International Journal of Information Management 43 (2018) 248–260

Contents lists available at ScienceDirect

International Journal of Information Management

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

Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory

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

Universidade Federal de Pernambuco, CDSID – Center for Decision Systems and Information Development, Recife, Brazil

ARTICLE INFO

Keywords:
Cybersecurity
Information security
Risk analysis model
Fuzzy decision theory
Fault tree analysis

ABSTRACT

Cybersecurity, which is defined as information security aimed at averting cyberattacks, which are among the main issues caused by the extensive use of networks in industrial control systems. This paper proposes a model that integrates fault tree analysis, decision theory and fuzzy theory to (i) ascertain the current causes of cyberattack prevention failures and (ii) determine the vulnerability of a given cybersecurity system. The model was applied to evaluate the cybersecurity risks involved in attacking a website, e-commerce and enterprise resource planning (ERP), and to assess the possible consequences of such attacks; we evaluate these consequences, which include data dissemination, data modification, data loss or destruction and service interruption, in terms of criteria related to financial losses and time for restoration. The results of the model application demonstrate its usefulness and illustrate the increased vulnerability of e-commerce to cybersecurity attacks, relative to websites or ERP, due partly to frequent operator access, credit transactions and users' authentication problems characteristic of e-commerce.

1. Introduction

The recent boom of network-based technologies has produced a multitude of challenges to security and privacy (Gai, Qiu, Chen, Zhao, & Qiu, 2017; Gai, Qiu, Ming, Zhao, & Qiu, 2017; Gai, Qiu, Xiong, & Liu, 2018; Rahmani, Amine, Hamou, Boudia, & Bouarara, 2016). Indeed, cybersecurity and the attacks it aims to avert are regarded as among the most critical issues derived from the extensive use of networks (Gan & Brendlen, 1992); network security is a major problem because of the manifestations of threats in the forms of viruses, worms and botnets (Yang & Lui, 2014).

Ben-Asher and Gonzalez (2015) observe that one common target for cyberattacks is the public web server that connects a corporate network to the Internet; this public web server acts as a bridge, and enables attackers to access and deface the corporate web site. After gaining control of the web server, an attacker can also launch a Denial of Service (DoS) attack from within the network. However, (Huang et al., 2009) emphasize that the potential consequences of cyberattacks are not merely technical and can have broader implications. As such, cyberattacks represent an important issue for all organizations concerned with economic impacts, and interested in protecting its full scope of digital.

In terms of sheer numbers, cybercrime has been on the rise, with more than 59 million registered in 2015 (Bendovschi, 2015; Gartner Group, 2018); the level of damage sustained by its victims has also increased (Bendovschi, 2015). Cyber threats refer to internet-based attempts to damage or disrupt Information Systems (IS) and hack critical information; this means that one factor contributing to the surge in cyberattacks is, quite simply, the increased number of individual users accessing the internet. Most of the 3 billion people who access the internet annually do so in the absence of the proper training and protection that a technical security staff provides; therefore, individual internet users represent a significant point of weakness in cybersecurity (Anderson & Agarwal, 2010; Bang, Lee, Bae, & Ahn, 2012).

Thus, risk analysis is an important activity that organizations must perform, to prevent the attacks and/or negative consequences that can arise from them. Indeed, many researchers have already proposed cybersecurity models intended to help organizations counter cyberattacks. However, two critical gaps symptomatic to several of these proposals ultimately motivated the development of this paper and will

* Corresponding author at: Universidade Federal de Pernambuco, CDSID – Center for Decision Systems and Information Development, Caixa Postal 5125, CEP: 52.070-970, Recife, Brazil.

E-mail addresses: anapaulahg@hotmail.com (A.P. Henriques de Gusmão), maisa@cdsid.org.br (M. Mendonça Silva), thiagopoleto@hotmail.com (T. Poleto), lucio@cdsid.org.br (L. Camara e Silva), apcabral@ufpe.br (A.P. Cabral Seixas Costa).

https://doi.org/10.1016/j.ijinfomgt.2018.08.008
Received 24 January 2018; Received in revised form 20 July 2018; Accepted 25 August 2018
Available online 31 August 2018

be fully articulated in the next section, which is dedicated to giving an account of related works, but generally speaking, they involve the following: (i) a lack of structured methods for identifying the causes of cyberattack scenarios, and (ii) a lack of quantitative measures for the impacts associated with cyberattacks, including metrics that would facilitate analyses of financial risk and restoration time.

To fill these two gaps, account for the association between risk analysis and decision theory (Borgonovo, Cillo, & Smith, 2018) and in recognition of the multiplicity of criteria usable for a given risk analysis (Almeida et al., 2015; Medeiros, Alencar, & De Almeida, 2017), this paper proposes a multicriteria approach to cybersecurity risk analysis. More precisely, it considers the construction and analyses of payoff matrices reflecting effects obtained via different combinations of alternatives and scenarios. The resulting proposed approach provides the opportunity to comment about an evaluation of the particular criteria, as well as the aggregated multicriteria risks. For the construction of scenarios, this paper proposes the use of fault tree analysis (FTA), to determine the vulnerability of cybersecurity and identify the potential consequences of cyberattacks. The alternatives evaluation process was developed using decision theory and fuzzy analysis. Therefore, the main contributions of this paper are twofold:

(1)

(1) We propose a structured approach to characterizing the causes of cyberattack scenarios that relies on the FTA method.
(2) We propose an approach to measuring cyberattack scenarios that considers the risk of financial losses and analysis of restoration time analysis via the fuzzy theory decision.

The significance of our work hinges on the fact that our model was specifically developed to facilitate the quantitative evaluation of the cybersecurity risks associated with particular applications, instead of prioritizing potential risks, as previously proposed in several papers (Abdo, Kaouk, Flaus, & Masse, 2017; Grant, Edgar, Sukumar, & Meyer, 2014; Lopez-nicolas & Jose, 2008; Mik, 2012). As such, this paper analyzed website, e-commerce and enterprise resource planning (ERP) attacks, respectively (although it is possible to evaluate other applications), acknowledging each application's importance to the organizational context and its vulnerability to attacks, and considering possible consequences such as data dissemination, data modification, data loss or destruction and service interruption, in terms of criteria related to both financial losses and time for restoration.

The remainder of this paper is organized as follows: Section 2 presents an account of related literature regarding cybersecurity and cybersecurity risk models; Section 3 provides a methodological background on fault tree analysis, fuzzy theory, and decisions under uncertainty; then, Section 4 introduces the methodology explaining the mechanism of the proposed approach, followed by Section 5, which provides a numerical example validating the proposed approach; discussions of the main findings, along with the implications for theory and practice, are presented in Section 6; and finally, Section 7 is dedicated to conclusions, limitations of the study, and suggestions for future works.

2. Related works

This section presents related works regarding cybersecurity and cyberattack risk assessment models. It also outlines the limitations of these previous approaches and, consequently, details the main contributions of this paper.

2.1. Cybersecurity

Cybersecurity is defined as information security—applied to computing systems, computer networks or the Internet, as a whole—aimed at averting cyberattacks, including but not limited to, malicious attempts to damage or destroy a computing system or network (Von Solms & van Niekerk, 2013). In general, cyberspace assets require protection from extremely hostile environments and intended harm targeting private organizations and government agencies (Wang, Zheng, Lou, & Hou, 2015; Whitley, 2009). According to the Gartner Group (2018), in 2017, the global cybersecurity market was valued at USD 103.84 billion. This amount of money, in addition to the cost of the damages sustained by the main consequences of the attacks (e.g., loss of information, reestablishment of the system, among others), justifies the efforts of so many researchers to study and gain a better understanding of the subject. We emphasize three main areas characteristic of the cybersecurity studies that have been undertaken.

The first area is related to technology, with a particular focus on developing technological solutions to reduce or identify threats and attacks. Goodall, Lutters, and Komlodi, (2009) studied cybersecurity analysis and the practical aspects of intrusion detection, highlighting the expertise required to successfully detect intrusions. Kim, Yan, and Zhang, (2015) presented an effective automated detection system, namely *DART*, to identify fake webpages on the Internet. Bou-Harb, Debbabi, and Assi, (2013) presented an approach composed of two techniques intended to tackle the challenges of detecting corporate cyber scanning and clustering distributed reconnaissance activity, respectively. Burmester, Magkos, and Chrissikopoulos, (2012) described a framework for modeling the security of a cyber-physical system in which the behavior of the adversary is controlled by a threat model that captures—in a unified manner—the cyber aspects (with discrete values) and the physical aspects (with continuous values) of the cyber-physical system. Dasgupta (2007) focused on building an autonomic defense system, using immunological metaphors for information gathering, analyzing, decision making and launching responses to threats and attacks. Rejeb, Leeson, and Green, (2006) proposed an algorithm for localizing the sources of multiple attacks and identifying their nature in all-optical networks. Recent works have also focused on wireless smart grid networks (Gai, Qiu, Chen et al., 2017, 2017b), mobile data sharing and transferring (Gai, Qiu, Chen et al., 2017, 2017b), and transmissions using multi-channel communications (Gai, Qiu, Chen et al., 2017, 2017b; Gai et al., 2018). However, several of these approaches do not measure the impacts of a cyberattack and/or do not evaluate these attacks in a managerial manner, contradicting (Soomro, Shah, & Ahmed, 2016), which argued that, because technological solutions depend on information security policy and organizational strategies, they should be approached from a managerial perspective.

The second area in the research is related to the analysis of investments in cybersecurity. Bojanc, Jerman-Blažič, and Tekavčič, (2012) presented a financial approach to assessing the required information and communication technology (ICT) security investment that considered return on investment (ROI), net present value (NPV) and internal rate of return (IRR), to quantify the costs and benefits of security investments. Chai, Kim, and Rao, (2011) examined the value of an investment in Information Technology (IT) security, based on stock market investors' reactions to firms' IT security investment announcements. Bojanc and Jerman-Blažič (2008) presented a mathematical model to optimize security-technology investment evaluation and decision-making processes, based on a quantitative analysis of the security risks and a digital-assets assessment in an organization. There are several limitations to these approaches, including the lack of studies assessing the risk of financial losses. Indeed, according to Patel, Graham, and Ralston, (2008) assessing the financial losses that result from information security attacks complicates already-challenging risk assessment models.

The third research area concerns models aimed at measuring the risk of cyberattacks. Organizations should identify and evaluate the main threats, prior to investing in internal-use protection technologies, because they need risk metrics to prioritize expenditures of their limited resources, to make their IS more secure (Cowley, Greitzer, & Woods, 2015). However, numerical approaches to quantifying cybersecurity

risk are still very few, relative to qualitative ones (Patel et al., 2008). Therefore, this paper focuses on the third area, because: (i) it provides guidance for more efficient technological solutions to prevent attacks; (ii) it renders the analysis of investments more easily; and (iii) it has been minimally explored in prior research. Therefore, the next section presents cyberattack risk assessment models, along with the gaps identified in the foregoing literature on these models that motivated the development of this paper. It also describes this paper's mode of overcoming the limitations of these previous studies.

2.2. Cyberattack risk assessment models

According to Patel et al. (2008), risk-assessment methods can be either qualitative or quantitative. Qualitative risk-assessment methods are used primarily in cases where risk-assessment calculations are simple and, therefore, when it is either unnecessary or impossible to quantify threat frequency and other technical issues. The quantitative risk analysis methods are mathematical instruments for evaluating risk where mathematical procedures, such as fuzzy theory, fault trees, and multicriteria methods are used.

The quantitative methods of risk analysis are incorporated into what the literature refers to as probabilistic risk assessment (PRA), which is a systematic methodology for assessing the risks associated with an entity (Ralston, Graham, & Hieb, 2007). The PRA encompasses different methods, such as fault/attack (FTA) tree analyses, event tree analysis (ETA) and failure mode and effect analysis (FMEA). Although they share a common purpose, they approach risk assessment distinctively. Deductive methods, such as the FTA, aim to determine the causes of an undesirable event. To do this, they start by defining the undesirable event and then trace backward, to causes. By contrast, inductive methods, such as the FMEA, aim to determine the consequences, by defining an instigating event and tracing forward, to consequences.

Shin, Son, Khalil ur, and Heo, (2015) proposed a cybersecurity risk model, based on a Bayesian network that enables the evaluation of both the procedural and technical aspects of cybersecurity. Jaganathan, Cherurveettil, and Sivashanmugam, (2015) proposed a mathematical model for predicting the impact of a cyberattack, based on the number of vulnerabilities that influence cybersecurity, given the environmental information required. Silva, de Gusmão, Poleto, Silva, and Costa, (2014) proposed a multidimensional approach that uses fuzzy theory and FMEA for information security risk management. Similarly, Silva, Poleto, Camara, Henriques, and Cabral, (2016) proposed a risk management model based on a multidimensional perspective of big data risk analysis, which integrates FMEA and grey theory. Kawanaka, Matsumaru, and Rokugawa, (2014) presented a method for quantifying the risk of cyberattacks on production control systems that result from the failure to apply security patches, expressing the risk as a monetary amount. Shaikh, Adi, and Logrippo, (2012) proposed two dynamic risk-based decision methods for enhancing control over access to healthcare systems. Zhang, Ho, and He, (2009) presented an approach for measuring the impacts of attacks on security systems, using a cost-benefit analysis and a set of benchmark data to suggest a rational response. Rice and AlMajali (2014) discussed the fragmented landscape of studies regarding the risk of cyberattacks on smart metering systems, drawing on concepts from systems engineering and fault tolerance design to organize and unify the pieces. Lo and Chen (2012) proposed a hybrid procedure for assessing risk in information security and verified the proposal in a health insurance institute. Finally, given that risk assessment models rely predominantly on probability models, which form the basis for informed decision making related to risk in many areas. Gusmão, Silva, Silva, Poleto, and Costa, (2016) propose a risk analysis model for information security based on Decision Theory. Although these authors use the ETA/FTA method, their model is based solely on the criterion of financial losses.

As such, our model departs from previous research, because it contributes to the identification and discovery of causal chains that lead to failures and provides quantitative evaluations of the effects of a potential cyberattack, in terms of criteria of both financial losses and time for restoration. More precisely, given that the first step toward preventing, detecting and evaluating the consequences of cyberattacks is understanding the current causes of failure in cyberattack prevention, and the extent to which prior research has failed to provide structured methods for characterizing the causes of cyberattack scenarios, this paper proposes the use of FTA. Indeed, based on the literature review, it appears that organizations are susceptible to cybersecurity risks such as data dissemination, data modification, data loss or destruction, service interruption and critical information infrastructure breakdown. As such, threats must be found and eliminated. Although there are several PRA techniques, as described above, the use of FTA is also justifiable as a way of understanding the context of cyberattacks and possible scenarios by focusing on a particular accident event and providing possible failure causes. Moreover, experts usually find that it difficult to give numerical values, because of the uncertainties involved or the quantitative immeasurability of the risk factor. In fact, Ralston et al. (2007) observe that the natural extension to PRA involves the use of fuzzy logic. Thus, this paper uses fuzzy decision theory, because fuzzy concepts provide a way of dealing with uncertainty in both the probabilistic parameter estimates and subjective judgments. The next section provides a methodological background on FTA methodology, fuzzy theory, and decisions under uncertainty.

3. Methodological background

A brief description of the framework of fault tree analysis (FTA) is given in the next subsection. Subsequently, the fuzzy theory and its properties are presented, followed by a subsection dedicated to decisions under conditions of uncertainty.

3.1. Fault tree analysis

Fault tree analysis (FTA is a technique for conducting safety and reliability analyses, using a graphic representation to model causal chains that lead to failures (Hauptmanns, 2002; Ruijters & Stoelinga, 2015). It also provides a structured tree format that offers a high-level understanding of a system without the need for a detailed analysis, allowing for timely detection of scenarios that lead to hazards (Ferdous, Khan, Veitch, & Amyotte, 2009; Hauptmanns, 2004).

This technique has been applied in many contexts. For example, (Chi, Lin, & Dewi, 2014) applied FTA to representing the causal relationships among events and causes that contributed to fatal falls in the construction industry. Rahman, Varuttamaseni, Kintner-Meyer, and Lee, (2013) developed a new method that permits customers to predict the reliability of a distribution power system, using FTA and customer-weighted values of component failure frequencies and downtimes. Yuhua and Datao (2005) estimated the probability of failure for oil and gas transmission pipelines by using fuzzy FTA. To better understand human behavior, when incidents occur. Doytchev and Szwillus (2009) propose an analytical concept that combines FTA and task analysis (TA). Cheng, Li, Chu, Yeh, and Simmons, (2013), in a case study of an aerospace manufacturer, used FTA to decrease an inventory and improve its turnover rate.

In the cybersecurity context, the initial step of FTA is to define a possible cyber-attack failure event and trace its influences back to the basic influential factors. From this initial event, it is possible to visualize different causes and levels of cyberattack. Nevertheless, cyberattacks are attempts by hackers to damage or destroy computer networks or systems, and they vary in complexity, magnitude and impact. The aim of FTA is to find the minimal cut set, which refers to a combination of minimum basic events, the occurrence of which will cause the top event. By analyzing cut sets, actions can be prioritized to prevent the occurrence of the top event and find weak points in the system (Mahmood, Ahmadi, Verma, Srividya, & Kumar, 2013). To evaluate the

complexity, magnitude and impact of a cyberattack, this paper proposes the use of fuzzy theory and decisions under uncertainty, which are described in subsections 3.2 and 3.3.

3.2. Fuzzy theory

According to Zadeh (1965), 1975) and Pedrycz, Ekel, and Parreiras, (2011), a fuzzy set theory can be defined as a set of objects in which the membership values—which express the degree to which each object is compatible with the features distinctive to the collection—can assume values between 0 (complete exclusion from the collection) and 1 (complete membership to the collection). Then, a fuzzy set C is described by a membership function that maps the elements of a universe X to the unit interval [0,1] (Pedrycz et al., 2011):

$$C: X -> [0, 1]$$

A fuzzy set can also be viewed as a set of ordered pairs of the form *{x, C(x)}* where *x* is an element of *X* and *C(x)* denotes its corresponding degree of membership.

Membership functions can be represented in different forms. The most common membership functions are: triangular; trapezoidal, T-membership, S-membership, Gaussian and exponential. The type of membership function should reflect the problem that is being confronted, the perception of the concept represented and the level of detail required.

The triangular membership function is the form adopted in this paper to represent the alternatives evaluation. This type of membership function can be described as follows (Pedrycz et al., 2011):

$$C(x, a, m, b) = \begin{cases} 0 & if\ x \le a \\ \frac{x-a}{m-a} & if\ x \in [a, m] \\ \frac{b-x}{b-m} & if\ x \in [m, b] \\ 0 & if\ x \ge b\,, \end{cases} \quad (1)$$

where the three parameters *a*, *b* and *m* represent, respectively, the lower and upper bounds and the modal value of the fuzzy set. One reason for choosing this type of function is that triangular fuzzy sets are the simplest possible model for establishing grades of membership.

3.3. Decisions under uncertainty

Raiffa (1968) proposed a scheme for organizing and systematizing the decision-making process. Pursuant to this scheme, the consequences of any action are cannot be regarded as certain, since events, which cannot be predicted, may intervene to affect the outcomes. These decisions under uncertainty are required in many real-life situations. With this in mind, Belyaev (1977) defines the stages necessary for resolving decision problems under uncertainty:

- statement of the problem;
- identification of the nature states that are representatives for the problem;
- calculation and preliminary analysis of solution alternatives;
- calculation of payoff matrix;
- analysis of payoff matrix and choice of rational actions; and
- choice and implementation of action.

As several types of uncertainty are encountered in complex systems problems (Ekel, Martini, & Palhares, 2008), the statement of a problem is not an easy task. Among other things, in this stage, the decision maker (DM) must establish the correct form of an evaluation function $F(A_i, \theta_s)$ that estimates the consequence of i different actions A under s different natures states θ.

In this function, it is necessary to choose a finite number s of points that sufficiently characterize the set θ of nature states. The number of nature states should be established by accounting for the peculiarities of the problem and the available computational power. The next stage—preliminary analysis of solution alternatives—aims to identify the dominant alternatives.

Table 1
Payoff Matrix.

	θ_1	...	θ_s	...	θ_S
A_1	$F(A_1, \theta_1)$	...	$F(A_1, \theta_s)$	...	$F(A_1, \theta_S)$
...	...	...	...	...	...
A_i	$F(A_k, \theta_1)$	...	$F(A_k, \theta_s)$	...	$F(A_k, \theta_S)$
...	...	...	...	...	...
A_I	$F(A_K, \theta_1)$	...	$F(A_K, \theta_s)$	...	$F(A_K, \theta_S)$

The calculation of the payoff matrix consists of evaluating each action/alternative A_i $(i = 1;...;I)$ for all selected natures states θ_s $(s = 1;...;S)$. A generic payoff matrix is illustrated in Table 1.

The stage of analysis that involves the payoff matrix and choice of rational actions is supported by one or more (when the aim is comparing the recommendations) criteria proposed for uncertainty conditions (the criteria of Wald, Laplace, Savage and Hurwitz). However, none of them inspires wholehearted confidence, and no single criterion can be used for the final choice of action. Thus, final choices must be made by DMs, based on their experience and intuition (Belyaev, 1977; Ekel et al., 2008).

According to Ekel et al. (2008), the criterion of Laplace, used in this paper, is oriented to choosing the solution alternative A^L for which the estimate $\overline{F}(A_i)$ is the maximum.

$$\max_{1 \le i \le I} \overline{F}(A_i) = \max_{1 \le i \le I} \frac{1}{S} \sum_{s=1}^{S} F(A_i, \theta_s) \quad (2)$$

In Eq. (2), $\overline{F}(A_i)$ is the objective solution average level for the given solution alternative. Thus, $\overline{F}(A_i)$ is estimated by (3).

$$\overline{F}(A_i) = \frac{1}{S} \sum_{s=1}^{S} F(A_i, \theta_s) \quad (3)$$

$F(A_i)$ represents the objective function maximum level (the most optimistic estimate, if the objective function is to be maximized, or the most pessimistic estimate if the objective function is to be minimized for the considered solution alternative) or the objective function minimum level (the most pessimistic estimate if the objective function is to be maximized, or the most optimistic estimate if the objective function is to be minimized for the considered solution alternative). Therefore, $F(A_i)$ could be estimated, respectively, by (4) and (5).

$$F^{\max}(A_i) = \max_{1 \le s \le S} F(A_i, \theta_s) \quad (4)$$

$$F^{\min}(A_i) = \min_{1 \le s \le S} F(A_i, \theta_s) \quad (5)$$

Considering that $R(A_i, \theta_s)$ is an over-expenditure that occurs under a combination of the θ_s and the alternative A_i, instead of the locally optimal solution alternative under this nature state θ_s, the risk maximum level is defined by (6) (Belyaev, 1977).

$$R^{\max}(A_i) = \max_{1 \le s \le S} R(A_i, \theta_s) \quad (6)$$

This risk shows a relative difference of the objective function values under the choice of one solution alternative over another and characterizes a damage level associated with the situation's uncertainty.

In this paper, based on the approach described by Bellman and Zadeh (1970) and Ekel et al. (2008), each objective function $F_p(A)$ is replaced by a fuzzy membership function $\mu_{Cp}(A)$ for a given criterion p, where $p = 1,..., q$. A fuzzy solution D is produced as a result of the intersection $D = \cap_{p=1}^{q} \mu_{Cp}$, where $\mu_D(A_i) = \min_{1 \le p \le q} \mu_{Cp}(A_i)$ for a fuzzy solution D with the given fuzzy sets of the type C_p. The intersection operation leads to a solution that proves the maximum degree

$$\max \mu_D(A_i) = \max_{1 \le i \le I} \min_{1 \le p \le q} \mu_{Cp}(A_i, \theta_s) \tag{7}$$

which reduces the problem to finding

$$A = \arg\max_{1 \le i \le I} \min_{1 \le p \le q} \mu_{Cp}(A_i, \theta_s) \tag{8}$$

To obtain the solution of (8), one may use the condition

$$\mu_{Cp}(A_i, \theta_s) = \frac{F_p(A) - \min F_p(A)}{\max F_p(A) - \min F_p(A)}^{\lambda_p} \tag{9}$$

for maximized objective functions or

$$\mu_{Cp}(A_i, \theta_s) = \frac{\max F_p(A) - F_p(A)}{\max F_p(A) - \min F_p(A)}^{\lambda_p} \tag{10}$$

for minimized objective functions, where λ_p are important factors for the corresponding objective functions. Finally, Laplace's criterion can be written according to (11).

$$\max_{1 \le i \le I} \mu_D(A_i) = \max_{1 \le i \le I} \frac{1}{S} \sum_{s=1}^{S} \min_{1 \le p \le q} \mu_{Cp}(A_i, \theta_s) \tag{11}$$

Equations (12),(13) and (14) represent, respectively, the membership function maximum level, the membership function minimum level and membership function average level.

$$\mu_D^{\max}(A_i) = \max_{1 \le s \le S} \mu_D(A_i, \theta_s) \tag{12}$$

$$\mu_D^{\min}(A_i) = \min_{1 \le s \le S} \mu_D(A_i, \theta_s) \tag{13}$$

$$\overline{\mu}_D(A_i) = \frac{1}{S} \sum_{s=1}^{S} \mu(A_i, \theta_s) \tag{14}$$

More details on the application of approach described by Bellman and Zadeh (1970) to decision making in fuzzy environments (decisions under uncertainty) can be found in (Ekel et al., 2008).

4. Proposed model

The aim of the proposed model is to evaluate the consequences of potential cyberattacks, considering such possibilities as data dissemination, data modification, data loss or destruction and service interruption, in terms of criteria of both financial losses and time for restoration.

The proposed cybersecurity model includes five phases: expert identification, understanding the causes of possible attack scenarios, definition of criteria, fuzzy assessment and finally, aggregation and ordering. Thus, the main aim is practical support for controlling and evaluating cybersecurity attacks, including, for example, contributions to the identification and discovery of causal chains that lead to failures, evaluations of the consequences of a cyberattack and evaluations of a potential cyberattack's effects, in terms of some criteria. However, it could also be regarded as a specific procedure per security attribute evaluation method (SAEM), which helps information-system stakeholders determine the extent to which their security investment is consistent with the expected risks (Butler, 2002).

The main structure of this model is shown in Fig. 1 and detailed as follows.

4.1. Expert identification

Throughout the decision-making process, it is necessary to identify a person or group of people who, based on experience, act at the right time to maximize the decision value and are able to identify the following: the vulnerabilities of the organization and, consequently, the potential accidents; possible scenarios; and the chances of occurrence and judgments about each of these elements. This is called expert identification.

4.2. Understand the causes of possible attack scenarios

To allow for timely detection of scenarios that lead to hazards, this paper proposes the use of the FTA technique. The resulting influence hierarchy (Fig. 2) is depicted as an upside-down tree that shows the failure events. Using the event tree, the possible outcomes of an initiating event and the sequences that may result, in each outcome, can be identified.

The procedure for performing a FTA in the context of cyberattacks consists of the following steps shown in (Table 2).

Other hybrid techniques of risk analysis, such as human error analysis techniques (HEAT), event tree analysis (ETA), risk-based maintenance (RBM) method, highlighted by Marhavilas, Koulouriotis, and Gemeni, (2011), could have been used, but this paper applies FTA, because it focuses on a particular accident event and provides a method for determining possible failure causes of cyberattacks. The results of FTA support analysis of the vulnerability of a system's cybersecurity and identify the possible consequences of cyberattacks, as illustrated in Table 3.

4.3. Definition of criteria

Considering the uncertainties of risk analysis, this paper proposes the use of models presented in (Ekel et al., 2008). Further, as this paper deals with cybersecurity risk analysis, it appears inappropriate to estimate solution consequences on the basis of a single criterion.

Therefore, this paper relies on two criteria for evaluation: financial losses and time for restoration. According to Butler (2002), security managers could identify risk as a product of cost and threat, if threat data were available, which they are only rarely, and all costs could be described in economic terms. In fact, Jaganathan et al. (2015) showed that cost implications must be considered. For instance, Silva et al. (2014) developed an information security risk model that considers cost as a criterion for evaluating possible consequences. The second criterion considers the ability to rapidly repair, reconstitute or replace damaged/disabled services and return to an acceptable level of functionality. It may also involve repairing or replacing parts that have suffered physical damage from a cyberattack. Some of these parts may require long lead times for replacement, due to skilled installation workforce availability issues. For example, an attacker may have access to valuable information and also sabotage the network services (Ben-Asher & Gonzalez, 2015). Although this paper considers only these two criteria, the process it outlines is not restricted to them.

4.4. Fuzzy assessment of potential accidents

This step consists of the evaluation of each alternative a_i regarding the criteria j identified by the managerial expert. Three alternatives were chosen, based on their importance to the organizational context and their vulnerability to attacks, according to the literature. For instance, Offutt (2002) argues that websites are especially critical with regard to cybersecurity, because the world wide web has transformed from a static collection of HTML web pages into a dynamic platform that comprises e-commerce, collaborative work and distribution of information and entertainment. Lokhande & Meshram, (2013) observe that no one in the E-Commerce industry is satisfied with its present ability to measure the costs and probabilities of cyberattacks. Moreover, these authors assert that there are no standard methodologies for cost measurement, and that the study of the frequency of attacks is hindered by the reluctance of organizations to publicize their experiences with security breaches. Finally, the ERP Cybersecurity survey (2017), conducted by Crowd Research Partners and ERP Scan, interviewed more than 1900 cybersecurity experts and found that 89% expect to see a surge in attacks on ERP systems. Considering these examples, available

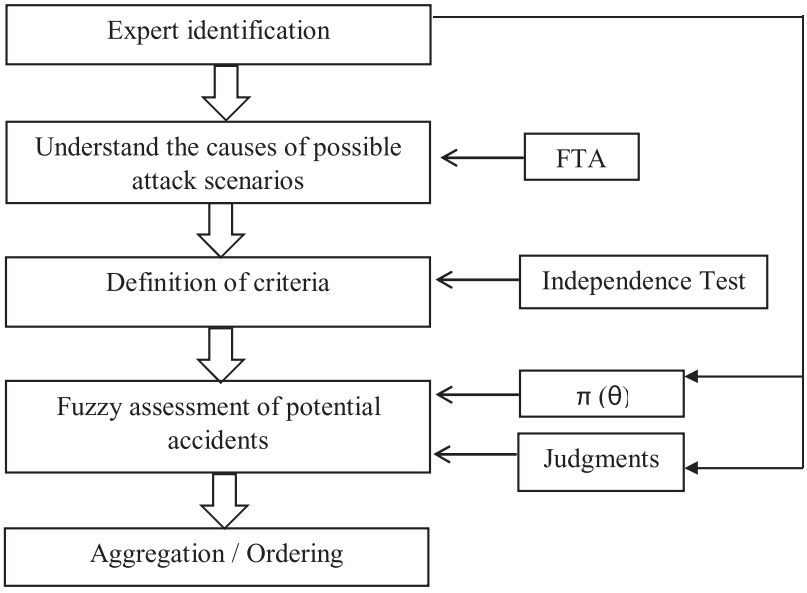

Fig. 1. Steps of the proposed model.

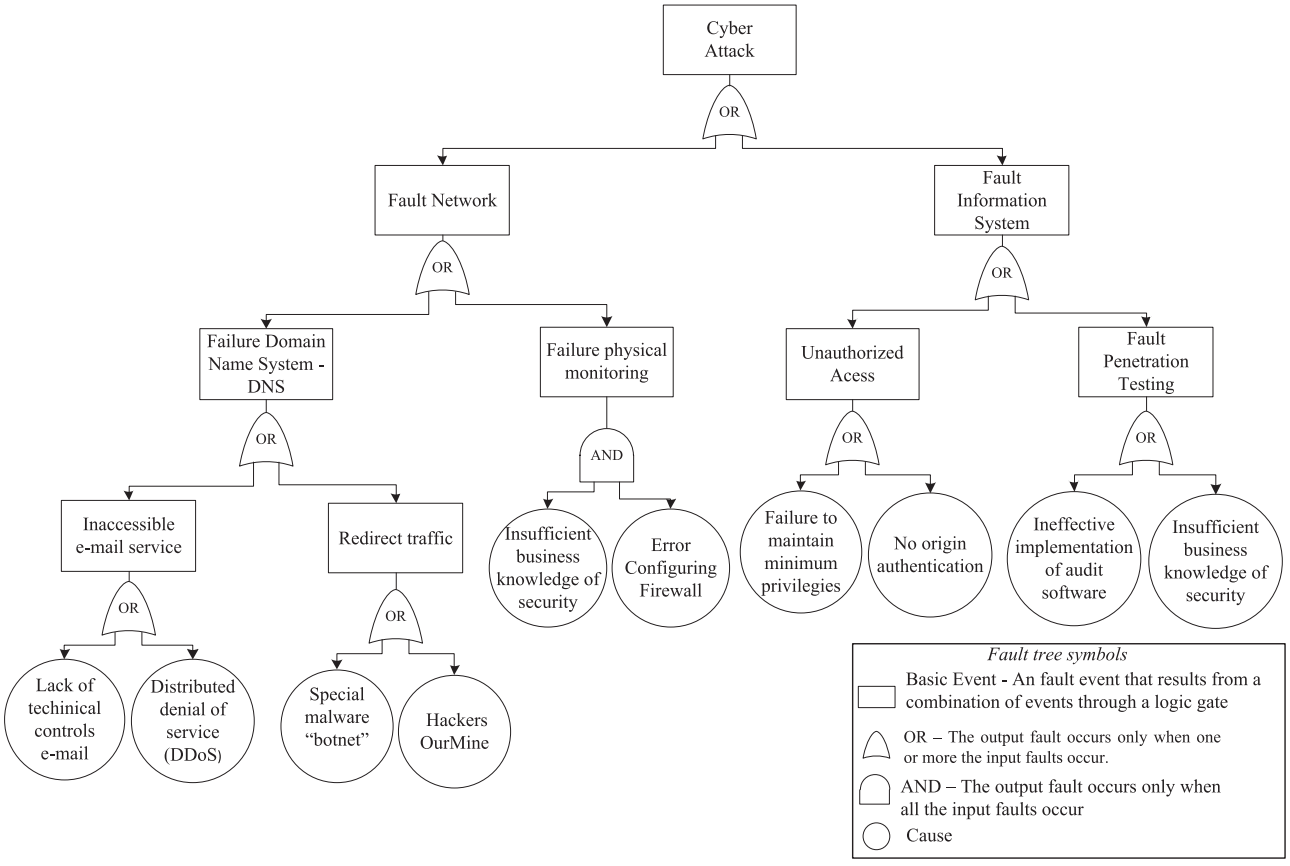

Fig. 2. Structure produced by the application of FTA in cyberattacks on a computer.

in the literature, Table 3 explicitly describes the three alternatives evaluated in this paper.

With the criteria and alternatives established, it remains to define the nature states Table 4. Next, an alternatives evaluation must be performed by the expert, using fuzzy logic and the priori probabilities ($p(s_j)$), represented by π(θ).

4.5. Aggregation / ordering

The final steps involve aggregating all of the criteria used and ordering the alternatives, according to the magnitude of their consequences and using the foregoing Eqs. (2–14). The next section provides a numerical application, to illustrate the applicability of our approach.

Table 2
Procedure for fault tree analysis.

Step	Definition
Step 1	Define the system of interest regarding the cyberattacks and as initial conditional causes of failure in the security system.
Step 2	Define the top event for the analysis and specify the problem of interest that the analysis will address.
Step 3	Define the treetop structure. Determine the events and conditions (i.e., intermediate events) that lead most directly to the top event, which in this case can be faulty network and fault IS.
Step 4	Explore each branch in successive levels of detail. Determine the events and conditions that lead most directly to each intermediate event.

5. Numerical application

This section provides an example, based on a real-life context, to illustrate the applicability of the present proposal. Although actual data (in terms of the required information) have not been used, the data used to provide an overview of the model are, nevertheless, realistic and were provided by an information security expert. 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 under evaluation.

Three indicators were recommended by Cooke, ElSaadany, and Huang, (2008), to properly select experts, and they are as follows: the number of scientific publications, recommendations from a wide range of experts, and experiences of previous similar studies.

Pursuant to the aforementioned recommendations, the expert employed for this paper is a senior academic, with more than 20 years of experience. She holds a PhD in information systems (IS), has published eleven research papers in this field and her age is between 40–49 years. She also has experience as a consultant on IS to companies in the private sector. Her main research interest and practitioner's area include information security and cybersecurity. However, this step could also identify a group of experts and accomplish the analysis by considering their judgement, using specific procedures to aggregate their opinions.

To proceed with the analysis, it is necessary to, first, define the nature states, the criteria and the alternatives. Next, the alternatives evaluation must be performed by the expert, 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, as noted in Section 3.3.

Thus, the nature states (θ), which are the possible result scenarios (nature states) regarding the alternatives, are defined as data dissemination (θ_1), data modification (θ_2), data loss or destruction (θ_3) and service interruption (θ_4), as can be seen in Table 3.

Based on Shameli-Sendi, Cheriet, and Hamou-Lhadj, (2014), we propose the use of two criteria: financial losses (in thousands of dollars) and restoration time (in hours), to justify the use of a multicriteria approach. It is important to note here that two interdependency tests (interdependency in utility and additive interdependency) were performed, using an elicitation process. Both tests demonstrated the independence of these two criteria, which allowed us to use decision theory (Appendix A and Appendix B). For more details, see the study conducted by (Keeney & Raiffa, 1976).

Table 4
Potential Consequences.

Nature States (θ)	Description
data dissemination (θ_1)	This involves the distribution or transmission of confidential data to other unauthorized users.
data modification (θ_2)	This involves the deletion, insertion or alteration of information in an unauthorized manner.
data loss or destruction (θ_3)	This involves the theft of confidential information
service interruption(θ_4)	This involves rendering the service unavailable or reducing its performance (Whitley, 2009).

Table 5
Expert's Elicitation Evaluation for Financial Criterion.

Alternatives (A_i)	θ_1	θ_2	θ_3	θ_4
Website	VL	L	M	VL
E-Commerce	H	VH	H	VH
ERP	M	H	H	H

The elicitation process for monetary losses is simple, as money has a clear meaning for most people. Similarly, recovery time is also easy to understand. In the present example, a minor financial loss and a shorter recovery time is preferable to the DM (the information security expert).

The example focuses on the invasion of website, e-commerce and ERP. Tables 5 and 6 illustrate the expert's evaluation concerning each pair of alternatives and nature state, according to each criterion. This evaluation was performed using a 5-point linguistic scale, ranging from very low (VL) to very high (VH). Experts sometimes find it difficult to assign numerical values, because of the uncertainties involved or because the risk factor is quantitatively immeasurable. This model thereby minimizes this difficulty.

As seen in Tables 7 and 8, we used triangular fuzzy numbers, according to a linguistic scale, for both criteria.

Tables 9 and 10 were obtained using (9) and (10). The aggregate payoff matrix is shown in Table 11.

The risk matrix was obtained using (5) and the alternatives ranking was constructed using the criterion of Laplace (11). These results are illustrated in Table 12.

According to the evaluation, e-commerce is the riskiest alternative, followed by ERP and website. The next section presents a brief discussion of these results, compares them with the principal findings in the existing literature and outlines the main contributions for research and implications for practice.

Table 3
Potential Alternatives and Their Cyberattack Consequences.

Alternative	Description	Source
Deface website	A common target for cyberattacks is the public web server that connects a corporate network to the Internet. The web server typically runs http and ftp services, and the attacker gains control over the server by exploiting vulnerabilities in these services.	Nabi (2011) and Offutt (2002)
E-Commerce	E-commerce businesses that accept credit card payments on a case-by-case basis can experience breaches of sensitive cardholder data, which may involve large fines and, in many cases, bad press and a loss of trust and credibility (Nabi, 2011).	Nabi (2011) and Ganesan, Gobi, and Vivekanandan, (2010)
Enterprise Resource Planning (ERP)	These platforms store the most valuable information and run the core business processes of an organization. Components may be prone to vulnerabilities that can be exploited to compromise the system. Thus, cyberattacks who breach an ERP platform will be able to impose high-impact attacks against the victim organization (Nunez, 2012).	Nunez (2012), Goel and Kiran (2012) and ERP Cybersecurity survey (2017).

Table 6
Expert's Elicitation Evaluation for Restoration Time Criterion.

Alternatives (A_i)	θ_1	θ_2	θ_3	θ_4
Website	L	VL	M	H
E-Commerce	M	H	H	VH
ERP	M	H	M	VH

Table 7
Verbal Scale Regarding Monetary Range.

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

Table 8
Verbal Scale Regarding Time to Restoration Range.

Linguistic Terms	Fuzzy Number	Values	Unit
Very low	Triangular	(1; 3; 8)	Hours
Low	Triangular	(6; 12; 30)	Hours
Moderate	Triangular	(24; 36; 48)	Hours
High	Triangular	(40; 72; 120)	Hours
Very high	Triangular	(96; 160; 240)	Hours

Table 9
Modified Payoff Matrix for Financial Criterion.

Alternatives (A_i)	θ_1	θ_2	θ_3	θ_4
Website	(1; 1; 1)	(0.89; 0.86; 0.89)	(0.72; 0.69; 0.69)	(1; 1; 1)
E-Commerce	(0.39; 0.41; 0.4)	(0; 0; 0)	(0.39; 0.41; 0.4)	(0; 0; 0)
ERP	(0.72; 0.69; 0.69)	(0.39; 0.41; 0.4)	(0.39; 0.41; 0.4)	(0.39; 0.41; 0.4)

Table 10
Modified Payoff Matrix for Restoration Time Criterion.

Alternatives (A_i)	θ_1	θ_2	θ_3	θ_4
Website	(0.95; 0.94; 0.91)	(1; 1; 1)	(0.76; 0.79; 0.83)	(0.59; 0.56; 0.52)
E-Commerce	(0.76; 0.79; 0.83)	(0.59; 0.56; 0.52)	(0.59; 0.56; 0.52)	(0; 0; 0)
ERP	(0.76; 0.79; 0.83)	(0.59; 0.56; 0.52)	(0.76; 0.79; 0.83)	(0; 0; 0)

6. Discussion

It is well-established that, in the field of information security, threats change rapidly, rendering many traditional approaches to security obsolete or indeed, unworkable, in terms of e-commerce and Business to Business (B2B) models. E-commerce involves several functional requirements, such as transacting data, transacting payments or marketing information, as well as using credit card numbers when consumers make purchases from a retailer. In fact, due to the complex nature of e-commerce business activities, the software necessary to support these transactions, and thus, the high dependence of e-commerce on information technology, renders e-commerce significantly more vulnerable to cybersecurity threats than ordinary websites and ERP systems.

For instance, Whitley (2009) observed that new or modified threats assume many forms and require radical reviews of IT policies. This author demonstrated a concern regarding one main issue: growth in risks with regard to e-commerce content. Similarly, Nabi (2011) noted that the major cause for concern about e-commerce relates to the perceived security and privacy risks associated with e-transactions (e.g., data, smart cards, credit cards and exchange of business information by means of online transactions). Further, Bella, Giustolisi, and Riccobene, (2011) argued that privacy is a major concern in e-commerce and that there are two main paradigms for protecting the customer's privacy: maintaining a customer's trust and a customer's anonymity. Trompeter and Eloff (2001) addressed ethical issues of e-business information security controls.

Similarly, a cyberattack on e-commerce can also cause disruptions affecting business, leading to a lower volume of sales, or no sales at all. Moreover, it can also result in losses due to the following: fraud, legal costs, recovery and cleanup costs, regulatory fines, loss of customer accounts, opportunity costs of reduced sales (due to reduced customer trust), costs of recovering unanticipated damage to infrastructures. In addition, as sales may be lost if customers are unable to access the company's e-commerce, service interruption may be regarded as one of the worst scenarios. It is important to note that this interruption is not always associated with the hosting company, but rather with the hackers who perpetrated an attack on the sales organization system that caused this kind of damage.

This study's main findings are consistent with the existing literature. However, one important point is that, when the method is applied to different organizations, the results reflect the type of business and size of the organization under analysis and the perceptions of the expert. Consequently, the results of this paper reflect the perception of an expert, with regard to a specific situation based on realistic data; as such, other results may be derived by applying this proposal in other contexts.

6.1. Contributions to research

This study contributes to the information security literature in several ways. First, it investigates the circumstances and consequences of cyberattacks from a broader managerial view. Prior research, regarding cybersecurity risk assessment, tends to focus on the infrastructural impacts of a disaster and, consequently, neglects the evaluation of the risk of cyberattacks in other contexts (e.g., software applications). However, the inability to measure potential consequences across different scenarios of cyberattacks, renders it virtually impossible to do a good job of ensuring information security. Second, this study analyses risk scenarios by accounting for the judgments of experts and multiple criteria, to provide a more strategic and less technical evaluation of these scenarios and promote new insights in this

Table 11
Aggregate Payoff Matrix with Characteristics Estimates.

(A_i)	θ_1	θ_2	θ_3	θ_4	μ_D^{Max} (Ai)	μ_D^{Min} (Ai)	$\overline{\mu}_D$ (Ai)
Website	(0.95; 0.94; 0.91)	(0.89; 0.86; 0.89)	(0.72; 0.69; 0.69)	(0.59; 0.56; 0.52)	(0.95; 0.94; 0.91)	(0.59; 0.56; 0.52)	(0.79; 0.76; 0.75)
E-Commerce	(0.39; 0.41; 0.4)	(0; 0; 0)	(0.39; 0.41; 0.4)	(0; 0; 0)	(0.39; 0.41; 0.4)	(0; 0; 0)	(0.19; 0.21; 0.2)
ERP	(0.72; 0.69; 0.69)	(0.39; 0.41; 0.4)	(0.39; 0.41; 0.4)	(0; 0; 0)	(0.72; 0.69; 0.69)	(0; 0; 0)	(0.38; 0.38; 0.37)
μ_D^{Max} (θi)	(0.95; 0.94; 0.91)	(0.89; 0.86; 0.89)	(0.72; 0.69; 0.69)	(0.59; 0.56; 0.52)			

Table 12
Risk Matrix.

Alternatives (A_i)	θ_1	θ_2	θ_3	θ_4	R^{Max} (Ai)	Ranking
Website	(0; 0; 0)	(0; 0; 0)	(0; 0; 0)	(0; 0; 0)	(0; 0; 0)	3rd
E-Commerce	(0.56; 0.53; 0.51)	(0.89; 0.86; 0.89)	(0.33; 0.28; 0.29)	0.59;0.56;0.52)	(0.89;0.86;0.89)	1st
ERP	(0.23; 0.25; 0.22)	(0.50; 0.45; 0.49)	(0.33; 0.28; 0.29)	(0.59;0.56;0.52)	(0.59;0.56;0.52)	2nd

area. Third, this research shows that fault tree analysis and fuzzy decision theory complement each other, and were relevant to providing an effective definition of the causes of possible accident scenarios and a fuzzy assessment of potential accidents regarding cybersecurity risks.

Consequently, these three contributions also motivate the development of further risk assessment research in cybersecurity, as the model proposed herein presents a great deal of flexibility, not only with respect to the definition of the scenarios, but also with regard to the use of multiple criteria. Several of these possibilities are presented in the Section 7.1, which describes the study's limitations and offers suggestion for further research.

6.2. Implications for practice

From a practical viewpoint, the results of this study suggest several potential avenues of modified conduct for practitioners and information security professionals addressing the issue of vulnerability regarding cyberattacks.

Four implications are cited below, three of which are directly related to the results obtained in this work, which identifies e-commerce as the riskiest application for cyberattacks, and the fourth concerns the implication of using our model in other contexts. In general, the main findings of this paper and its implications are consistent with the literature discussed in previous sections and, therefore, a large part of the recommendations following the implications can also be obtained from the aforementioned literature. Indeed, as Internet transactions develop, business success will depend on ensuring customer safety. Thus, the empirical results suggest that the risk assessment of cyberattacks from the proposed model can provide more accurate information, thereby leading companies to design e-commerce systems that ensure the security of the privacy and of customers' data.

The first implication concerns the need to improve public awareness of these safety measures. To do so, companies must take a more proactive approach to influencing and even providing security features to their customers, to prevent them from being the sources of such threats. Banking companies, perhaps because they are attacked most severely, exemplify organizations that already operate this way, by requiring that user proceed in a safe manner, via enabling iToken devices in their customers' computers.

The second implication relates to the fact that e-commerce security issues are often associated with privacy issues. The harmful potential of cyberattacks and the consequent harm of organizations is directly associated with access to and misuse of information from the organization's customers. In this sense, organizations should invest in mechanisms that prevent access to private information in the case of cyberattacks; for example, automatic network defense system and advanced digital cryptography system might be implemented.

The third practical implication relates to the fact that infrastructure is a crucial security dimension, because vulnerabilities in e-commerce can permit intruders to infiltrate the network and cause undesirable damage to system operations. Therefore, investment in infrastructure should include not only technologies and devices to prevent the occurrence of cyberattacks or to minimize the impact of these attacks (the first two practical implications), but also to generate backups that enable contingency operation of the enterprise systems in case of cyberattacks, to minimize their impact, from the point of view of system interruption and financial losses–two aspects addressed in this work.

Finally, the fourth implication concerns the use of our proposed model in different contexts, which may identify potential risks in other applications. In this sense, our proposal provides insights regarding the risk of cyberattacks that may significantly affect the organization and society, due to unavailability of the service; for example, consider the major problems that emerge from the failure of electricity networks. Further, our proposal can potentially facilitate the development of better skills to generate more high-quality cybersecurity via preemptive diagnosis.

7. Conclusion

Faced with the Conclusions ongoing increase in the use of digital media by organizations that support their business and, consequently, their possible associated risks, those organizations must adopt methodologies that enable them to analyze and measure potential internal impacts that may result from cyberattacks. It is worth noting that, despite two decades of research in the area, extant approaches suffer from serious limitations, as shown in the mains findings of Shameli-Sendi et al. (2014). Moreover, making a direct comparison of ERP, websites and e-commerce, regarding risk, is a novelty in the field. Consequently, proposals such as those advanced in this paper are of great importance and can address this gap.

This paper expands on the research deriving from the study conducted by Gusmão et al. (2016), in which a cybersecurity risk analysis model, developed through the integration of decision theory and fuzzy logic, was proposed. Further, detection of scenarios that lead to hazards was structured using fault tree analysis. In this structured analysis, important aspects could be identified, to determine the vulnerability of cybersecurity and ascertain the potential consequences of cyberattacks.

To illustrate the applicability of the proposed model, an example was developed, using three alternatives for evaluation (a website, ERP and e-commerce), regarding data dissemination, data modification, data loss or destruction and service interruption consequences, in terms of both financial costs and time to restoration. The results of the model application demonstrate its usefulness and show that e-commerce may be more vulnerable to cybersecurity attacks than websites or ERP, partly due to frequent operator access, credit transactions and users' authentication problems.

7.1. Limitations and suggestion for further research

Although our study makes a number of contributions, as shown in Section 6, it suffers from some limitations. First, the use of a probabilistic approach is restricted to situations in which risk might be predictable (e.g. natural disasters, accidents). However, where there is malicious intent behind an attack, security risks are frequently short-lived or transient (i.e., unpredictable). This makes sense, because skilled attackers use innovative and creative ways to circumvent controls, which renders them unconstrained by probabilistic estimates. Second, our proposal accounts for the analysis of risk from the view of a single expert. However, the context of information security is complex. Therefore, drawing on the combined knowledge of multiple experts would be appropriate, to harness as much human expertise as possible and increase the robustness of how estimates are made.

One path forward, for future research, is developing an information security maturity model, to quantify the risk level associated with a

given organization. Future research can also be incorporated into our model: (i) other criteria, such as expenses related to customer support and financial penalties or lawsuits; (ii) new threats from the introduction of new IT services into organizations, such as cloud-based business services (Ali, Warren, & Mathiassen, 2017; Ratten, 2016; Venters & Whitley, 2012). This paper also suggests the performance of time series modeling, to directly compare e-commerce, ERP and websites, using datasets of vulnerabilities.

Acknowledgements

This research was partially supported by the Universidade Federal de Pernambuco, and the GPSID – Decision and Information Systems Research Group. The authors would like to thank CNPQ – the Brazilian National Council for Scientific and Technological Development. We would also like to thank the two anonymous referees for their valuable comments, which improved the quality of the paper.

Appendix A. Utility independence Test

L1				L2			
Worst prize		Best prize		Worst prize		Best prize	
Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time
1.000	120	120	0	1.000	0	120	120
L1				L2			
Worst prize		Best prize		Worst prize		Best prize	
Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time
1.000	120	200	0	1.000	0	200	120
L1				L2			
Worst prize		Best prize		Worst prize		Best prize	
Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time
1.000	120	400	0	1.000	0	400	120
L1				L2			
Worst prize		Best prize		Worst prize		Best prize	
Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time
1.000	120	600	0	1.000	0	600	120
L1				L2			
Worst prize		Best prize		Worst prize		Best prize	
Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time
1.000	120	120	40	1.000	40	120	120
L1				L2			
Worst prize		Best prize		Worst prize		Best prize	
Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time
1.000	120	200	40	1.000	40	200	120
L1				L2			
Worst prize		Best prize		Worst prize		Best prize	
Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time
1.000	120	400	40	1.000	40	400	120
L1				L2			
Worst prize		Best prize		Worst prize		Best prize	
Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time
1.000	120	600	40	1.000	40	600	120
L1				L2			
Worst prize		Best prize		Worst prize		Best prize	
Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time
1.000	120	120	80	1.000	80	120	120
L1				L2			
Worst prize		Best prize		Worst prize		Best prize	
Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time	Financial Criterion	Restoration time

1.000	120	200	80	1.000	80	200	120
L1 Worst prize Financial Criterion 1.000	Restoration time 120	Best prize Financial Criterion 400	Restoration time 80	L2 Worst prize Financial Criterion 1.000	Restoration time 80	Best prize Financial Criterion 400	Restoration time 120
L1 Worst prize Financial Criterion 1.000	Restoration time 120	Best prize Financial Criterion 600	Restoration time 80	L2 Worst prize Financial Criterion 1.000	Restoration time 80	Best prize Financial Criterion 600	Restoration time 120
L1 Worst prize Financial Criterion 1.000	Restoration time 120	Best prize Financial Criterion 120	Restoration time 120	L2 Worst prize Financial Criterion 1.000	Restoration time 120	Best prize Financial Criterion 120	Restoration time 120
L1 Worst prize Financial Criterion 1.000	Restoration time 120	Best prize Financial Criterion 200	Restoration time 120	L2 Worst prize Financial Criterion 1.000	Restoration time 120	Best prize Financial Criterion 200	Restoration time 120
L1 Worst prize Financial Criterion 1.000	Restoration time 120	Best prize Financial Criterion 400	Restoration time 120	L2 Worst prize Financial Criterion 1.000	Restoration time 120	Best prize Financial Criterion 400	Restoration time 120
L1 Worst prize Financial Criterion 1.000	Restoration time 120	Best prize Financial Criterion 600	Restoration time 120	L2 Worst prize Financial Criterion 1.000	Restoration time 120	Best prize Financial Criterion 600	Restoration time 120

Appendix B. Additive Utility independence test

	L1			
The certainty equivalent 500	Financial Criterion 120	Restoration time 0	Financial Criterion 1.000	Restoration time 0
	L1			
The certainty equivalent 500	Financial Criterion 120	Restoration time 40	Financial Criterion 1.000	Restoration time 40
	L1			
The certainty equivalent 500	Financial Criterion 120	Restoration time 80	Financial Criterion 1.000	Restoration time 80
	L1			
The certainty equivalent 500	Financial Criterion 120	Restoration time 120	Financial Criterion 1.000	Restoration time 40
	L1			
The certainty equivalent 40	Financial Criterion 120	Restoration time 120	Financial Criterion 120	Restoration time 0
	L1			
The certainty equivalent 40	Financial Criterion 200	Restoration time 120	Financial Criterion 200	Restoration time 0
	L1			
The certainty equivalent 40	Financial Criterion 400	Restoration time 120	Financial Criterion 400	Restoration time 0
	L1			
The certainty equivalent 40	Financial Criterion 800	Restoration time 120	Financial Criterion 800	Restoration time 0

	L1			
The certainty equivalent	Financial Criterion	Restoration time	Financial Criterion	Restoration time
40	1.000	120	1.000	0

References

Abdo, H., Kaouk, M., Flaus, J., & Masse, F. (2017). *A safety/security risk analysis approach of industrial control systems: A cyber bowtie - Combining new version of attack tree with bowtie analysis. Computers & security*.

Ali, A., Warren, D., & Mathiassen, L. (2017). Cloud-based business services innovation : A risk management model. *International Journal of Information Management, 37*(6), 639–649.

de Almeida, A. T., Cavalcante, C. A. V., Alencar, M. H., Ferreira, R. J. P., de Almeida-Filho, A. T., & Garcez, T. V. (2015). *Multicriteria and multiobjective models for risk, reliability and maintenance decision analysis*.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613–643.

Bang, Y., Lee, D., Bae, Y., & Ahn, J. (2012). Improving information security management : An analysis of ID – password usage and a new login vulnerability measure. *International Journal of Information Management, 32*(5), 409–418.

Bella, G., Giustolisi, R., & Riccobene, S. (2011). Enforcing privacy in e-commerce by balancing anonymity and trust. *Computers & Security, 30*(8), 705–718.

Bellman, R. E., & Zadeh, L. A. (1970). Decision-making in a fuzzy environment. *Management ScienceManagement Science, 17*(4), 141–164.

Belyaev, L. S. (1977). *A practical approach to choosing alternative solutions to complex optimization problems under uncertainty. RM-77-7, Vol. 1*. International Institute for Applied Systems Analysis.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51–61.

Bendovschi, A. (2015). Cyber-attacks – Trends, patterns and security countermeasures. Procedia economics and finance 28. *7th International Conference on Financial Criminology,* 24–31.

Bojanc, R., & Jerman-Blažič, B. (2008). Standard approach for quantification of the ICT security investment for cybercrime prevention. *Proceedings - The 2nd International Conference on the Digital Society,* (30), 7–14.

Bojanc, R., Jerman-Blažič, B., & Tekavčič, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. *Information Processing & Management, 48*(6), 1031–1052.

Borgonovo, E., Cillo, A., & Smith, C. L. (2018). On the relationship between safety and decision significance. *Risk Analysis*.

Bou-Harb, E., Debbabi, M., & Assi, C. (2013). A systematic approach for detecting and clustering distributed cyber scanning. *Computer Networks, 57*(18), 3826–3839.

Burmester, M., Magkos, E., & Chrissikopoulos, V. (2012). Modeling security in cyber-physical systems. *International Journal of Critical Infrastructure Protection, 5*(3–4), 118–126.

Butler, S. A. (2002). *Security attribute evaluation method: A cost-benefit approach. 24th International Conference on Software Engineering (ICSE' 02)*232–249.

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems, 50*(4), 651–661.

Cheng, C.-Y., Li, S.-F., Chu, S.-J., Yeh, C.-Y., & Simmons, R. J. (2013). Application of fault tree analysis to assess inventory risk: A practical case from aerospace manufacturing. *International Journal of Production Research, 51*(21), 6499–6514.

Chi, C.-F., Lin, S.-Z., & Dewi, R. S. (2014). Graphical fault tree analysis for fatal falls in the construction industry. *Accident; Analysis and Prevention, 72*, 359–369.

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.

Cowley, J. A., Greitzer, F. L., & Woods, B. (2015). Effect of network infrastructure factors on information system risk judgments. *Computers & Security, 52*, 142–158.

Dasgupta, D. (2007). Immuno-inspired autonomic system for cyber defense. *Information Security Technical Report, 12*(4), 235–241.

Doytchev, D. E., & Szwillus, G. (2009). Combining task analysis and fault tree analysis for accident and incident analysis: A case study from Bulgaria. *Accident; Analysis and Prevention, 41*(6), 1172–1179.

Ekel, P. Y., Martini, J. S. C., & Palhares, R. M. (2008). Multicriteria analysis in decision making under information uncertainty. *Applied Mathematics and Computation, 200*(2), 501–516.

https://erpscan.com/edocs/erp-cybersecurity-survey-2017 [Accessed on December, 23, 2017].

Ferdous, R., Khan, F., Veitch, B., & Amyotte, P. R. (2009). Methodology for computer aided fuzzy fault tree analysis. *Process Safety and Environmental Protection, 87*(4), 217–226.

Gai, K., Qiu, M., Xiong, Z., & Liu, M. (2018). Privacy-preserving multi-channel communication in Edge-of-Things. *Future Generation Computer Systems, 85*, 190–200.

Gai, K., Qiu, L., Chen, M., Zhao, H., & Qiu, M. (2017). SA-EAST : Security-Aware Efficient Data Transmission for ITS in Mobile Heterogeneous Cloud Computing. *ACM Transactions on Embedded Computing Systems, 16*(2), 1–22.

Gai, K., Qiu, M., Ming, Z., Zhao, H., & Qiu, L. (2017). Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. *IEEE Transaction on Smart Grid, 8*(5), 2431–2439.

Gan, B., & Brendlen, J. H. (1992). Nuclear power plant digital instrumentation and control modifications. *IEEE Conference on Nuclear Science Symposium and Medical Imaging, 2*, 25–31.

Ganesan, R., Gobi, M., & Vivekanandan, K. (2010). A Novel Digital Envelope Approach for A Secure E-Commerce Channel. *International Journal of Network Security, 11*(3), 121–127.

Gartner Group (2018). *Cyber security market - segmented by type of security, solution, services, deployment, industry, and region - growth, trends, and forecast.* Retrieved fromhttps://www.gartner.com/newsroom/id/3836563.

Goel, S., & Kiran, R. (2012). Vulnerability management for an enterprise resource planning system. *International Journal of Computer Applications, 53*(4), 19–22.

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. *Information Technology and People, 22*(2), 92–108.

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*(2), 99–122.

Gusmão, A. P. H., Silva, L. C., Silva, M. M., Poleto, T., & Costa, A. P. C. S. (2016). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management, 36*(1), 25–34.

Hauptmanns, U. (2002). Analytical propagation of uncertainties through fault trees. *Reliability Engineering & System Safety, 76*, 327–329.

Hauptmanns, U. (2004). Semi-quantitative fault tree analysis for process plant safety using frequency and probability ranges. *Journal of Loss Prevention in the Process Industries, 17*(5), 339–345.

Huang, Y. L., Cárdenas, A., Amin, S., Lin, Z. S., Tsai, H. Y., & Sastry, S. (2009). Understanding the physical and economic consequences of attacks on control systems. *International Journal of Critical Infrastructure Protection, 2*(3), 73–83.

Jaganathan, V., Cherurveettil, P., & Sivashanmugam, P. M. (2015). Using a prediction model to manage cyber security threats. *The Scientific World Journal, 2015*, 1–5.

Kawanaka, T., Matsumaru, M., & Rokugawa, S. (2014). Software measure in cyber-attacks on production control system. *Computers & Industrial Engineering, 76*, 378–386.

Keeney, R. L., & Raiffa, H. (1976). *Decisions with multiple objectives – Preferences and value tradeoffs.* John Wiley & sons.

Kim, D. W., Yan, P., & Zhang, J. (2015). Detecting fake anti-virus software distribution webpages. *Computers & Security, 49*, 95–106.

Lo, C. C., & Chen, W. J. (2012). A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems With Applications, 39*(1), 247–257.

Lokhande, P. S., & Meshram, B. B. (2013). E-commerce spplications: vulnerabilities, attacks and countermeasures. *International Journal of Advanced Research in Computer Engineering & Technology, 2*(2).

Lopez-nicolas, C., & Jose, F. (2008). Customer Knowledge Management and E-commerce : The role of customer perceived risk. *International Journal of Information Management, 28*, 102–113.

Mahmood, Y. A., Ahmadi, A., Verma, A. K., Srividya, A., & Kumar, U. (2013). Fuzzy fault tree analysis: A review of concept and application. *International Journal of System Assurance Engineering and Management, 4*(1), 19–32.

Marhavilas, P. K., Koulouriotis, D., & Gemeni, V. (2011). Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000-2009. *Journal of Loss Prevention in the Process Industries, 24*(5), 477–523.

Medeiros, C. P., Alencar, M. H., & De Almeida, A. T. (2017). Multidimensional risk evaluation of natural gas pipelines based on a multicriteria decision mo del using visualization tools and statistical tests for global sensitivity analysis. *Reliability Engineering & System Safety, 165*(April 2016), 268–276.

Mik, E. (2012). Mistaken identity, identity theft and problems of remote authentication in e-commerce. *Computer Law & Security Report, 28*(4), 396–402.

Nabi, F. (2011). Designing a framework method for secure business application logic integrity in e-commerce systems. *International Journal of Network Security, 12*(1), 29–41.

Nunez, M. (2012). Cyber-attacks on ERP systems. *Datenschutz Und Datensicherheit - DuD, 36*(9), 653–656.

Offutt, J. (2002). Quality attributes of Web software applications. *IEEE Software, 19*(2), 25–32.

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). *Methods and applications. Fuzzy multicriteria decision-making: Models*. JohnWiley Sons, Ed.).

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.

Rahman, A. F., Varuttamaseni, A., Kintner-Meyer, M., & Lee, J. C. (2013). Application of fault tree analysis for customer reliability assessment of a distribution power system. *Reliability Engineering & System Safety, 111*, 76–85.

Rahmani, A., Amine, A., Hamou, R. M., Boudia, M. A., & Bouarara, H. A. (2016). De-identification of unstructured textual data using artificial immune system for privacy

preserving. *International Journal of Decision Support System Technology, 8*(4), 34–49.
Raiffa, H. (1968). *Decision analysis.* Wesley, Reading.
Ralston, P. A. S., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions, 46*, 583–594.
Ratten, V. (2016). Continuance use intention of cloud computing : Innovativeness and creativity perspectives. *Journal of Business Research, 69*(5), 1737–1740.
Rejeb, R., Leeson, M. S., & Green, R. J. (2006). *Multiple attack localization and identification in all-optical networks, 3*(1), 41–49.
Rice, E. B., & AlMajali, A. (2014). Mitigating the risk of cyber attack on smart grid systems. *Procedia Computer Science, 28*(Cser), 575–582.
Ruijters, E., & Stoelinga, M. (2015). Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Computer Science Review, 15–16*, 29–62.
Shaikh, R. A., Adi, K., & Logrippo, L. (2012). Dynamic risk-based decision methods for access control systems. *Computers & Security, 31*(4), 447–464.
Shameli-Sendi, A., Cheriet, M., & Hamou-Lhadj, A. (2014). Taxonomy of intrusion risk assessment and response system. *Computers & Security, 45*, 1–16.
Shin, J., Son, H., Khalil ur, R., & Heo, G. (2015). Development of a cyber security risk model using Bayesian networks. *Reliability Engineering & System Safety, 134*, 208–217.
Silva, M. M., de Gusmão, A. P. H., Poleto, T., Silva, L. C. E., & 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*(6), 733–740.
Silva, M. M., Poleto, T., Camara, E. S. L., Henriques, D. G. A. P., & Cabral, S. C. A. P. A. (2016). Grey theory based approach to big data risk management using FMEA. *Mathematical Problems in Engineering, 2016*, 1–15.
Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*, 215–225.
Trompeter, C. M., & Eloff, J. H. P. (2001). A framework for the implementation of socio-ethical controls in information security. *Computers & Security, 20*(5), 384–391.
Venters, W., & Whitley, E. A. (2012). A critical review of cloud computing: Researching desires and realities. *Journal of Information Technology, 27*(3), 179–197.
Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102.
Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). DDoS attack protection in the era of cloud computing and Software-Defined Networking. *Computer Networks, 81*, 308–319.
Whitley, E. A. (2009). Informational privacy, consent and the “control” of personal data. *Information Security Technical Report, 14*(3), 154–159.
Yang, Z., & Lui, J. C. S. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation, 74*, 1–17.
Yuhua, D., & Datao, Y. (2005). Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis. *Journal of Loss Prevention in the Process Industries, 18*(2), 83–88.
Zadeh, L. A. (1965). Fuzzy sets. *Information and Control, 8*(3), 338–353.
Zadeh, L. B. (1975). The concept of a linguistic variable and its application to approximate reasoning—II. *Information Sciences, 8*(4), 301–357.
Zhang, Z., Ho, P. H., & He, L. (2009). Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach. *Computers & Security, 28*(7), 605–614.