Academic Journal of Economic Studies
Vol. 5, No. 3, September 2019, pp. 120–125
ISSN 2393-4913, ISSN On-line 2457-5836

Theoretical Approaches to Estimate the Information Security Risks

Cristina Ștefănescu[1], Loredana Elena Comănescu[2], Ciprian Buhuși[3], George Adrian Bîlcan[4]

[1,2,3,4]Valahia University, Romania,[1]E-mail: cristina.stefanescu@gmail.com, [2]E-mail: comanescu.loredana.elena@gmail.com, [3]E-mail: ciprian.buhusi@gmail.com, [4]E-mail: bilcangeorgeadrian@gmail.com

Abstract

The risk analysis aims to assess relationships between assets, threats, vulnerabilities and security measures to determine potential losses. However, tools for risk analysis should be thoroughly checked to meet the managerial decisions. This article presents the implications and challenges of using quantitative and qualitative methodologies for assessing information security risks for control. The results show that the quantitative information is expressed more easily understandable by people with marginal training in related areas of information technology.

Key words

Security risks, information security, managerial decisions

JEL Codes: H55

Received: 25 July 2019 **Revised: 10 August 2019** **Accepted: 20 August 2019**

1. Introduction and literature review

Risk management is 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 (Ben-Asher and Gonzalez, 2015). This process involves identifying, analysing, evaluating, treating and monitoring risks associated with information security organizational level.

To ensure the success associated with information security risk management is crucial involvement of senior management by actively promoting its process and providing the necessary resources (Petrescu *et al.,* 2012). Also, this practice has proved particularly successful in situations where risk management was carried out by mixed teams that included administrators and information systems managers in the organization's production system.

Given that organizational activities and assets are in constant restructuring that information technology is one of the most effervescent areas of the modern economy and human and technological resources of an organization are adjusted frequently, and the activities associated with risk minimization referring to information technology must be reviewed and regularly updated in order to asses such changes and to determine a current efficiency level of implemented controls (Sîrbu, 2012).

Establish a risk management program involves a first phase, setting goals of this activity, which may include reducing insurance costs or reduce risk of sensitive information leaking outside the organization (Simmonds, 2017). Organizational risk management is not strictly serial process, the succeeding steps in a predetermined order and a component affects only the next. Organizational risk management process is a multifaceted and iterative process in which almost every component has the possibility and even going to affect the other.

By determining its intention before initiating a program of risk management, the institution can evaluate the results and can determine the effectiveness. Also in the planning necessary to perform risk management program requires the appointment of a person or team responsible for implementation. A successful team requires the integration of all organizational levels on this team level, or at least a good collaboration with all team members' at all significant levels of the organization, a collaboration generally facilitated by the involvement and support of the organization's management. Risk management is a logical and systematic manner associated with establishing the context, risk identification, risk analysis, risk assessment and ultimately treated. This approach implies, however, communication of the observed, and monitoring and periodic review of the treatment of risk.

Risk assessment refers to identifying risks to be addressed and is done by calculating the product of the probability of the adverse event and its consequences. Risk can be compared to predetermined criteria. In the evaluation software can be used as Monte Carlo simulations, sensitivity analysis and probability distribution.

In general, technological aspects are identified by comparison with standards established profile either producers or independent bodies. Generally, at this stage weaknesses of the system are determined based on a variety of automated tools, including tools for testing the integrity of files, antivirus, and system efficiency by limiting access passwords, security communications, and many other instruments.

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. Since removing all security risks is usually impractical or almost impossible manager's responsibility to address this stage in terms of lowest cost and implement adequate security measures to reduce risks to an acceptable level with minimal impact on resources and the organization's mission.

In accordance with ISO/IEC 27001, the stage immediately after completion of the risk analysis is to develop a risk treatment plan, which should underpin decision on how each of the identified risks should be managed. The criteria for activation of the plan in case of unforeseen events specific to the organization and be established in the security policy on the continuation of emergency. In establishing the criteria for activating the contingency plan may be considered the following: the number of system equipment that may be affected by the incident; number of critical elements of the system affected by the incident, expected duration of the shutdown of the system.

2. The importance of Security Risk Assessment Tools

To achieve identification and information security risk assessment is essential to identify threats and vulnerabilities in the system they can exploit (Sîrbu, 2012). For each pair threat/vulnerability, determine the severity of impact on the organization's information assets (loss of confidentiality, integrity or availability there) and determine the likelihood that vulnerabilities exploitation in conditions of security controls implemented at the system level.

More in detail, the threats can result in events such as sags biological contamination or leakage of toxic chemicals, natural disasters, hardware malfunction or software, loss or damage to data integrity, sabotage, theft or vandalism. In turn, vulnerabilities relate to weaknesses in logical or physical security of organizational assets that a threat can exploit to affect them. Vulnerabilities are generally classified as physical security vulnerabilities, menu systems security; communication security processes associated personnel, plans, policies, procedures, management, support, and other types.

There are situations where confidentiality is critical, being able to take damage, to some extent, the objective availability and mechanisms hindering access to the system and thus to information - case met the information with high sensitivity with as the classified information. In other cases, availability is critical, even at the expense of privacy - operative situations where quick access to information is crucial for the performance of certain tasks/activities.

In general, the risks can be transferred, dismissed, reduced or accepted. An example of risk transfer is purchase an insurance policy from a company specialized in risk identified. Rejecting an assumed risk by ignoring his organization, this may be long-term, highly dangerous policy. Also, risks can be reduced by implementing or improving methods and tools for risk minimization (controls), but always taking into account both the benefits and costs associated with these methods and tools. Thus, if the cost exceeds the benefits that these controls will enjoy the organization, then it can decide to accept additional risks at the expense of securing the organization's information system.

Tools for risk analysis should be thoroughly checked to meet the intended purpose; taking into account the possible use of them in the risk analysis has been the subject of managerial decisions. The following sections provide guidance on selection of software tools for risk analysis. This component is necessary to identify the goods and their value expressed in either qualitative or quantitative. It is also possible to obtain information about threats, vulnerabilities and security measures recommended. Some software tools for quantitative risk analysis using approximations to calculate risk. An approximation loss for an organization is obtained by estimating the frequency of an undesired event that affects the organization's objectives and the quantitative impact that may result.

Most risk analysis tools have in the main menu functions "on- line help" Some tools provide user menus that are accessed questionnaires, calculations, reports and installation procedures. Some use the entire screen interactive introduction to data and include database management, taking and word processing functions. Other tools allow the user to develop various formats of reports and questionnaires. Some manufacturers also make products available to the beneficiary demonstration versions of the software package to a better understanding of the instrument.

Associated with the organization of information security controls are generally classified as actions, procedures, techniques or equipment (Sicari et al., 2015). The robustness of a control is generally associated with robustness default or obtained by human intervention as effective in preventing risks. Also, the controls are classified in terms of their explicitness controls documentation and formal and ad hoc controls in terms of discussing the release mode manual controls or automatic, and in terms of the time they are applied, preventive controls are classified detective.

Categorizing risks (internal/external), the magnitude of the impact (strategic or operational), belonging to a class of problems, levels of responsibility in risk management, congruence measures to be taken and so on, are elements on which its system is designed group organization.

Risk avoidance seems at first glance to be suitable decision for all risk categories. At the same time, however, risk avoidance causes loss of opportunities to be more efficient and consistent operational responsibilities assumed by the organization by accepting risk opportunities that could be exploited. Likewise, adopting a position of risk acceptance is also unlikely given the amount of information assets to the organization and the damage it can bring damage security objectives of the organization. For these reasons, the treatment of information security risks are adopted generally a risk reduction strategy.

The level of risk that an organization inevitably will keep after implementing a risk management program called residual risk (Landoll, 2010). 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. It can then be used by the risk management team or the management of the organization to identify those areas where the controls is not appropriate and strengthen them in order to further reduce the level of risk to which information is subject organization. In general, management establishes a target (maximum) residual risk and risk management team do all the best to achieve this target.

Accepting a certain level of residual risk is generally based on the organization's policy, a formal process for identifying and measuring risk, the level of uncertainty associated with the risk assessment process itself, as well as cost-benefit analysis of controls identified.

A model of cost-benefit analysis would address a communication system and that store and process sensitive information for an organization. For this system was not activated component of the operating system audit user activity. The report recommended the need for risk analysis of activation of this component. Therefore, for correct decision making, management organization decided achieving cost - benefit analysis to determine whether to activate the audit facility for system analysis.

Frequently, the costs of implementation of security measures outweigh the costs of its non-implementation. As a result, management of the organization plays an important role in decisions on implementing measures for the security system and communication, and the information therein.

On the other hand, the use of quantitative methods involves the assumption of drawbacks associated with them, such as the complexity of the calculations necessary to determine values of different variables (and the lack of explanations can lead to lack of trust management for some values obtained using methods of "black box").

The various qualitative methodologies or qualitative partly led to the implementation of specific tools necessary for the collection of information risk assessment information, but with no generally agreed standard (Armaghan *et al.,* 2012). Thus, to determine the likelihood of exploitation of a specific vulnerability of the system is the combination of the frequency with which the associated threat occurs. This probability is related to a number of factors including system architecture, the external environment, how to control access to protected information assets, as well as the effectiveness of controls implemented.

Determining the magnitude or severity of the impact of a particular threat involves identifying potential losses in each category of security (confidentiality, integrity and availability), while the probability associated with its production (Rot, 2008). The impact may be associated with loss of system functionality or other assets of the organization, degradation, reducing response time for legitimate users, loss of public confidence in the organization or unauthorized disclosure of sensitive data.

Another important feature of the software risk analysis tool is the presentation of the final result. The main purpose of using such a tool is to help staff involved in risk reduction to select security measures in the list provided by the program. It should be noted that not all risk analysis tools have this feature. It is important that risk analysis tool to highlight where it is necessary to apply recommended measures to protect critical assets and information.

Risk management is a process that requires the involvement of employees of the organization, at all levels of command, from the top management to the execution. Each of these levels must know their responsibilities for risk management and to exercise them. Ultimately, the general manager shall be responsible for all activities carried out within the organization. Other managers should support risk management philosophy adopted within the organization to promote organizational procedures to ensure compliance with approved and coordinate risk management within their sphere of responsibility, in accordance with the risk tolerance of the organization, the specific component.

The personnel having responsibilities concerning risk management, financial personnel, internal auditors have also clear responsibilities regarding the support of risk management process. It is possible that the external personnel could also have responsibilities in performing the management process of organizational risk, according to well-established procedures. The board of directors must provide an oversight of the management process of organizational risk and has to be aware of the risk appetite and risk tolerance level specific to the organization. Some other external entities of the organization, such as customers, suppliers, business partners, external auditors, regulators and financial analysts often provide useful information for an efficient risk management process, but they are not responsible for the effectiveness of this process and also they are not part of the organizational risk management.

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;
- Sometimes ignore the importance of training and staff development in the context of change that will take place;
- Change is successful only if the organization's staff change their attitude to adapt to new conditions created by the change;
- Implementing a system with increased security personnel responsibilities.

Finally, determining the level of risk is generally made based on the probability that a given threat exploiting vulnerability in the system and the gravity that having this threat has on the organization's information assets. Mathematically, the risk is determined as the product of probability and severity of threats manifestation of their impact on the confidentiality, availability and integrity of the information system of the organization (Sîrbu, 2012). However, the consequences can be expressed in terms of average or expected value. This estimate is consistent with the Monte Carlo simulation technique, which may be obtained to obtain a distribution of values or the product.

Among the advantages of using qualitative methods is included that in general, there is no need to accurately determine the financial value of assets, but rather their effects in terms of general information security (confidentiality, availability, integrity). Also, qualitative assessment of the risks associated with information security also requires a number of disadvantages, including the fact that risk assessment and the results of this process are essentially subjective, influenced by qualified and experienced analysts.

3. Result and discussions

Risk analysis is the part of the risk management process which is concerned with minimizing risks associated with the occurrence of threats from internal or external environment of the organization assumed or unknown exploit vulnerabilities of the information system and thus affects the security of information assets. Also, risk analysis involves associating frequency with which the threats associated with these risks may occur, as the impact they may have on the optimal deployment of the organization's normal activities analysed.

Once the organization's leadership understood the information about the technology and information that lead to the formation of the identified risks and their potential impact on the organization, it is recommended to prioritize these risks, depending on the severity that their production might have on the organization.

Likelihood and magnitude of impact are the basic elements of this prioritization, which may include items such as the costs, associated with implementing such controls or deemed cost of removing the negative effects produced by their production.

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.

The objective elements underlying confidence building can be, for example, results of the IT & C products used or the security measures that convey information systems sensitive. Level of experience, stability is subjective elements which complete and sometimes even replace, the objective elements on which trust entity. In general, trust is associated with certain circumstances, such as the total amount transacted, sensitivity or criticality of information, the potential loss of property or life, etc. Confidence in an entity is not transitive and gaining general experience and measurements.

Between the concepts of risk, organizational culture and trust there is a direct relationship. 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.

Where risks have been properly identified, analyzed and prioritized, the risk of loss of time finding ways to counteract the losses that have a low probability of occurrence. Large temporal resource allocation analysis and management of risks can divert resources unlikely to be used much more efficiently. During the life cycle of an activity may appear a multitude of events unlikely, but if the risk is unlikely, we recommend a strategy addressing risk acceptance and management of losses if the risk materializes.

Most often, organizations adopt combined strategies for addressing the risks identified in the risk analysis stage security. In dealing with risks to information conveyed through information and communication systems, the predominant strategy is to determine the implementation of measures to reduce risks so as to ensure the objectives of information security - confidentiality, integrity, availability, authenticity and non-repudiation - in order to fulfill properly the organization's mission. For this reason, in what follows we will focus on how to implement an approach to reduce the identified risks to the information conveyed through computer systems and communications.

Adapting to change requires the identification of risks that may arise in the future as a result of changes visible. By organizational culture of risk, risk managers must prepare in time to cope with future risks.

4. Conclusions

The goal of information security is to be able not just to put in place 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. A superficial evaluation of the information security assembly, including security awareness, leads to the lack of feed-back necessary for the decision-making process with regard to the necessity of implementing adequate corrective measures for improving the information security management. In this context, information security policies are adopted on empirical criteria, without being based on a critical assessment of the internal and external factors characteristic to the organization.

According with the results of this research, 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.

In practice, the companies always use a combination of the quantitative and qualitative methods, depending on the characteristics of the organization investigated the degree of uncertainty associated with the method of analysis and risk management. Thus, if all the elements of this analysis (the value of assets, impact severity, frequency threats, effectiveness of controls, uncertainty and probability threat materializes) are expressed in quantitative terms, the process can be characterized as a fully quantitative one. Otherwise, depending on the wording of these measurements, risk management is partly or wholly qualitative one.

Risk assessment information based on the six distinct elements considered in risk management: the value of information assets, threat frequency, and severity vulnerabilities exploitation in the production of threats organizational effectiveness of

risk minimization procedures (controls), their cost, as the level of uncertainty associated with the process information risk management.

The extent to which these variables are measured using independent and objective measurement methods, such as replacement cost value information assets or annual frequency associated with information security threats, risk assessment methodology is considered quantitative. If all six variables are measured quantitatively, the methodology is quantitative. Future research is important because certain events with a negative impact on the objectives to be transformed into opportunities if they are identified early.

References

Armaghan B., Abd Rashid, R. Chaudhry, J. A. (2012). A survey of information security risk analysis methods, Smart Computing Review, vol. 2, no. 1, pp. 79-94, February 2012
Ben-Asher, N., Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51-61.
Landoll D. J., (2010). The security risk assessment handbook: a complete guide for performing security risk assessment, Second Edition, CRC Press, Taylor & Francis Group.
Petrescu, M., Sîrbu, N., Petrescu, A. G.., Braboveanu M., (2012). Security Awareness – Major Piece in the Puzzle of Information Security, Transylvanian Review, Cluj-Napoca.
Rot, A. (2008). IT Risk Assessment: Quantitative and Qualitative Approach, Proceedings of the World Congress on Engineering and Computer Science, WCECS 2008, October 23-24, San Francisco, USA.
Sîrbu, N. (2012). Teză doctorat „Optimizarea deciziei manageriale pe baza analizei riscului în domeniul securităţii informaţiilor", Universitatea Valahia, Târgovişte.
Sicari, S., Rizzardi, A., Grieco, L.A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.
Simmonds, M. (2017). How businesses can navigate the growing tide of ransom ware attacks. Computer Fraud & Security, 3, 9-12.