Measurement 51 (2014) 214–223

Contents lists available at ScienceDirect

Measurement

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

A fuzzy model for assessment of organization vulnerability

Aleksandar Aleksić *, Miladin Stefanović, Danijela Tadić, Slavko Arsovski

Faculty of Engineering, University of Kragujevac, Serbia

ARTICLE INFO

Article history:
Received 26 July 2013
Received in revised form 30 December 2013
Accepted 4 February 2014
Available online 11 February 2014

Keywords:
Organization vulnerability
Business processes
Fuzzy sets

ABSTRACT

There are many factors that can make an organization and its business unsafe and endanger its sustainable development. Exposure of an organization to existing risks may vary and it can be studied from different perspectives, but undoubtedly increased vulnerability of an organization can lead to disaster. This paper investigates the general vulnerability of an organization and proposes a model for its assessment. The process approach has been employed to define the model of an organization, as well as the fuzzy approach for mathematical modeling of uncertainties. An assessed value of organization vulnerability is obtained by using linguistic expressions which are close to human thinking. The mathematical model of organization vulnerability is solved through fuzzy sets with input data defined by a management team. The model for vulnerability assessment is verified through an illustrative example. The obtained results represent an input for future research which should include a good benchmark base for the tested organizations and their continuous improvement.

1. Introduction

The concept of vulnerability covers several connotations which are often directed to the sensitivity (susceptibility) of a system to harm [1]. In information science, vulnerability represents any known weakness in a system that could potentially be exploited by malicious software or hackers [2]. If an organization is a part of the supply chain, the situation is even more complex. Supply chain vulnerability [3] may be defined as an exposure to serious disturbance. Although there are different vulnerability assessment tools, software and procedures that cover different factors (informational, etc.), there is an obvious absence of a similar approach for organization factors which makes it an important issue. Besides this, there is no generally accepted definition of the quantification of vulnerability in the field of organizations and management. Having in mind the fact that vulnerability has a close connection with risk assessment, it makes the assessment of organization vulnerability even more complex.

A few decades ago, risk was quantified as a measure of the probability and severity of adverse effects [4] which was updated to the level where risk is seen as a triplet of scenario, likelihood, and consequence [5]. According to ISO standards, vulnerability represents the intrinsic properties of something that creates susceptibility to a source of risk that can lead to a consequence (ISO/IEC Guide 73). In the field of ecology, which has treated the vulnerability of ecosystems for many years, the generally accepted definition of vulnerability [6,7] is presented as a multidimensional concept that consists of exposure, sensitivity and adaptive capacity. An adequate point of view, when an organization is the focus, is that vulnerability can be presented as a weakness in the organization that potentially opens the door for threats and risks [8]. Risks may lead to incidents if they are not treated properly and vulnerability highlights the notion of susceptibility to a risk scenario [9].

This paper proposes a model which implies that organization vulnerability may be quantified in the scope of

* Corresponding author. Tel.: +381 642708188.
E-mail addresses: aaleksic@kg.ac.rs (A. Aleksić), miladin@kg.ac.rs (M. Stefanović), galovic@kg.ac.rs (D. Tadić), cqm@kg.ac.rs (S. Arsovski).

http://dx.doi.org/10.1016/j.measurement.2014.02.003
0263-2241/

exposure, sensitivity and adaptive capacity aspects. The goal is to present a model for assessment of organization vulnerability that may arise from internal sources and in this manner the model is tested on 32 small and medium enterprises (SMEs) of the production industry.

The estimation of vulnerability indicators' (VI) weights and uncertain parameter values cannot be performed by using precise numbers [10]. It seems a more realistic approach to use linguistic expressions instead of numerical values. In this paper, modeling of these linguistic variables is performed by using fuzzy sets. The fuzzy sets theory [11,12] provides an overview of the larger framework of issues that deal with two distinct forms of uncertainties-vagueness and ambiguity. The vagueness is associated with the difficulty of precise distinctions in the world and ambiguity is associated with situations in which the choice between two or more alternatives is left unspecified [11]. The fuzzy sets theory and its application in various management problems are described in [13]. By assessing vulnerability, organizations get a chance to successfully manage their own vulnerability and also improve their business practice and resilience.

2. A literature review

A significant number of scholars have explored vulnerability in different scientific areas such as information systems [14], supply chains [15], and monitoring systems [16], but only a few of them deal with business organization issues.

Sustainability science [17] has emerged as a paradigm for addressing human–environment issues from different scientific fields. It may be said that sustainability science maintains very significant interests in issues of vulnerability and resilience. Complex and changeable conditions have implied the need for the vulnerability communities [1] to treat the full dimensions of coupled human–environment systems. In order to do so, three main challenges need to be analyzed: measuring vulnerability, treating perceptions of risk, and addressing governance. The conceptualization of risk may be analyzed through the ideas of Kaplan [5] concerning the risk triplet which includes a scenario, the likelihood of the manifestation of that scenario, and the consequences of events within that scenario. Other scholars [18] argue that risk is an inherent property of an engineered system and define risk as the measure of probability and severity of consequences. Understanding the nature of risk and reducing its level within an organization are the major tasks in risk assessment. In order to do it in a proper way, the emphasis is often on assessing the expected harm from the occurring event. If an undesired event happens, vulnerability [6] depends not only on exposure to an event, but also on the degree to which normal system reliability is compromised during harmful event.

The connection between vulnerability and resilience has been analyzed in various fields. In a wider context, the concept of vulnerability is often treated as being subject to a range of effects that include exposure to disruptions, external stresses, sensitivity to perturbation and the system's capacity for response [19]. If this representation is in focus, resilience is considered a subset of a systems' capacity for response. Through this point of view, vulnerability [19] refers to the capacity to preserve the structure of a system, while resilience refers to the capacity to recover from disturbances within the concept of sustainability. On the other hand, engineered system analysis implies that resilience capacities [20] are seen as a function of adaptive capacity, absorptive capacity and restorative capacity. Organizational resilience [20] seizes the capabilities of an organization to recognize threats, evaluate the current risk analysis models in order to be competitive, self-regulate, prepare for future protection efforts, and include the ability to reduce potential risks as candidates of factors influencing the system's resilience. In this manner, the relationship between resilience and vulnerability is interconnected, so vulnerability assessment dictates the appropriate resilience action to be taken in order to reinforce a system's resistance to shock events, reorganize resources and make structural adjustments to accommodate likely changes or enhance preparedness for recovery operations.

From the perspective of a corporate value net [21], vulnerability is emphasizing the fact that different originated factors (including outside entities, for example suppliers) lead to incidents which cause vulnerability of the whole net. The main issues in the field of assessment of organization vulnerability are methodology, categorization and classification of the organization vulnerability [21]. Categorization and classification of enterprise vulnerability is a very complex issue and there are not many papers dealing with it. Common factors [22] that can cause an SME to fail are insufficient forward planning, issues with cash flow, the inability to capture and manage innovation, lack of investment, lack of business experience, and little external support. These organization inadequacies can downsize organizational ability to effectively respond to the disruptions which make them significant sources of vulnerability. Planning strategies, participation in exercises, capability and capacity of internal resources, capability and capacity of external resources and organizational connectivity may be also seen as a categorized group of sources of organization vulnerability [23]. The lack of papers with clarification of the mentioned issues can be explained by the fact that classification is a continuous activity, since vulnerability may arise from new emerged risks such as new technology risks, economic and political risks or globalization itself which has significantly increased clients' expectations. If SMEs are the focus, overcoming vulnerability is determined by an organization's environment and by the SMEs' own properties. SMEs form a very significant part of the EU economy – accounting for 99.8% of non-financial enterprises in 2012 [24]. In employment terms, SMEs provided an estimated 67.4% of jobs in the non-financial business economy in 2012. It may be noticed that SMEs have a limited approach to resources [25] which makes them open to the external environment. It makes them significantly vulnerable so they have to define an appropriate strategy and assure the resources for dealing with potential risks and scenarios that may arise from them. Defining an appropriate business strategy, aligned with enhancing mechanisms for coping with vulnerability, may have an influence on an organization's sustainability and have an