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