Cybersecurity Risks in Romanian Companies

Anca Gabriela Petrescu
Valahia University, Romania

Marius Petrescu
Valahia University, Romania

Ioana Panagore
Valahia University, Romania

Florentina Raluca Bîlcan
Valahia University, Romania

INTRODUCTION

Risk management process is proving to be an essential factor for the development and stability of an organization, it is the basis for developing a sustainable strategy for achieving organizational objectives and the basis for planning and decision making (Singh & Fhom, 2017).

At the same time, sophisticated attacks are expected directed to the staff users of the communication and information systems, such as social engineering attacks, correlation between office, ISP, and home computers or mobile device attacks. State-sponsored cyber terrorism is of great concern for state authorities, as this new form of terrorism is cheap and ready available to practically everyone, on each side of the world and it can lead to major disruptions in modern societies. The uncertainty may take the form of either threats or opportunities. Thereby, each manager must handle threats, because otherwise the organization's objectives cannot be met and capitalize the opportunities to the benefit of the organization, proving efficiency (McQuade, 2006; He, Chen, Chan, & Bu, 2012).

Among the most important factors of disruptive impact on the activities of an organization, risk factors are, by far the leading place.

Risk, as defined in the western socio-economic and military environments, can occur anywhere: within the organization, structure, and decision-making process, the relationship with the external environment, the management and policies of the organization (Ruževičius & Gedminaitė, 2007).

In order to identify, analyze and organize organizational risk assessment activities to reiterate the importance of the organizational concepts of systems theory perspective (Hjortdal, 2011; Chen, Ge, & Xie, 2015).

Risk treatment is the second important step in risk management organizational stage where management organization has the key role in the adoption of the most appropriate decision in terms of the balance between the need to fulfill the performance indicators proposed and costs (Hadžiosmanović, Bolzoni, & Hartel, 2012).

Stage security risk treatment is based entirely on the results of the risk analysis phase, the risks have been identified and ranked in terms of the impact that their implementation can have on the organiza-

DOI: 10.4018/978-1-7998-3473-1.ch087

tion's mission. This is why, security mechanisms have to be properly designed and commensurate with the specific threats for the specific types of information (Tropina & Callanan, 2015).

Choosing an effective strategy development organization should consider the risks and vulnerabilities exposed to treatment solutions adapted to the needs of each organization's risk and reduce costs, both short and long term. Meanwhile, the adoption of certain measures that contribute to risk management is conditioned by the nature of the organization and the costs incurred for these measures.

As such, also in Romanian companies, concern continues to diminish the effect of unwanted influence involves a compulsory, dedication of resources which, if prolonged neglect can radically affect the overall level of resources of an organization and therefore, the quality of its task.

In order to achieve this aim, the chapter analyzes a number of problems of research. Firstly, this study explores the Romanian organizations' attitude towards information technology security. Secondly, the protection of this infrastructure represents a major concern of authorities all around the world. Information security has become a top of mind issue for the public, media and government. And last but not least, it investigates the necessity to develop a structured process of information security risk within the organization. It must be borne in mind that, regardless of the type of organization, the field of activity or form of organization, there is uncertainty both in organization and in the environment in which it operates. Given that uncertainty is a fact of life, then the uncertainty response should become a permanent managerial concern.

However, collective efforts are necessary, at both national authorities' level and managers of public and private organizations in order to ensure a safe and trusted cyber space. The awareness of potential threats and vulnerabilities is thus vital, as well as preoccupation towards cooperation in countering them by well-established rules and mechanisms created at national and organizational level.

BACKGROUND

Information technology security threats are most often defined as being "those circumstances or events that constitute potential danger to the normal state of a communication and information system, in which the confidentiality, integrity and availability of information, resources and services are ensured" (Ministry of Communications and Information Society, 2011).

Organizations have to expand and deepen their current information security risk frameworks to address these key threats (Andress, 2003; Hong, Kim, & Cho, 2010; Mittelman, 2011). This process implies a more profound understanding of the risks associated with each threat, and a better capacity of tailoring the security framework to align with the organization's identified risks, regulatory requirements and perhaps most important – the increasing dependencies on information technology (Willems, 2011; Stepchenko & Voronova, 2015; Malatras, Geneiatakis, & Vakalis, 2016; Lin, Lin, & Pei, 2017). In addition, as we pointed out previously, management vision must change radically, from a passive or reactive management style to a proactive style, ready at any moment to face the challenges of achieving the objectives of the organization (Tiago, Manoj, & Espadanal, 2014; Agrawal & Tapaswi, 2017).

Contrariwise, the allocation of material resources, human and too big for the risk management process can lead to non-completion of projects or even not starting them. This is where the organization's approach is to stop the progression of the project until the risk management process.

Another important aspect to note is that of a special form of risk, namely the risk of managerial behavior in the face of organizational changes: managers hoped that the change will solve the fundamental problems of the organization; there is insufficient time for planning the implementation of change;