Chimica Acta*, *70*(1), 3–29.

Geum, Y., Cho, Y., & Park, Y. (2011). A systematic approach for diagnosing service failure: Service-specific FMEA and grey relational analysis approach. *Mathematical and Computer Modelling*, *54*, 3126–3142.

Goodman, S.L. (1996). Design for Manufacturability at Midwest Industries, Harvard Business School, February 2, Lecture.

Hoo, K. S. (2000). *How much is enough? A risk-management approach to computer security* (Working Paper). Palo Alto, CA: Consortium for Research on Information Security and Policy (CRISP), Stanford University.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*, 139–154.

Li, M., & Tang, M. (2013). Information security engineering: A framework for research and practices. *International Journal of Computers Communications*, *8*, 578–587.

Lin, Q.-L., Wand, D.-J., Lin, W.-G., & Liu, H.-C. (2014). Human reliability assessment for medical devices based on failure mode and effects analysis and fuzzy linguistic theory. *Safety Science*, *62*, 248–256.

Liu, H. C., Liu, L., Liu, N., & Mao, L. X. (2012). Risk evaluation in failure mode and effects analysis with extended VIKOR method under fuzzy environment. *Expert Systems with Applications*, *39*, 12926–12934.

Ozkan, S., & Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management*, *30*, 567–572.

Pam, E. D., Li, K. X., Wall, A., Yang, Z., & Wang, J. (2013). A subjective approach for ballast water risk estimation. *Ocean Engineering*, *61*, 66–76.

Patel, S. C., Graham, J. H., & Ralston, P. A. S. (2008). Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. *International Journal of Information Management*, *28*, 483–491.

Pedrycz, W., Ekel, P., & Parreiras, R. (2011). *Fuzzy multicriteria decision-making: Models methods and applications*. John Wiley and Sons.

McDemortt, R. E., Mikulak, R. J., & Beauregard, M. R. (2008). *The basics of FMEA* (2nd ed.). New York: Taylor & Francis Group.

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.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, *14*(1), 45–60.

Vinnem, J. E., Seljelid, J., Haugen, S., Sklet, S., & Aven, T. (2007). Generalised methodology for operational risk analysis. In *Proceedings of the European safety and reliability conference. ESREL 2007 – Risk, reliability and societal safety* (pp. 61–68).

Wall, M., Pugh, H. R., Reay, A., & Krol, J. (2002). *Failure modes, reliability and integrity of floating storage unit (FPSO FSU) turret and swivel systems* (Offshore Technology Report, 2001/073). HSE Books.

Wang, Z., & Kerre, E. E. (2001). Reasonable properties for the ordering of fuzzy quantities (I). *Fuzzy Sets and Systems*, *118*(3), 375–385.

Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, *31*, 360–365.

Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*, 338–353.

Zadeh, L. A. (1975). The concept of a linguistic variable and its application to approximate reasoning—I. *Information Sciences*, *8*(3), 199–249.

Zadeh, L. A. (1996). Fuzzy logic computing with words. *IEEE Transactions on Fuzzy Systems*, *4*, 2.

Maisa Mendonça Silva is an Assistant Professor at Universidade Federal de Pernambuco, where she teaches Operational Research topics. She holds a PhD in Production Engineering from the same university. Her special research interests are: Game Theory, Optimization methods, Fuzzy Theory and multicriteria decision aid.

Ana Paula Henriques de Gusmão is an Assistant Professor at Federal University of Pernambuco, where she is Coordinator of the Graduate program in Production Engineering. She holds a PhD in Production Engineering from the Federal University of Pernambuco. Her special interest lies in Information Systems, mainly on the following topics: information systems management, decision support systems, multicriteria decision aid and group decision.

Thiago Poleto is a PhD student at Universidade Federal de Pernambuco and has experience in Information Systems and Decision Support.

Lúcio Camara e Silva is an Assistant Professor at Universidade Federal de Pernambuco and has a PhD in Production Engineering from the same university. He has experience in Operational Research, Information Systems, Decision Support and Project Management.

Ana Paula Cabral Seixas Costa has a PhD in Production Engineering from Universidade Federal de Pernambuco. She is a CNPQ research and assistant professor at Universidade Federal de Pernambuco. She has experience in Production Engineering with emphasis on Information Systems, Decision Support and Multicriteria Decisions.