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
0268-4012/

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