Bîlcan, Florentina Raluca; Ghibanu, Ionuț Adrian; Bratu, Ion Ionuț et al.

Article

Risk and uncertainty in information society

Provided in Cooperation with:
Dimitrie Cantemir Christian University, Bucharest

Reference: Bîlcan, Florentina Raluca/Ghibanu, Ionuț Adrian et. al. (2019). Risk and uncertainty in information society. In: Academic journal of economic studies 5 (4), S. 126 - 131.

Academic Journal of Economic Studies
Vol. 5, No. 4, December 2019, pp. 126–131
ISSN 2393-4913, ISSN On-line 2457-5836

Risk and Uncertainty in Information Society

Florentina Raluca Bîlcan[1], Ionuț Adrian Ghibanu [2], Ion Ionuț Bratu [3], George Adrian Bîlcan[4]

[1,2,3,4] Valahia University, [1]E-mail: bilcan.florentina.raluca@gmail.com, [2]E-mail: ghibanu.ionut.adrian@gmail.com,
[3]E-mail: bratu.ion.ionut@gmail.com, [4]E-mail: bilcan.george.adrian@gmail.com

Abstract

Uncertainty and risk can be found anywhere, combined in different proportions, so that for any assumed conscious process that takes place in any field of activity, uncertainty cannot be eliminated. This article presents a series of general and specific problems that organizations in the current economic context may face in carrying out their activity, then finding solutions to optimize this activity through the risk minimization models. The results show that a number of tools and models that are currently being applied with great success in organizations have a potential that is still undesirable and could contribute to a greater extent to improving their performance and sustainability.

Keywords

Information society, risk, uncertainty, probability, confidentiality

JEL Codes: D80, D81

Received: 13 October 2019 **Revised: 21 October 2019** **Accepted: 30 October 2019**

1. Introduction and literature review

The new rules of the information society apply both at the economic level, directing the new economy, but also at the political, social, administrative, cultural levels, transforming reality into a new form of virtual perception (Liu *et al.,* 2018). Using the Internet brings many benefits and allows for competitive advantages, but also brings the vulnerability of computer-based systems (Karanja, 2017). Uncertainty and risk can be found anywhere, combined in different proportions that direct attention to the concrete implications they generate in the economic environment (Core, 2015). In the specialized literature, several terms are encountered which refer, from one perspective or another, to the same thing, but without a consensus on the differences of significance between them: risk, uncertainty, probability of occurrence (McQuade, 2006; Winkler, 2010; Krombholz *et al.,* 2015).

However, in the opinion of many authors, the risk is regarded as a phenomenon that comes from circumstances for which the decision maker is able to identify possible events and even the probability of their occurrence, but without being able to specify exactly which of these events will occur effective (Turban and Volonino, 2011; Sarabi *et al*., 2016; Wu *et al*., 2019).

It can be said, therefore, that it comes from the impossibility of accurately assessing what is the possible event, identified as such by the decision maker, which will materialize effectively and determine a certain level of risk. From this point of view, the risk of information security has as main source the instability of the business climate and the inability of the economic agent to counteract in time and without high costs the effects generated by this continuous evolution (He *et al*., 2012). Thus, the relationship between risk and uncertainty is a complex relationship. In contrast to risk, uncertainty is described as the situation in which the decision maker cannot identify all or even any of the possible events to occur and even less to be able to estimate the probability of their occurrence, having the mathematical meaning of an incomplete variable defined (Karim, 2007). Uncertainty involves very vague anticipation of some elements so that no forecast can be made about what is happening.

Each of the three decision-making situations - certainty, risk and uncertainty - is most often defined in relationship with the other two. Such an approach makes it much easier to define the sphere as accurately as possible to understand each concept and its positioning as correct as possible in relation to the others. Depending on the degree to know the evolution and future effects of a particular event, the three concepts can be hierarchical thus: at the extreme the certainty and the uncertainty, respectively, while the risk is placed in an intermediate position.

The adoption of a decision under conditions of uncertainty is characterized by the following elements: the decision maker is not aware of the existence of a problem; the decision maker has inadequate quantitative, qualitative information, which are not relevant; incomplete information that does not allow a complete list of the consequences of a decision to be formulated (Karanja, 2017).

At the same time, many theorists believe that uncertainty has two components: an objective component - objective uncertainty (identified not infrequently with the notion of risk), and a subjective component - subjective uncertainty (Yar, 2006; Peltier, 2010; Holsapplea *et al*., 2014). The subjective character of the uncertainty must be assessed from the perspective of the estimates regarding the occurrence of a risk-generating event and is based on the own assessments or perceptions of the decision maker according to the information available to him at the time, while the objective uncertainty can be assimilated to the situation where the possible results are known and most of those involved in the decision-making process. As for our attempt to measure risk, we lose out view that systematic deviations are disastrous for the result. Anyhow, when faced with uncertainty, we tend to underestimate the risk of doing the same thing as before and overestimate the risk of moving in a new direction. Also, if we find ourselves in conditions of uncertainty and consider that all events have the same probability of occurrence then we can no longer speak of uncertainty (Singer and Friedman, 2014). Privacy and security issues of IoT devices and the communication information has been focussed in research work that gives bits of knowledge into the most essential existing issues of security and protection of the Cloud Computing, Internet of Things and Cloud of Things ideas particularly classification issue (Tiago *et al*., 2014). It is not surprising, under these conditions, that the management of randomness requires without question its prior measurement, and its introduction in the decision equation, affects the quality and accuracy of the estimates regarding the future developments and results of the company.

2. The general and specific problems of organizations in the information society

Over the past several years, the security and machine-learning communities have developed novel techniques for constructing adversarial samples malicious inputs crafted to mislead and therefore corrupt the integrity of systems built on computationally learned models (Skilton and Hovsepian, 2018). With the development of the Internet, cyber-attacks are changing rapidly and the cyber security situation is not optimistic (Arukonda and Sinha, 2015; Karanja, 2017).

Today, the organizations work to achieve a future result in an uncertain situation characterized most often by different degrees of risk (Liu *et al.,* 2018). Changing from random to risk means confronting nature quantifiable of the latter and represents a challenge for companies (McQuade, 2006). The false sense of security of communications amplifies the decision-making act of managers operating in a highly competitive economy and calls for a series of technical solutions designed to reduce the major losses caused by data theft or the insertion of distorted data.

Regardless of the perspective of its approach, it can be considered that the information security risk has three fundamental determinants, between which there are interdependence relations:

- the lack of control (reduced degree of control) over the future evolution of some events, phenomena whose production leads to losses, being risk generators; this absence of the control of reference also to the impossibility of the decision maker to establish "a priori" which result will occur;
- the limited time for making the decision affects the quality and quantity of the information accumulated and generates problems related to understanding the specific nature of each situation and problems to analyze.

Following the analysis of previous studies (Winkler, 2010; Holsapplea *et al*., 2014; Karanja, 2017), three main components must include any attempt to define the information security risk:

- the existence of a potential loss, which can occur in three forms: actual results lower than the anticipated results or which could have been obtained (the actual results being compared with the results of actions, similar decisions or with the other results estimated to be obtained by the decision maker), negative results (actual losses), loss of opportunities;
- the probability of a loss, identified by the decision maker by different methods;
- exposure to loss during the course of an action, which may lead to an increase in the magnitude of the loss or the likelihood of a loss occurring.

When analysing the potential risk from the perspective of economic information security technologies, the following should be taken into account:

- confidentiality - any organization has information that, if disclosed or stolen, could have a significant impact;
- integrity - protection of information against unintentional or accidental changes;
- availability - refers to ensuring that information is accessible to authorized users when and where they need it and in the required form.

Even if all the information security risks in an organization's activity are identified, they cannot be fully included in the risk management program. As these risks will not materialize and their consequences do not all have the same magnitude, it is advisable to make a pre-selection of those who are treated in the next stages. In the evaluation stage of information security risks, the possibility of occurrence of risks and the magnitude of their effects are evaluated.

The most difficult step is to establish the strategy for responding to information security risks. The development of a risk response system represents the action phase within the information security risk management process, in which attempts are made to capitalize on opportunities and diminish negative results. The period in which the information security risk was only recognized as negative effects corresponds to specific practices. These consist of strategies for responding to threats, respectively, avoiding, transferring, mitigating and accepting the information security risk.

What remains after applying the avoidance, transfer and mitigation strategies is the residual risk. This includes the security risks of minor and uncontrollable information, over which no action is possible. In the case of threats, the strategy of accepting the risk of information security is adopted, in which one uses the contingency funds or the risk budgets and the risk is controlled and monitored.

In some cases, organizations seek to identify information security risks, understanding that adding certain risks may have a minimal impact on the overall risk, or in the case of an information security risk transfer strategy, they may reduce the organization's risk. Essentially, managers have realized that information security risks are not absolutely avoidable and that, in fact, informed risk-taking is an additional weapon to gain competitive advantage.

From the point of view of the efforts, the implementation of modern methods for managing information security risks (Liu *et al.,* 2018) determines certain costs:

- the cost of purchasing computer products;
- the cost of providing the specialized labor force in the use of computer products and interpreting the results obtained by using them;
- the cost of ensuring the appropriate framework is a cost attributed to the construction of an office equipped with equipment necessary for the use of computer products;
- cost of advice by specialists, in special situations, when the organization needs guidance, that they can get through their analysis and are useful in the proper use of information technology products.

A strict report on the costs regarding the implementation of the risk analysis management in the information security and the possible losses involved is not conclusive, but it helps to outline a primary image on the necessity of implementing these methods, within the organization management.

In practice, authentication ensures confidentiality, integrity, non-repudiation, availability and protection of information, but risk assessment is very difficult and totally dependent on a specific environment (Landoll, 2010). For instance, as the business needs the different Application Programming Interfaces for the agility of the business, the Cloud is perfect vehicle and provide the service access point for the evolving these in the particular field or domain, which can be maintained and delivered to the specific customers. Cloud computing utilizes data innovation as assistance over the system and can furnish end-clients with incredibly solid calculation ability and colossal memory space with minimal effort.

But, perils of Cloud computing incorporate criminal hacking, unseemly access by rebel directors, and the vulnerability of where information dwells in this present reality where thoughts of security contrast and guidelines change crosswise over national fringes. So as to productively and securely build elements trust relationship in the cloud and cross-mists condition, character the executive's administrations are essential in Cloud computing foundations to validate clients and to help adaptable access control to administrations, in view of User-ID properties (also known as attributes) and past connection archives.

Anyway, regular case of attack is cushion flood where the working framework or programming hangs and uncontrolled organization string that can be utilized to crash a program or to execute noxious code. Programming sellers frequently discharge security updates to address these blemishes; refreshing frameworks with the most recent security updates can alleviate these attacks.

On the other hand, the methods and algorithms for predictive analytics such as regression analysis, machine learning, and neural networks have existed for some time. Recently, the software products have also been integrated into specific applications, such as for campaign management (Turban and Volonino, 2011). As a result of that, the business is relied

upon to develop immensely, determined predominantly by the services that enable clients to reinforcement their records while guaranteeing simple accessibility of documents in instances of hard drive crash.

Withal, access rights may be generated depending on the applications or the systems that support them. The problems could be solved by the security policy adopted by the company, but also by the methods of securing the applied conception and development. As programmers invent more and more security technologies, making it increasingly difficult to exploit technological vulnerabilities, attackers will increasingly refocus on exploiting the human element. Naturally, adopting the recommended security measures requires a significant investment both in time and financial resources.

Therefore, the absence of appropriate security measures exposes businesses to high risks and can prove to be extremely expensive. For that reason, the rapid introduction of advanced technologies in security practices can induce complex effects, sometimes not very well mastered, on policies, strategies and organizations, public or private, in charge of ensuring security. What has changed in recent years is the treatment of the wide variety of information security risk, in a holistic manner, raising the information security risk management to a higher managerial responsibility.

3. Results and discussions

The development of electronic business has led to a new level of security, much maximized. From a technical point of view, precise estimations of the evolution of a certain risk in a short time did not allow the effective counteracting of the influence of the human factor in increasing the vulnerability of the organizations (Andress, 2003; Karanja, 2017). Most decisions regarding the security of information are made in conditions of risk and uncertainty with incomplete knowledge of the various variables, which explains to a lesser or greater extent the differences in approach (Zhang *et al.,* 2018).

Analysing all the general and specific problems of the organizations in the information society, we can observe certain common characteristics of risk definition. First of all, it can be said that the risk derives from uncertainty: the decision is currently taking place and the implementation and the results generated will occur in the future; the uncertainty comes from the ignorance as to which event of the identified ones will occur and at what moment, what will be the real effects and the amplitude of its production. Secondly, the risk of information security involves the idea of potential loss and involves taking measures from the decision maker. The vulnerability of information systems can be mathematically modelled under conditions of objective uncertainty as a function of a particular nature of the event itself, and under conditions of risk as a function of the impact of the event occurring on an organization. In addition to aforementioned vulnerabilities, there are several other vulnerabilities that are also emerging at a rapid rate. For instance, vulnerability was discovered in flash application on windows operating system that was gaining the access to the system with elevated privileges.

Even so, managers' assessments of the future vulnerability of information systems have a predominantly subjective character. In order to better substantiate the decision and reduce the number of strangers with whom it is operated, it is necessary to improve the security of information, in order to analyse a conversion of uncertainty into risk. Essentially, the success of a business depends to a large extent on the options that a manager has when making the decision regarding what risks of information security is willing to accept for a level expected to be realized (Core, 2015). The risk analysis goes through the study of the functional needs of the security and through the determination - depending on the foreseeable consequences of a disaster - of the properties to be insured. Risk assessment involves qualitative and quantitative factors.

In contrast to risk, uncertainty is described as the situation where the decision maker cannot identify all, or even none of the possible cyber-attacks to occur, let alone be able to estimate the probability of their occurrence, having the mathematical meaning of an incomplete variable defined (Weber, 2010). Uncertainty involves very vague anticipation of cyber-attacks, so no forecast can be made about what will happen.

Most often, in practice, the terms of uncertainty and risk, they are used with identical meanings in order to emphasize the difficulty of establishing the exact information security risk and they are associated with the idea of exposure to a potential loss, often the meaning of the two concepts, being reduced in economic practice to the possibility of a situation occurring unfavorable in the future. In other words, when we know the probabilities associated with the occurrence of a particular event and the resulting consequences but we do not know when such an event will occur, we are at risk and when we know neither the consequences nor the probabilities, we have uncertainty.

Identifying the information security risk thus becomes the first step in conducting a business on a conscious, responsible basis, thereby understanding the process by which exposures to potentially harmful factors are continuously and systematically identified (Winkler, 2010). Finding damage after its production is more unpleasant and certainly more expensive than preventing it from occurring. The lack of identification of the potential dangers causes that the losses that can be registered are a surprise for the company and the unconscious retention of some risks is not the happiest initiative for the decision makers. For the protection of information to be effective, we must be able to protect the material that

supports it, the software that processes it, but also the general environment that surrounds it. It is a problem of enterprise in which its general direction is widely involved in the process of prevention and problem solving.

4. Conclusions

The information society allows wide access to information, a new way of working and knowledge, amplifies the occurrence of risk and uncertainty in any organization. Organizations and people are worried about how security and consistency respectability can be kept up in this new condition. Since talking about the risk of information security means waiting for it to be evaluated, and the correctness of quantifying an aggregate size requires approaching information security as a process. The results of the quantifications regarding the risk and the uncertainty we use to make decisions and the managers are responsible for the correctness of the evaluation because they bear the responsibility for both them and the company.

In addition, there is talk of a risk when future events occur produce as a measurable probability, while uncertainty is present, when the probability of the occurrence of future events is indeterminate or incalculable. Since the risk of cyber security can be quantified, organizations can take the necessary measures to protect themselves against the risk (actually converting the risk into uncertainty). For all that, unlike risk, uncertainty cannot be eliminated or insured. Information security risk assessment is necessary because it provides information in choosing the best management tools, but also because it helps to determine the relative importance in the overall context. In this way, situations can be avoided where an entrepreneur concentrates his efforts on risks that are less likely, leaving to segments of the activity exposed to real threats.

Starting from the description of the information security risk, it becomes clear that there are several dimensions that need to be evaluated, namely: probability of occurrence and level of consequences - impact and severity of impact. Regardless of the method of analysis used, uncertainty is more drastic than risk and comes in most cases from the absence of information, from its poor quality or as a result of certain failures of the decision maker's information system.

In conclusion, awareness of risk and uncertainty is not sufficient, neither in economic life nor elsewhere. In the absence of questions about their causes and effects, the perception we have about them may be more important than many other aspects. It is important for each company to determine one acceptable level of risk that he is willing to take. Certain progress has been made in terms of identifying and analysing the security risks of information, but it will take many years to unify security views. Information security risks are the main source of development opportunities, improvement. Higher advantages can be obtained by taking advantage of the opportunities that arise from accepting certain risks. An information security risk management program helps to make much better-informed decisions.

Acknowledgement

This work is supported by project POCU 125040, entitled "Development of the tertiary university education to support the economic growth - PROGRESSIO", co-financed by the European Social Fund under the Human Capital Operational Program 2014-2020.

References

Andress, A. (2003). Surviving Security: How to Integrate People, Process, and Technology. Auerbach Publications, Boca Raton, FL, USA.

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

Core, F (2015). Big data analytics: a managerial perspective, Springer.

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

Holsapplea, C., Lee-Postb, A., & Pakath, R. (2014). A unified foundation for business analytics. Decision Support Systems, 64, 130–141.

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. Information & Computer Security, 25(3), 300-329.

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

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113-122.

Landoll D. J. (2010). The security risk assessment handbook: a complete guide for performing security risk assessment, Second Edition, CRC Press, Taylor & Francis Group.

Liu, Q., Li, P., Zhao, W., Cai, W., Yu S. & Leung, V. C. M. (2018). A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View, in IEEE Access, Vol. 6, pp. 12103-12117.

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

Peltier, T.R. (2010). Information security risk analysis. Third Edition, CRC Press, Taylor & Francis Group, Auerbach Publications.

Sarabi, A., Naghizadeh,P., Liu, Y., & Liu, M. (2016). Risky business: Fine-grained data breach prediction using business profiles. Journal of Cybersecurity, 2(1), 15–28.

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

Skilton, M. & Hovsepian, F. (2018). The 4th industrial revolution. Cham: Palgrave Macmillan.

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.

Turban, E., & Volonino, L. (2011). Information Technology for Management: Improving Strategic and Operational Performance (8th Edition). Danvers, MA: Wiley & Sons.

Weber, R.H. (2010). Internet of Things—New security and privacy challenges. Computer Law and Security Review, 26, 23–30.

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

Wu, Q., Sun, M., Zhou, C. & Zhang, P. (2019). Precise Point Positioning Using Dual-Frequency GNSS Observations on Smartphone. Sensors, 19, 2189.

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

Zhang, Z.-X., Wang, L., & Wang, Y.-M. (2018). An Emergency Decision Making Method for Different Situation Response Based on Game Theory and Prospect Theory. Symmetry, 10, 476.