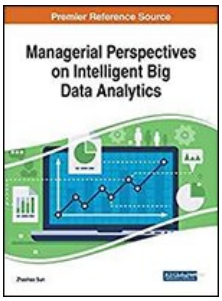

Managerial Perspectives on Intelligent Big Data Analytics

by Zhaohao Sun

Chapter 12: Proactive Information Security Strategy for a Secure Business Environment

Ionica Oncioiu,
Titu Maiorescu University,
Romania

Anca Gabriela Petrescu,
Valahia University,
Romania

Diana Andreea Mândricel,
Titu Maiorescu University,
Romania

Ana Maria Ifrim,
Titu Maiorescu University,
Romania

ABSTRACT

Taking into consideration the competitive market, the protection of information infrastructure for a company means competitive advantage. The protected information along with risk analysis are the underlying decision making in the company: either development, positioning on new markets, expansion on emerging markets, exit markets, or acquisitions. At the same time, the protection of information together with operational business intelligence systems are the keys for the decisions of CEOs. Implementing appropriate security measures to counter threats such as attacks can be blocked, or its effects can be mitigated. In this context, this chapter intends to be a thorough reflection on the awareness of potential threats and vulnerabilities, as well as a preoccupation towards cooperation in countering them with well-established rules and mechanisms created at a national and organizational level. The results are relevant to better understand how the actors involved in information and communication technologies could develop new models of information systems and risk management strategies.

INTRODUCTION

Today it is considered that information is secured (protected) by ensuring a balanced availability, confidentiality, integrity, authenticity and non-repudiation of them, so far as is necessary entity created it or who uses it (Baskerville, 2010; Martinez-Caro et al., 2018; Tropina & Callanan, 2015).

Risks can impact organizations in the short, medium or long (Andress, 2003; Da Veiga, 2016; Stepchenko & Voronova, 2015). These risks are operational, tactical and respectively strategically (Gandotra, Singhal & Bedi, 2012). Strategy sets the long-term objectives of the organization; the term typically is approximately 3-5 years (Hong, Kim & Cho, 2010). Tactics is how organizations intend to achieve change (Hiller & Russel, 2013; Tutton, 2010).

Therefore, the risks generally associated tactical projects, mergers, acquisitions, product development, and so on (Bojanc & Jerman-Blažic, 2012). Operations are routine activities of the organization, having, in turn, associated operational risks (Gkioulos et al., 2017). Implementing appropriate security measures to counter threats such as attacks can be blocked or its effects can be mitigated (McQuade, 2006).

Prevention means that the attack will be prevented (Baskerville, Spagnoletti & Kim, 2014; Renaud et al., 2018). Typically, prevention involves implementation of mechanisms that users not be able to counteract and are implemented correctly, unaltered, so the attacker cannot alter those (Singer & Friedman, 2014). Prevention mechanisms are cumbersome and often interfere with the use of the system to the point that, sometimes hamper normal use thereof (Winkler, 2010). But some simple preventive mechanisms with as passwords (which are designed to prevent unauthorized users from using the system) have become widely accepted plan (Banker, Chang, & Kao, 2010; Sveen, Torres & Sarriegi, 2009). Once implemented, the resources protected by mechanisms not are monitored to identify any security issues, at least in theory (Ruževičius & Gedminaitė, 2007).

At the same time, this process requires a division of responsibilities clearly delineated within the organization, creating a culture of risk prevention at all levels of the organization (Landoll, 2010).

Organizational culture has also impact on the level of risk tolerance, reflected in opening the organization to adopt cutting-edge

high technology (Da Veiga, 2016). For example, it is expected to open such organizations that are engaged in research and development (Ahmad, Maynard & Park, 2014; Flowerday & Tuyikeze, 2016). These organizations are prepared to adopt new technologies and, therefore, more likely to see these technologies in terms of the potential benefits against the potential disadvantages (Karim, 2007).

In contrast, organizations that are involved in activities related to information security can be more conservative, their appetite for new technologies being booked, especially if the products are developed less known entities or unreliable (Clarke-Sather et al., 2011). These types of organizations are often reluctant to adopt new technologies and are more inclined to look at new products rather in terms of the damage it can cause. Another example is the cases of organizations customize their software and services or develop applications or services solely for them (Shamala, Ahmad, Zolait & Sahib, 2015). Other organizations may be reluctant to use software or services developed by other entities (Dor & Elovici, 2016). This reluctance may result in other risks. On the other hand, there are organizations seeking maximize the benefits of modern technologies such as cloud computing, service oriented architectures, calling for it to external entities (Mohammed, Ibrahim, & Ithnin, 2016; Renwick & Martin, 2017). Given that the organization typically has no control over how external entity performing the analysis and handling of information security risks, additional risks may concerns the organization (Peltier, 2010).

Therefore, recognition and acceptance of the significant influence that organizational culture has on managerial decisions on the approach to information security risk is a key factor in enabling effective risk management process (Chai, Kim &. Raoc, 2011; Bojanc, Jerman-Blaic & Tekavcic, 2012). For all that, understanding the impact that organizational culture has on treatment programs for risk analysis and information security is important given the fact that these processes may involve major changes throughout the organization these changes must be managed effectively and understanding culture embedded in an organization plays an important role in bringing about the changes that affect the entire organization (Flores, Antonsen & Ekstedt, 2014). Implement processes analysis, treatment and monitoring of information security risks requires a major change throughout the organization (Soomro, Hussain Shah & Ahmed, 2016).

This change involves the alignment of personnel, processes and organizational culture with the new objectives of the organization, strategy and approach to risk communication mechanisms for risk-related information between the entities concerned (Anderson & Choobineh, 2008). To effectively manage these changes, organizations can use the considerations of organizational culture as a key component in their strategic thinking and decision-making processes such as strategy development approach for risk (Baskerville, 2010). If the manager is aware of the importance of organizational culture has increased opportunities to achieve the organization's strategic objectives through proper risk management (Eloff & Von Solms, 2000). When several organizations are working together to fulfill common objectives might appear different approaches that can lead to different risk management strategies, which would create new risks and determine the tendency to accept more readily the risks (Fenz, 2014).

Besides the fact that the staff is directly responsible for the risk analysis takes on a heightened awareness of the risks to the security of information managed by the organization, all staff of the organization is accountable about threats and vulnerabilities resulting from the use communications and information systems processing, storing and transmitting information (Chen, Ge & Xie, 2015). Resuming regular risk analysis process security is a good opportunity to involve all staff who manages sensitive information. In this way, the staff will be aware of the importance and sensitivity of the actions we take and will be less reluctant to comply with the security requirements sometimes constitutes barriers to timeliness (Hausmann et al., 2014).

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 (Gandino, Celozzi & Rebaudengo, 2017).

However, the protection of information infrastructure implies that no access, modification, deletion or otherwise denial of access to data or network resources or services is performed by unauthorized persons or entities (Chou, Seng-Cho & Tzeng, 2006). Cyber security incidents recorded in recent years are likely to demonstrate that while policies and technology are critical components of any system of data protection, they alone can not provide effective protection of information (Ahmad, Hadgkiss & Ruighaver, 2012; Yar, 2006). Risk awareness information security is the first line of defense personnel is true perimeter security computer networks, and their behavior is critical to the protection of information handled by these systems (Choi et al., 2014).

In this context, this chapter intends to be a thorough reflection on the awareness of potential threats and vulnerabilities, as well as a preoccupation towards cooperation in countering them with well-established rules and mechanisms created at a national and organizational level. This chapter is also relevant to better understand how the actors involved in information and communication technologies could develop new models of information systems and risk management strategies.

This chapter is structured as follows: the first section introduces the dynamics of the information technology security threat; in the second section, research methodology is discussed; in the third section, the results of the study and statistics analysis are shown; in the last section, the conclusions and limitations are covered.

BACKGROUND

Detection is particularly useful where an attack cannot be prevented, but can also indicate the effectiveness of preventive mechanisms (Malatras, Geneiatakis & Vakalis, 2016). Detection mechanisms accepts that an attack may occur; the goal is to determine if an attack is about to occur or has occurred, and to report this procedure. However, the attack can be monitored to collect data on the nature, severity, and results (Arukonda & Sinha, 2015). Typical detection mechanisms monitor various aspects of the system, looking for action and information indicating an attack (Krombholz et al., 2015). An example of such mechanisms is providing an alarm when the user enters the wrong password more than three times. The procedure for obtaining access to the system can be continued, but history records system audit report an unusually high number of erroneous input passwords (Collins & McCombie, 2012). Detection mechanisms do not prevent compromise of parts of the system, which is a serious drawback (Lin, Lin & Pei, 2017). Protected resources detection mechanisms must be monitored continuously or periodically to identify any security issues (Wang & Hu, 2014).

This is why, security mechanisms have to be properly designed and commensurate with the specific threats for the specific types of information (Agrawal & Tapaswi, 2017). Organizations have to expand and deepen their current information security risk frameworks to address these key threats (Smith, 2005). 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.

Over the time, a large number of methodologies for identifying information security risks were proposed and adopted and simplified approach to different methodologies has led to their classification in quantitative and qualitative, especially in terms of metrics used to quantify risk (Friedberg et al., 2016; Kesan & Hayes, 2012).

A qualitative method using words or descriptive scales and the form a hierarchical structure that alternates between "rarely" and "almost certainly" (Singh & Fhom, 2017). Such a method is intended to prioritize the likelihood and the consequences of which can range from insignificant to moderate to severe.

Quantitative analysis is based criteria to establish the possibility of producing an event and its consequences. The possibility of the occurrence probability is expressed as, not in the form of frequency, thereby ensuring that the risks were compared to a similar base (Liaudanskienel, Ustinovicius & Bogdanovicius, 2009). When we speak of the possibility of occurrence of similar events small possibility of this happening can be treated as a single event.

Method OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation - Evaluation Threats, Assets and Organizational Vulnerability Critical) based on the definition of complex, systematic and contextual essential components of an information system, using a three-stage organization to determine the risks associated with privacy, integrity and availability of information assets critical to the proper performance of the organization considered (Karim, 2007). Measuring losses or impact severity level of risk can be both qualitative and quantitative, depending on available resources collective organizational and risk management information security system.Determination of information security risks is generally difficult because information about threats and asset values are generally more difficult to obtain and quantify and risk factors are constantly changing (Tu et al., 2018). OCTAVE risk analysis based on the methodology involves the use of risk scenarios associated with each critical asset of the organization (Gaidelys & Valodkiene, 2011).

Another mixed method (qualitative and quantitative risk assessment, known as VaR (Value Risk) based on the identification of the most severe effects of the production risks could have on the objectives of the organization, in a horizon type and a given confidence interval and aims to achieve optimal balance between the risks assumed and necessary expenses of minimizing them. The four steps proposed by the VAR methodology includes identifying threats, estimating the probability of these threats, the calculation VAR (value risk) and determining controls to prevent or minimize the effects of identified risks (He et al., 2012).

As such, concern continues to diminish the effect of unwanted influence involving 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 (Mittelman, 2011).

Among the most important factors of disruptive impact on the activities of an organization, risk factors are by far the most significant (Yang, Wu & Wang, 2014). 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 (Campbell, Gordon, Loeb & Zhou, 2003; Sá-Soares, Soares & Arnaud, 2014).

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 (Broadbent & Schaffner, 2016). 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 (Hjortdal, 2011). To identify, analyze, and organize organizational risk

assessment activities to reiterate the importance of the organizational concepts of systems theory perspective (Xu et al., 2018). 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 organization's mission (Okamoto & Takashima, 2015). This is why security mechanisms must be properly designed and commensurate with the specific threats for the specific types of information (Tropina & Callanan, 2015).

The proposed research framework consists of nine independent constructs (past crimes and threats, facility characteristics (static and dynamic), current security measures, existing vulnerabilities, reducing consequences, procedures and training, security personnel, virtual infrastructure security, corporate security policy), one dependent variable (security management framework) within two different characteristics (technological and organisational) and build research hypotheses.

Current security measures is defined as the degree in which a new technology or innovation is consistent with current technologies and addresses the needs of the company (Willems, 2011). It is especially important for companies to make sure that all changes in their infrastructure, services and / or technologies are compatible with their existing vulnerabilities (Hoang & Ruckes, 2017). Therefore, the following hypotheses is defined for this study:

- **Hypothesis One $_{a}$:** Perceived advantages of adopting current security measures have a positive effect on the information security strategy of companies
- **Hypothesis One $_{b}$:** Review of past crimes and threats with existing company technologies has a positive effect on the information security strategy of companies
- **Hypothesis One $_{c}$:** Observability of existing vulnerabilities has a positive effect on the information security strategy of companies
- Virtual infrastructure security is the level at which the existence and availability of technology are visible to others (Tiago, Manoj & Espadanal, 2014). Empirical data shows a direct relationship between the virtual infrastructure security and their effects on companies' information security strategy. Accordingly, the following hypothesis is proposed in this research:
- **Hypothesis One $_{d}$:** Availability of virtual infrastructure security has a positive effect on the information security strategy of companies

Procedures and training combine the necessary people, space and business processes which support the formation and development of companies (Fischbacher-Smith, 2016). One of the major purposes of a security personnel programme is stimulating employees by creating an environment for supporting the development and survival of new technologies (Khan et al., 2016). In the same manner, the availability of corporate security policy may affect the information security strategy of companies as hypotheses in the following:

- **Hypothesis Two $_{a}$:** Availability of procedures and training has a positive effect on the information security strategy of companies
- **Hypothesis Two $_{b}$:** Availability of security personnel has a positive effect on the information security strategy of companies
- **Hypothesis Two $_{c}$:** Availability of reducing consequences has a positive effect on the information security strategy of companies
- **Hypothesis Two $_{d}$:** Availability of the facility characteristics (static and dynamic) has a positive effect on the information security strategy of companies
- **Hypothesis Two $_{e}$:** Availability of corporate security policy has a positive effect on the information security strategy of companies

RESEARCH METHODOLOGY

In order to obtain an image of the Romanian organizations' attitude towards information security strategy for a secure business environment, the authors performed a detailed survey using questionnaires. The major objective of this research is to identify those factors affecting the information security strategy of companies. More specifically, we are trying to detect if there is any

significant relationship between two sets of characteristics (technologica and organisational) and the information security strategy of businesses. The findings suggest positive effects of technological and organisational characteristics on the information security strategy of businesses.

The survey was performed during the first trimester of 2018. The questionnaires were forwarded to 385 Romanian companies were randomly selected and contacted in two rounds.

The responding were representing different fields of activity: industry, commerce, transportation, finance, education, ICT, constructions, public administration, and non-governmental organizations. Considering the diversity of fields of activity and bearing in mind that the questionnaires were voluntarily completed, we estimate the findings of this research activity reflect in a good manner the attitude of the Romanian companies towards information security strategy.

In this study, a seven-point Likert-type scale ranging from ('1 = strongly disagree' to '7 = strongly agree') were utilized for measuring responses. In addition, ordinal or nominal scales were used to gain a more accurate response in a few questions. Normal distribution of variables is the most fundamental assumption in any multivariate analysis including SEM (Kaplan, 2000). Skewness and Kurtosis values were used to reflect a normal distribution of all variables in this research. Table 1 shows, for each research construct, its alpha value, mean, standard deviation and normality.

Responses were collected using questionnaires processed using the Scientific Package for Social Sciences (SPSS) 17.0 and the making of the database structure was achieved by defining variables in Variable View. It is also important to note that all completed questionnaires were checked in terms of background completeness and usefulness of data and using the statistical program previously mentioned, data analysis was materialized through frequency tables and histograms for each item, and the centralization of all items. In this research, Principal Components Analysis (PCA) and the orthogonal method with Varimax rotation along with Exploratory Factor Analysis (EFA) were employed through Statistical Package for Social Sciences (SPSS) version 21. The results of Bartlett's test (Table 2) were significant with χ^2= 10279.6 and p<0.05. Therefore, the factor analysis technique seems to be an appropriate analysis method for this study. The Kaiser-Meyer-Olkin (KMO) value for this research was 0.927 which is very close to 1 which indicates the appropriateness of factor analysis technique for this study. Following this, the path analysis process was used to investigate direct and indirect structural relationships between research variables.

Since all variables had a factor loading of 0.6 or better they were suitable for CFA testing. Evaluation of goodness-of-fit indices and other parameters estimates of the hypothesized structural model suggested that ten out of thirteen hypothesised paths were significant, hence supported. As a general rule, all variables with less than 0.05 factor loading should be removed. Also, as shown in Table 3, AVE estimates of each construct of this research is larger than Squared Inter-construct Correlation (SIC) estimate and so supports discriminate validity for each construct of this study.

Table 1: Variable reliabilities and descriptive statistics

	Alpha	Mean	Std Dev	Skewness	Kurtosis
Past Crimes and Threats (PCT)	0.850	5.33	1.372	-.290	-.838
Facility Characteristics (static and dynamic) (FC)	0.904	5.17	1.485	-.008	-1.134
Current Security Measures (CSM)	0.871	5.18	1.397	.133	-.905
Existing Vulnerabilities (EV)	0.921	5.18	1.484	-.104	-1.035
Reducing Consequences (RC)	0.911	5.19	1.392	-.220	-1.101
Procedures and Training (PT)	0.839	5.22	1.372	-.207	-.756
Security Personnel (SP)	0.897	5.26	1.367	-.093	-.738
Virtual Infrastructure Security (VIS)	0.797	5.21	1.407	-.604	.133
Security Management Framework (SMF)	0.931	5.16	1.408	-.111	-1.290
Corporate Security Policy (CSP)	0.876	4.48	1.538	-.465	-.474

Table 2: KMO statistics and Bartlett's Test of Sphericity

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.927
Bartlett's Test of Sphericity	Approx. Chi-Square	10279.647
	Df	1485
	Sig.	.000

A parameter estimate is significant at the.05 level when its Critical Ratio (CR) is more than 1.96. Moreover, the structural model fit was used to quantify each and every hypothesis as shown in Table 4.

According with the results it can be concluded that perceived advantage of adopting current security measures (β = 0.273) is the most influential construct on the information security strategy of companies followed by the facility characteristics (static and dynamic) (β = 0.203), past crimes and threats (β = 0.198), corporate security policy (β = 0.189), security personnel (β =

0.149), reducing consequences (β = 0.140), existing vulnerabilities (β = 0.123), and virtual infrastructure security (β= 0.229).

Moreover, the hypotheses analysis summary of this research is represent in Table 5.

SOLUTIONS AND RECOMMENDATIONS

Modern society is constantly subjected to during its development, the action of a multitude of disturbing factors (Xu et al., 2018). The influence can not be neglected because, over time, may increase up to the actual situation where the obstacles are sometimes insurmountable (Charki, Josserand & Boukef, 2017). As such, 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. Among the most important factors of disruptive impact on the activities of an organization, risk factors are, by far the leading place.

Table 3: Inter-construct correlations

	PCT	FC	CSM	EV	RC	PT	SP	VIS	SMF	CSP
Past Crimes and Threats (PCT)	1.000									
Facility Characteristics (static and dynamic) (FC)	.567	1.000								
Current Security Measures (CSM)	.556	.565	1.000							
Existing Vulnerabilities (EV)	.629	.552	.501	1.000						
Reducing Consequences (RC)	.599	.504	.553	.563	1.000					
Procedures and Training (PT)	.575	.519	.534	.548	.564	1.000				
Security Personnel (SP)	.529	.392	.320	.335	.279	.396	1.000			
Virtual Infrastructure Security (VIS)	.656	.624	.634	.609	.643	.626	.414	1.000		
Security Management Framework (SMF)	.637	.503	.449	.579	.550	.644	.391	.641	1.000	
Corporate Security Policy (CSP)	.531	.479	.416	.471	.410	.403	.402	.489	.488	1.000
** Correlation is significant at the 0.01 level (2-tailed)										

Table 4: Structural path analysis result

Dependent variables		Independent variables	Estimate	S.E.	C.R.	P
SMF	<---	CSM	0.273	0.075	3.640	***
SMF	<---	PCT	0.198	0.087	2.267	*
SMF	<---	EV	0.123	0.042	2.928	**
SMF	<---	VIS	0.229	0.06	0.488	0.626
SMF	<---	PT	0.351	0.082	4.254	***
SMF	<---	SP	0.149	0.066	2.244	*
SMF	<---	RC	0.140	0.059	2.372	*
SMF	<---	FC	0.203	0.056	3.625	***
SMF	<---	CSP	0.189	0.065	2.907	**

***p<.000, **p<.01, *p<.05, NS p>.05

Table 5: Hypotheses analysis summary

No		β	Findings
$H1_a$	Perceived advantages of adopting current security measures have a positive effect on the information security strategy of companies	0.273***	Significant
$H1_b$	Review of past crimes and threats with existing company technologies has a positive effect on the information security strategy of companies	0.198*	Significant
$H1_c$	Observability of existing vulnerabilities has a positive effect on the information security strategy of companies	0.123**	Significant
$H1_d$	Availability of virtual infrastructure security has a positive effect on the information security strategy of companies	0.229	Significant
$H2_a$	Availability of procedures and training has a positive effect on the information security strategy of companies	0.351***	Significant

***p<.000, **p<.01, *p<.05, NS p>.05

Table 5: Hypotheses analysis summary

No		β	Findings
$H2_b$	Availability of security personnel has a positive effect on the information security strategy of companies	0.149*	Significant
$H2_c$	Availability of reducing consequences has a positive effect on the information security strategy of companies	0.140*	Significant
$H2_d$	Availability of the facility characteristics (static and dynamic) has a positive effect on the information security strategy of companies	0.203***	Significant
$H2_e$	Availability of corporate security policy has a positive effect on the information security strategy of companies	0.189**	Significant
***p<.000, **p<.01, *p<.05, NS p>.05			

The goal of information security is to be able not only to implement measures to detect and mitigate attacks, but also to preemptively predict attacks, deter attackers from attacking, and thus defend the systems from attack in the first place (Arukonda & Sinha, 2015). In order for information security measures to have the capacity to deter conventional attacks, both due to aggression by external parties and those caused by internal sources, policies must be developed within each organization to parallel those developed at the governmental level.

Between the concepts of risk, organizational culture and trust there is a direct relationship (Kolkowska, Karlsson & Hedström, 2017). Changing an organization's operational needs as determined for example by changing mission requirements and exchange information with other entities may involve changing risk tolerance level, above the level set by the management of the organization. These measures lead to building confidence in the organization long term.

The interaction between trust in organization and organizational culture can also be observed when there is overlapping responsibility or uncovered areas between various parts of an organization may impact on the ability to undertake operative.

Developing a risk management process and its proper procedures are likely to enhance the credibility of the organization and the capital trust with its partners and investment. Demonstrating that the organization has structures and procedures to ensure effective protection of information that circulates determines both the organization's external partners (suppliers, customers, entities whose business depends on the organization in question) and to staff the faith that the organization operates in a consistent manner based on clear rules and procedures, which leaves no room for chaos and bias.

Limiting to a reactive management style is not a viable option for an efficient management. No organization can be managed on the basis of the "seeing and doing" principle. Equally important is the identification of possible threats before they materialize and produce adverse consequences to the objectives. This means adopting a proactive management style. Proactive management is based on the principle "it is better to prevent than to note a fact".

Many organizations adopt the practice of updating the risk management policy annually. This practice ensures that the overall approach to risk management is in line with the latest practices. At the same time, it offers the organization the opportunity to focus on future goals, on the identification of priorities in terms of risk management and to identify emerging risks.

In a stage where, as we pointed out above, information has become a basic resource of any organization, making the best decisions to protect this resource must be based on a coherent analysis.

FUTURE RESEARCH DIRECTIONS

Future research is important because certain events with a negative impact on the objectives to be transformed into opportunities if they are identified early. One of the limitations of this study is that the collected data was cross-sectional, and all hypotheses were examined for a particular period. In addition, the data in this study was collected within particular urban areas in Romania. Hence, special care should be taken when generalizing our findings to other country's businesses. Furthermore, the effects of demography are not included in this study, but some demographic factors may have more explanatory power than others which can be investigated in future research. Best practices will consist of technical and procedural security measures whose effectiveness in combating specific threats and vulnerabilities has been proven.

CONCLUSION

Big data was the relatively new way of conducting business by providing new insight (Yeow, Soh & Hansen, 2018). The two types of uses were categorized into either user facing or business facing (Lowry & Wilson, 2016). The business facing applications tended to provide system infrastructure and details analytics to either streamline internal practices or improve business decision making.

The manager of an organization should not be limited to treating each time, the consequences of events that have occurred, showing a passive management style, or respond to negative punctual events that may affect the organization's objectives,

proving a reactive management style. Treating the consequences does not eliminate the causes and, therefore, already materialized risks will occur in the future, usually with greater frequency and with an increased impact on the objectives. Managers must adopt a proactive management style, which means that it is necessary to design and implement measures to mitigate risks manifestation. Future-oriented response allows the organization to master, within acceptable limits, the past risks, which is the same as increasing the chances to achieve its objectives.

From another perspective, a better integration of data analysis and use of open data sources into design curriculums could prove to be invaluable to new designers who may benefit from exposure to new methods of research. A strong connection to the importance of alternate data collection methods as a source of design innovation and creativity could bring designers to big data to use in future projects.

Bearing in mind the conclusions outlined above, the organizations benefiting from an efficient management, "scrutinizing the horizon" is not limited to the immediate future, but consider further perspective, the trends projected for the external environment of the organization. In these situations, proactive management becomes a prospective management, in which the management tries to identify those risks that may arise due to changes in strategy or environment. The organization must be prepared to accept the change.

In order to consolidate and improve the information security posture, efforts should be based on a series of few principles that we consider to be essential bricks towards a building trust and credibility:

- Coordination, meaning that all policies approved and actions taken to be circumscribed to a unitary concept, according to convergent plans of action towards attaining information security, according to responsibilities and competencies of each organizational department within the organization; a team-oriented approach is vital in fighting against information security threats;
- Cooperation, meaning that all entities having responsibilities (either public institutions or private companies or non-governmental organizations) should collaborate at international, national and organizational level, in order to ensure an adequate response to information technology threats and to possible successful information security attacks;
- Efficiency, meaning that all resources, either financial, human, material, have to be correctly allocated and managed in order to address the primary needs and priorities;
- Prioritization, meaning that the efforts have to be focused on the protection of those communication and information systems supporting critical functions of the society and, respectively, of the organization;
- Dissemination, meaning that a proper transfer and sharing of information, expertise and best practices have to be ensured among persons with responsibilities in the field of protecting communication and information systems handling sensitive information or supporting critical functions.

Like any factor in a complex system, the benefits of information security are weighed against their total cost (including the additional costs incurred if the system is compromised). If the data or resources cost less, or are of less value, than their protection, adding security mechanisms and procedures is not cost-effective because the data or resources can be reconstructed more cheaply than the protections themselves. Unfortunately, this is rarely the case.

Residual risk is the risk that remains after security measures are implemented in a computer system and communications, as a consequence of the fact that not all threats can be countered and not all vulnerabilities can be eliminated or reduced to zero.

As we have seen, for safety information required increasingly more stringent use of cryptographic mechanisms that make information become inaccessible to unauthorized persons. On the other hand, there is concern becoming more serious on the use of cryptography by criminals in order to escape police observation.

Strategy to restore services and resources information system provides a quick and effective way to restore the operability of a system in case of interruption of its operation. The strategy should be linked to the impact on information security objectives in case of disruption of its operation and the maximum time allowed for the decommissioning of the system, as we have previously defined.

Overlapping benefits are also a consideration. Suppose the integrity protection mechanism can be augmented very quickly and cheaply to provide confidentiality. Then the cost of providing confidentiality is much lower. This shows that evaluating the cost of a particular security service depends on the mechanism chosen to implement it and on the mechanisms chosen to implement other security services. The cost-benefit analysis should take into account as many mechanisms as possible. Adding security mechanisms to an existing system is often more expensive (and, incidentally, less effective) than designing them into the system in the first place.

REFERENCES

Agrawal, N., & Tapaswi, S. (2017). *Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing: A survey*. *Information Security Journal: A Global Perspective*, 26(1), 1–13.

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). *Incident Response Teams–Challenges in Supporting the Organisational Security Function*. *Computers & Security*, 31(5), 643–652. doi:10.1016/j.cose.2012.04.001

Ahmad, A., Maynard, S. B., & Park, S. (2014). *Information security strategies: Towards an organizational multi-strategy perspective*. *Journal of Intelligent Manufacturing*, 25(2), 357–370. doi:10.100710845-012-0683-0

Anderson, E., & Choobineh, J. (2008). *Enterprise information security strategies*. *Computers & Security*, 27(1-2), 22–29. doi:10.1016/j.cose.2008.03.002

Andress, A. (2003). *Surviving Security: How to Integrate People, Process, and Technology*. Boca Raton, FL: Auerbach Publications. doi:10.1201/9780203501405

Arukonda, S., & Sinha, S. (2015). *The innocent perpetrators: Reflectors and reflection attacks*. *Advanced Computer Science*, 4, 94–98.

Banker, R., Chang, H., & Kao, Y.-C. (2010). *Evaluating Cross-Organizational Impacts of Information Technology – an Empirical Analysis*. *European Journal of Information Systems*, 19(2), 153–167. doi:10.1057/ejis.2010.9

Baskerville, R. (2010). *Third-Degree Conflicts: Information Warfare*. *European Journal of Information Systems*, 19(1), 1–4. doi:10.1057/ejis.2010.2

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). *Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response*. *Information & Management*, 51(1), 138–151. doi:10.1016/j.im.2013.11.004

Bojanc, R., Jerman-Blaic, B., & Tekavcic, M. (2012). *Managing the Investment in Information Security Technology by Use of a Quantitative Modeling*. *Information Processing & Management*, 48(6), 1031–1052. doi:10.1016/j.ipm.2012.01.001

Bojanc, R., & Jerman-Blažic, B. (2012). *Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System*. *Organizacija*, 45(6), 276–288. doi:10.2478/v10051-012-0027-z

Broadbent, A., & Schaffner, C. (2016). *Quantum cryptography beyond quantum key distribution*. *Designs, Codes and Cryptography*, 78(1), 351–382. doi:10.100710623-015-0157-4

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). *The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*. *Journal of Computer Security*, 11(3), 431–448. doi:10.3233/JCS-2003-11308

Chai, S., Kim, M., & Raoc, R. (2011). *Firms' information security investment decisions: Stock market evidence of investors' behaviour*. *Decision Support Systems*, 50(4), 651–661. doi:10.1016/j.dss.2010.08.017

Charki, M. H., Josserand, E., & Boukef, N. (2017). *The paradoxical effects of legal intervention over unethical information technology use: A rational choice theory perspective*. *The Journal of Strategic Information Systems*, 26(1), 58–76. doi:10.1016/j.jsis.2016.07.001

Chen, H., Ge, L., & Xie, L. A. (2015). *User Authentication Scheme Based on Elliptic Curves Cryptography for Wireless Ad Hoc Networks*. *Sensors (Basel)*, 15(7), 17057–17075. doi:10.3390150717057 PMID:26184224

Choi, Y., Lee, D., Kim, J., Jung, J., Nam, J., & Won, D. (2014). *Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography*. *Sensors (Basel)*, 14(6), 10081–10106. doi:10.3390140610081 PMID:24919012

Chou, T.-Y., Seng-Cho, T. C., & Tzeng, G.-H. (2006). *Evaluating IT/IS Investments: A Fuzzy Multi-Criteria Decision Model Approach*. *European Journal of Operational Research*, 173(3), 1026–1046. doi:10.1016/j.ejor.2005.07.003

Clarke-Sather, A. R., Hutchins, M. J., Zhang, Q., Gershenson, J. K., & Sutherland, J. W. (2011). *Development of social, environmental, and economic indicators for a small/medium enterprise*. *International Journal of Accounting and Information Management*, 19(3), 247–266. doi:10.1108/18347641111169250

Collins, S., & McCombie, S. (2012). *Stuxnet: The emergence of a new cyber weapon and its implications*. *Journal of Policing. Intelligence and Counter Terrorism*, 7(1), 80–91. doi:10.1080/18335330.2012.653198

Da Veiga, A. (2016). *Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study*. *Information & Computer Security*, 24(2), 139–151. doi:10.1108/ICS-12-2015-0048

Dor, D., & Elovici, Y. (2016). *A Model of the Information Security Investment DecisionMaking Process*. *Computers & Security*, 63, 1–13. doi:10.1016/j.cose.2016.09.006

Eloff, M. M., & Von Solms, S. H. (2000). *Information Security Management: An Approach to Combine Process Certification and Product Evaluation*. *Computers & Security*, 19(8), 698–709. doi:10.1016/S0167-4048(00)08019-6

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). *Current challenges in information security risk management*. *Information Management & Computer Security*, 22(5), 410–430. doi:10.1108/IMCS-07-2013-0053

Fischbacher-Smith, D. (2016). *Breaking bad? In search of a (softer) systems view of security ergonomics*. *Security Journal*, 29(1), 5–22. doi:10.1057j.2015.41

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). *Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture*. *Computers & Security*, 43, 90–110. doi:10.1016/j.cose.2014.03.004

Flowerday, S. V., & Tuyikeze, T. (2016). *Information security policy development and implementation: The what, how and who*. *Computers & Security*, 61, 169–183. doi:10.1016/j.cose.2016.06.002

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2016). *STPA-SafeSec: Safety and security analysis for cyber-physical systems*. *Journal of Information Security and Applications*, 29, 1–12.

Gaidelys, V., & Valodkiene, G. (2011). *The Methods of Selecting and Assessing Potential Consumers Used of by Competitive Intelligence*. *Inzinerine Ekonomika-Engineering Economics*, 22(2), 196–202.

Gandino, F., Celozzi, C., & Rebaudengo, M. (2017). *A Key Management Scheme for Mobile Wireless Sensor Networks*. *Applied Sciences*, 7(5), 490. doi:10.3390/app7050490

Gandotra, V., Singhal, A., & Bedi, P. (2012). *Threat-Oriented Security Framework: A Proactive Approach in Threat Management*. *Procedia Technology*, 4, 487–494. doi:10.1016/j.protcy.2012.05.078

Gkioulos, V., Wangen, G., Katsikas, S. K., Kavallieratos, G., & Kotzanikolaou, P. (2017). *Security Awareness of the Digital Natives*. *Information*, 8(2), 42. doi:10.3390/info8020042

Hadžiosmanović, D., Bolzoni, D., & Hartel, P. H. (2012). *A log mining approach for process monitoring in SCADA*. *International Journal of Information Security*, 11(4), 231–251. doi:10.100710207-012-0163-8

Hausmann, V., Williams, S. P., Hardy, C. A., & Schubert, P. (2014). *Enterprise Information Management Readiness: A Survey of Current Issues, Challenges and Strategy*. *Procedia Technology*, 16, 42–51. doi:10.1016/j.protcy.2014.10.066

He, D., Chen, C., Chan, S., & Bu, J. (2012). *Secure and efficient handover authentication based on bilinear pairing functions*. *IEEE Transactions on Wireless Communications*, 11(1), 48–53. doi:10.1109/TWC.2011.110811.111240

Hiller, J., & Russel, R. (2013). *The challenge and imperative of private sector cybersecurity: An international comparison*. *Computer Law & Security Review*, 29(3), 236–245. doi:10.1016/j.clsr.2013.03.003

Hjortdal, M. (2011). *China's use of cyber warfare: Espionage meets strategic deterrence*. *The Journal of Strategic Studies*, 4(2), 1–24.

Hoang, D., & Ruckes, M. (2017). *Corporate risk management, product market competition, and disclosure*. *Journal of Financial Intermediation*, 30, 107–121. doi:10.1016/j.jfi.2016.07.003

Hong, J., Kim, J., & Cho, J. (2010). *The trend of the security research for the insider cyber threat*. *International Journal of Future Generation Communication and Networking*, 3(2), 31–40.

Karim, H. V. (2007). *Strategic security management: a risk assessment guide for decision makers*. Amsterdam: Elsevier.

Kesan, P. J., & Hayes, M. C. (2012). *Mitigative counterstriking: Self-defense and deterrence in cyberspace*. *Harvard Journal of Law & Technology*, 25(2), 474–529.

Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., & Ahmad, I. (2016). *Network forensics: Review, taxonomy, and open challenges*. *Journal of Network and Computer Applications*, 66, 214–235. doi:10.1016/j.jnca.2016.03.005

Kim, S. H., Wang, Q.-H., & Ullrich, J. B. (2012). *A Comparative Study of Cyberattacks*. *Communications of the ACM*, 55(3), 66. doi:10.1145/2093548.2093568

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). *Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method*. *The Journal of Strategic Information Systems*, 26(1), 39–57. doi:10.1016/j.jsis.2016.08.005

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). *Advanced social engineering attacks*. *Journal of Information Security and Applications*, 22, 113–122. doi:10.1016/j.jisa.2014.09.005

Landoll, D. J. (2010). *The security risk assessment handbook: a complete guide for performing security risk assessment* (2nd ed.). New York: CRC Press.

Liaudanskienel, R., Ustinovicius, L., & Bogdanovicius, A. (2009). *Evaluation of Construction Process Safety Solutions Using the TOPSIS Method*. *Inzinerine Ekonomika-Engineering Economics*, 64(4), 32–40.

Lin, Z., Lin, D., & Pei, D. (2017). *Practical construction of ring LFSRs and ring FCSRs with low diffusion delay for hardware cryptographic applications*. *Cryptography and Communications*, 9(4), 431–440. doi:10.100712095-016-0183-8

Lowry, P. B., & Wilson, D. (2016). *Creating agile organizations through IT: The influence of internal IT service perceptions on IT service quality and IT agility*. *The Journal of Strategic Information Systems*, 25(3), 211–226. doi:10.1016/j.jsis.2016.05.002

Malatras, A., Geneiatakis, D., & Vakalis, I. (2016). *On the efficiency of user identification: A system-based approach*. *International Journal of Information Security*, 15(1), 1–19.

Martinez-Caro, J.-M., Aledo-Hernandez, A.-J., Guillen-Perez, A., Sanchez-Iborra, R., & Cano, M.-D. (2018). *A Comparative Study of Web Content Management Systems*. *Information*, 9(2), 27. doi:10.3390/info9020027

McQuade, S. (2006). *Understanding and Managing Cybercrime*. Boston: Allyn & Bacon.

Mittelman, J. H. (2011). *Global (in) security: The confluence of intelligence and will*. *Global Change, Peace & Security*, 23(2), 135–139. doi:10.1080/14781158.2011.580954

Mohammed, F., Ibrahim, O., & Ithnin, N. (2016). *Factors influencing cloud computing adoption for e-government implementation in developing countries: Instrument development*. *Journal of Systems and Information Technology*, 18(3), 297–327. doi:10.1108/JSIT-01-2016-0001

Okamoto, T., & Takashima, K. (2015). *Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption*. *Designs, Codes and Cryptography*, 77(2), 725–771. doi:10.100710623-015-0131-1

Peltier, T. R. (2010). *Information security risk analysis* (3rd ed.). New York: CRC Press, Auerbach Publications.

Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018). *Is the responsibilization of the cyber security risk reasonable and judicious? Computers & Security*, 78, 198–211. doi:10.1016/j.cose.2018.06.006

Renwick, S. L., & Martin, K. M. (2017). *Practical Architectures for Deployment of Searchable Encryption in a Cloud Environment*. *Cryptography*, 1(3), 19. doi:10.3390/cryptography1030019

Ruževičius, J., & Gedminaitė, A. (2007). *Business Information Quality and its Assessment*. *Inzinerine Ekonomika-Engineering Economics*, 52(2), 18–25.

Sá-Soares, F., Soares, D., & Arnaud, J. (2014). *Towards a Theory of Information Systems Outsourcing Risk*. *Procedia Technology*, 16, 623–637. doi:10.1016/j.protcy.2014.10.011

Shamala, P., Ahmad, R., Zolait, A. H., & Sahib, S. (2015). *Collective information structure model for Information Security Risk Assessment (ISRA)*. *Journal of Systems and Information Technology*, 17(2), 193–219. doi:10.1108/JSIT-02-2015-0013

Singer, W. P., & Friedman, A. (2014). *Cyber Security and Cyber War: What Everyone Needs to Know*. New York: Oxford University Press.

Singh, A., & Fhom, H. C. S. (2017). *Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection*. *International Journal of Information Security*, 16(2), 195–201. doi:10.100710207-016-0328-y

Smith, D. (2005). *Dancing with the mysterious forces of chaos: Issues around complexity, knowledge and the management of uncertainty*. *Clinician in Management*, (3/4), 115–123.

Soomro, Z., Hussain Shah, A. M., & Ahmed, J. (2016). *Information security management needs more holistic approach: A literature review*. *International Journal of Information Management*, 36(2), 215–225. doi:10.1016/j.ijinfomgt.2015.11.009

Stepchenko, D., & Voronova, I. (2015). *Assessment of Risk Function Using Analytical Network Process*. *Inzinerine Ekonomika-Engineering Economics*, 26(3), 264–271.

Sveen, F., Torres, J., & Sarriegi, J. (2009). *Blind Information Security Strategy*. *International Journal of Critical Infrastructure Protection*, 2(3), 95–109. doi:10.1016/j.ijcip.2009.07.003

Tiago, O., Manoj, T., & Espadanal, M. (2014). *Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors*. *Information & Management*, 51(5), 497–510. doi:10.1016/j.im.2014.03.006

Tropina, T., & Callanan, C. (2015). *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*. New York: Springer International Publishing. doi:10.1007/978-3-319-16447-2

Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). *Strategic value alignment for information security management: A critical success factor analysis*. *Information & Computer Security*, 26(2), 150–170. doi:10.1108/ICS-06-2017-0042

Tutton, J. (2010). *Incident Response and Compliance: A Case Study of the Recent Attacks*. *Information Security Technical Report*, 15(4), 145–149. doi:10.1016/j.istr.2011.02.001

Wang, W., & Hu, L. (2014). *A secure and efficient handover authentication protocol for wireless networks*. *Journal of Sensors*, 14(7), 11379–11394. doi:10.3390140711379 PMID:24971471

Willems, E. (2011). *Cyber-terrorism in the process industry*. *Computer Fraud & Security*, 3(3), 16–19. doi:10.10161361-3723(11)70032-X

Winkler, I. (2010). *Justifying IT Security – Managing Risk & Keeping your network Secure*. Qualys Inc.

Xu, R., Chen, Y., Blasch, E., & Chen, G. (2018). *BlendCAC: A Smart Contract Enabled Decentralized Capability-Based Access Control Mechanism for the IoT*. *Computers*, 7(3), 39. doi:10.3390/computers7030039

Yang, C. N., Wu, C. C., & Wang, D. S. (2014). *A discussion on the relationship between probabilistic visual cryptography and random grid*. *Information Sciences*, 278, 141–173. doi:10.1016/j.ins.2014.03.033

Yar, M. (2006). *Cybercrime and Society*. London: Sage.

Yeow, A., Soh, C., & Hansen, R. (2018). *Aligning with new digital strategy: A dynamic capabilities approach*. *The Journal of Strategic Information Systems*, 27(1), 43–58. doi:10.1016/j.jsis.2017.09.001

ADDITIONAL READING

Agrawal, N., & Tapaswi, S. (2017). *Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing: A survey*. *Information Security Journal: A Global Perspective*, 26(1), 1-13.

Karanja, E. (2017). *The role of the chief information security officer in the management of IT security*. *Information & Computer Security*, 25(3), 300–329. doi:10.1108/ICS-02-2016-0013

Kurosawa, K., Ohta, H., & Kakuta, K. (2017). *How to make a linear network code (strongly) secure*. *Designs, Codes and Cryptography*, 82(3), 559–582. doi:10.100710623-016-0180-0

Lee, C., Lee, C. C., & Kim, S. (2016). *Understanding information security stress: Focusing on the type of information security compliance activity*. *Computers & Security*, 59, 60–70. doi:10.1016/j.cose.2016.02.004

Lee, W., & Kim, N. (2017). *Security Policy Scheme for an Efficient Security Architecture in Software-Defined Networking*. *Information*, 8(2), 65. doi:10.3390/info8020065

Zangeneh, V., & Shajari, M. (2018). *A cost-sensitive move selection strategy for moving target defense*. *Computers & Security*, 75, 72–91. doi:10.1016/j.cose.2017.12.013

KEY TERMS AND DEFINITIONS

Availability:
Ensuring the conditions necessary for easy retrieval and use of information and system resources, whenever necessary, with strict conditions of confidentiality and integrity.

Cost:
The money form of all material and labor expenses made by the company to produce and market material goods, execution works and service works.

Cyber Physical Systems:
They are being set up by the internet of things that are machines, employees, products and products facilities being digitally interconnected by the internet.

Integrity:
The prohibition amendment—by deleting or adding—or the unauthorized destruction of information; integrity refers to confidence in the data and resources of a system by which to manage information.

Organizational Culture:
Values and behaviors that contribute to creating a social and psychological environment of an organization.

Prevention:
Implementation of mechanisms that users not be able to counteract and are implemented correctly, unaltered, so the attacker cannot alter them.

Risk Management:
The implementation and updating of methods and tools to minimize risks associated with the information system of an organization, such as the Information Security policies, procedures and practices associated formalized and adopted other means in order to bring these risks to acceptable levels.

SEM:
Structural equation modeling.

Threats:
The possibility of accidental or deliberate compromise of information security, the loss of confidentiality, integrity, or availability or impaired functions that provide authenticity and non-repudiation of information.

Vulnerabilities:
Gaps or weaknesses in the design and implementation of safety or security measures which could be exploited accidentally or intentionally by a threat.