European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2020.04.75

PEDTR 2019

18th International Scientific Conference "Problems of Enterprise Development: Theory and Practice"

DEVELOPMENT OF INFORMATION RISK MANAGEMENT THEORY

A. V. Korablev (a)*, M. V. Petrushova (b), A. V. Andreev (c)
*Corresponding author

(a) Samara State University of Economics, 443090, Soviet Army Str., 141, Samara, Russia, korablyov.av@yandex.ru
(b) Samara State University of Economics, 443090, Soviet Army Str., 141, Samara, Russia, tyri@yandex.ru
(c) Russian Timiryazev State Agrarian University, 127550, Timiryazevskaya Str., 49, Moscow, Russia, aav3008@mail.ru

Abstract

Authors investigate historically the concept of information risk as a function of the development of management theory. The paper shows how approaches to estimating risk depend on the mathematical apparatus used to quantify risk, ranging from probabilistic mathematical tools to fuzzy inference. In the economic field, managerial decision-making involves the use of asymmetric, incomplete, or restricted information. These negative properties of information result in uncertainty underlying many economic phenomena. That uncertainty is especially significant in the lending sector, the securities market, and the insurance market. Even as the significance of information support grows, modern management techniques are beginning to incorporate a new, risk-oriented approach to managing the collection, processing, storage, and transfer of information. This approach has emerged because of qualitative changes in information management: companies' financial losses from incidents relating to information security have drastically risen, and companies have dramatically increased spend on creating, operating, and improving information technology infrastructure. These changes have taken information technology management to a new level. A transition is underway from ancillary information-security processes to information risk management. To effectively manage information risks, the company must be aware that risk is a complex quantity that is always determined through a combination of several other variables.

Keywords: Information risk, subjective probability, fuzzy sets, risk magnitude, modern information technology.

https://doi.org/10.15405/epsbs.2020.04.75
Corresponding Author: A. V. Korablev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Historically, approaches to assessing and analyzing risk changed depending on the development of management theory. Until the early twentieth century, risk assessment methods developed as part of economic theory, where the concept of risk went hand in hand with the concept of uncertainty. In his 1921 book Risk, Uncertainty, and Profit, the American economist Frank H. Knight (2014) established the distinction between risk and uncertainty. At about the same time, in 1925, Henri Fayol (2013), a French mining engineer who developed a general theory of business administration, described a security function as one of the major management functions. The next stage in developing risk assessment methods was the appearance in 1965 of fuzzy-set theory and the mathematical apparatus of fuzzy inference, proposed by Lotfi A. Zadeh (2015). Researchers from Asia have significantly contributed to the development and formation of fuzzy logic.

In 1993, the US researcher Bart A. Kosko (1999) proved the fuzzy-approximation theorem, according to which any mathematical system can be approximated by a fuzzy logic system. It followed that using natural "if–then" statements and then formalizing them by means of fuzzy-set theory, one could describe, with any desired accuracy, an arbitrary input–output relationship without applying the complex apparatus of differential and integral calculi traditionally used to identify objects in management theory. This prompted wide use of fuzzy-set theory in practice. That is why in recent years, publications have centered on the applied research problems relating to the use of fuzzy-set theory.

The appearance of fuzzy logic in the second half of the twentieth century led to the use of risk assessment methods in analyzing and providing security for social, technical, environmental, and many other systems. That period saw general risk theory begin to develop with increasing intensity and to be used for security applications. It was not until the last quarter of the twentieth century that risk research in this field reached its final shape, prompted by practical security needs relating to data circulation in computer systems.

2. Problem Statement

The development of information security is based on solving applied problems to ensure it. Hence, from the late 1950s through the mid 1990s, security in computer systems—and therefore information risk—was managed by dedicated services responsible for national security. As businesses rapidly went computerized, a need arose for uniform standards for managing security risks. The first method for managing information security was set out in the 1998 British standard BS 7799-2. In 2005, ISO adopted it as an international standard, ISO/IEC 27001:2013. In 2001–2004, ISO also developed ISO/IEC 13335, a series of international standards for managing the security of information and communications technology. Later on, the third and fourth parts of this series, as well NIST 800-30, an American risk management standard, provided the basis for the ISO/IEC 27005: 2008 standard. In 2010, Russia adopted it as a Russian state standard, GOST R ISO/IEC 27005-2010 (Korablev & Petrushova, 2019). Recent publications have focused on managing security risks in modern information technology, such as wireless communication channels, distributed data processing, and cloud technology.

https://doi.org/10.15405/epsbs.2020.04.75
Corresponding Author: A. V. Korablev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

3. Research Questions

The literature does not provide an exact definition for information risk. In ISO 27005, information security risk refers to the potential for exploiting vulnerabilities in the flow of information to cause damage to an organization. BS 7799-3 defines risk as a combination of the probability of an event and its consequence (Geras'kin & Chkhartishvili, 2017). According to the Bank of Russia information security standard STO BR IBBS, risk is an uncertainty that implies the possibility of loss (damage). And Russia's Information and Information Technology and Protection Act defines risk as the probability of harm being caused to the lives or health of citizens, any property of individuals or legal entities, state or municipal property, the environment, or lives or health of animals or plants, considered with the severity of that harm in mind.

There are several approaches to identifying information risks. First, risk is understood as a probable event that can result in violating the properties of information: availability, confidentiality, and integrity. Primary measures for managing information security (information security risks) aim to combat illegal actions by potential attackers. Information risks manifest themselves in corporate information systems, which consist of hardware, software, and organizational management methods. Second, risks cause companies to incur financial losses. For that reason, they are categorized as economic risks. Unlike speculative risks, which can be both positive (e.g., successful stock-exchange speculation) and negative, information security risks are always negative. This classifies them as nonspeculative (net) risks, or probable financial loss events. Therefore, information risk is the danger of loss or damage resulting from the use of information technology by the company.

4. Purpose of the Study

Characterizing risk factors (such as threats, vulnerabilities, and damage) individually does not describe a risk. A discussion of risks should consider risk factors as a whole. Information risks are associated primarily with the vulnerability of information protected and with threats to its security. ISO/IEC 27001, a standard governing information security management, provides the following definitions (Korablev, Petrushova, Pogorelova, & Abrosimov, 2019). An information security threat is the likelihood of an event occurring in which the integrity, availability, and confidentiality of data are compromised. Vulnerability is a weakness in an information system that could be exploited by a threat source to carry out a threat to that system's security. Specialized literature points out that information vulnerability comes in many forms, such as loss, theft, or unauthorized destruction of the information carrier; misrepresentation; information blocked for authorized users; and disclosure. The vulnerability of an information system can occur in one or simultaneously several forms, depending on the occurrence of the information security threats associated with it. Thus, each form of vulnerability is characterized by specific information threats.

5. Research Methods

The magnitude of the information risk associated with the occurrence of a specific vulnerability with regard to a specific information resource can be expressed through the following equation:

$$IR = P_u \times P_v \times LOSS, \quad (1)$$

https://doi.org/10.15405/epsbs.2020.04.75
Corresponding Author: A. V. Korablev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

where IR is the risk magnitude; $P_u$is the probability of a threat; P_v is the probability of the associated vulnerability occurring; and $LOSS$ is the amount of loss.

Threat probability is the likelihood that a threat to an information resource will occur.

When calculating risk in practice, one uses not the mathematical expectation of threat probability but the potential number of attempts to carry out the threat within a limited period. The probability of a vulnerability is the likelihood of a destabilizing effect occurring that involves exploiting the vulnerability to cause damage to an information resource. Estimated quantitative values are used to determine the magnitude of risk, and they are obtainable from expert estimates and forecasts as well as from analysis of statistical data. Generally, loss is expressed in monetary units, and the magnitude of vulnerability varies from 0 to 1.

The magnitude of risk is quantifiable from

$$R_i = P_{yr} \times V_i \times LOSS_i \quad (2)$$

where R_i is the magnitude of the ith risk; P_{yr} is the predicted number of threat occurrence events over a precisely defined period (threat occurrence frequency); $LOSS_i$ is the amount of loss; and V_i is the magnitude of information vulnerability (the probability of this threat occurring that exploits the given form of vulnerability).

To calculate the probability of risk, we need to determine the sum of the overall probabilities of the threat occurring. In practice, an approach is used where the probability of a particular threat to an information resource depends on the status of the user (on a set of access rights or their absence).

$$P_u = 1 - \prod_{i=1}^{n}(1 - P_{ui}), \quad (3)$$

where P_u is the probability of the threat to protected information occurring; P_{ui} is the probability of the threat occurring subject to user status; and n is the number of users. To correlate risk with the associated threat, the overall probability P_u must be multiplied by the magnitude of potential loss from the occurrence of that particular threat.

6. Findings

It is noteworthy that subjective probability theory can be used to identify information risks. The classical concept of probability refers to the relative frequency of an event occurring within the scope of observation. The magnitude of objective probability is obtained by analyzing the multitude of observations that have taken place in the past. Subjective probability is, in turn, a measure of the expert's confidence that the event will actually take place. This probability is used when the information about observations is incomplete or lacking. Given the insufficiency and ambiguity of information, it is difficult for the expert to unequivocally determine the numerical value of subjective probability. In this case, checklists are drawn up in which the expert records answers about the comparative probability of several events (e.g., about the occurrence of security threats).

Most methods for obtaining quantitative subjective probability are based on surveying experts and differ in that they use either finite or infinite sets. For methods using a finite set, probability is estimated for individual events; for methods with an infinite set, distribution functions are used (Korablev, 2016).

https://doi.org/10.15405/epsbs.2020.04.75
Corresponding Author: A. V. Korablev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

The method for direct probability estimation (with a finite set). For each event, A_1,A_2...A_n, the expert indicates the probability of that event occurring. One of the varieties of this method assumes that initially the most probable event is selected and then its probability is estimated. Then the data are removed from the general list, and the expert determines probabilities for the remaining events. The sum of all probabilities should equal 1. The method's drawback is that the expert needs to monitor the sum of the probabilities (Geras'kin, 2018).

The ratio method (with a finite set). In the first step, the expert determines the most probable event and sets the probability P for it. In the second step, the expert determines the ratio of the remaining N probabilities P_i of the remaining i events to the unknown probability P (P_i/P). With the condition $\sum_{i=1}^{N} p_i = 1$ in mind, the expert recalculates the probability P_i.

The variable-interval method (with an infinite set). In this method, the expert must determine an interval on a set of random variables for which the probability of a random variable takes a value in the given interval and is equal to the given value t_0. Here, two equal probabilities are possible: the probability of a random variable is less than t_0; the probability of a random variable is greater than t_0.

Then the expert indicates the value of the random variable t_1 so that the variable divides the range of values greater than t_0 (less than t_0) into two parts with equal probabilities. Then the same steps are repeated for these two parts. The halving is continued until the expert is confident that they will not make a mistake in small intervals. The values obtained for t_0 and the associated probabilities (1/2–t_0; 3/4–t_1; 1/4–t_2; etc.) are graphed, and the points so obtained form a distribution function graph. There are also other methods for determining quantitative subjective probability: the fixed-interval method and the graphical method.

7. Conclusion

Given the above approaches, we can define information risk as the likelihood that, when information technology is used, an event occurs in which properties of information are compromised, causing the company to sustain financial losses. Modern risk management theory is based both on mathematical apparatus (fuzzy-set theory, probability theory) and on the use of information technology in its assessment. The use of fuzzy models in managing security risks is preferable to probability theory because typically in the security field, one's knowledge of the system or process under study is usually insufficient or uncertain; obtaining the required information involves various difficulties or is not possible at all; most of the information comes from expert data or empirical process descriptions; and parameters and input data are not accurate or correctly presented.

References

British standards institute code of practice for information security management (BS 7799/ISO 17799). Retrieved from: http://www.all.net/books/audit/bs7799.html. Accessed: 16.12.2019.

Fayol, H. (2013). *General and industrial management*. New York, N.Y.: Martino Fine Books.

Geras'kin, M. (2018). Modeling reflexion in the non-linear model of the stakelberg three-agent oligopoly for the Russian telecommunication market. *Automation and Remote Control*, *79*(5), 841-859. [in Rus.].

Geras'kin, M., & Chkhartishvili, A. G. (2017). Structural modeling of oligopoly market under the nonlinear functions of demand and agents' costs. *Automation and Remote Control*, *78*(2), 332-348. [in Rus.].

Information security of organizations of the banking system of the Russian Federation (STO BR IBBS). Retrieved from https://cbr.ru/Content/Document/File/46921/st-10-14.pdf Accessed: 17.12.2019.

Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013). Retrieved from https://www.iso.org/standard/54534.html Accessed: 16.12.2019. [in Rus.].

Information technology - Security techniques - Management of information and communications technology security (ISO/IEC 13335). Retrieved from https://www.iso.org/ru/standard/39066.html. Accessed: 17.12.2019.

Information technology - Security techniques - Information security risk management (ISO/IEC 27005). Retrieved from https://www.iso.org/ru/standard/75281.html Accessed: 17.12.2019.

Knight, F. (2014). *Risk uncertainty and profit*. New York, N.Y.: Martino Fine Books.

Korablev, A. V., & Petrushova, M. V. (2019). A fuzzy mathematical model for managing the digital transformation of business processes based on cloud services. *Espacios*, *40*(18), 16.

Korablev, A. V. (2016). The use of cloud technologies in banking. *Journal of Economy and Entrepreneurship*, *8*(73), 463-468. [in Rus.].

Korablev, A. V., Petrushova, M. V., Pogorelova, E. V., & Abrosimov, A. G. (2019). Mathematical model of economical assessment of investments in information provision for the management system of a modern company. In V. Mantulenko (Ed.), *17th International Scientific Conference "Problems of Enterprise Development: Theory and Practice". SHS Web of Conferences, 62* (11002). Les Ulis: EDP Science.

Kosko, B. (1999). *The fuzzy future: From society and science to heaven in a chip*. Boston: Harmony.

National institute of standards and technology special publication 800-39 (NIST SP 800-39). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf Accessed: 13.12.2019.

Zadeh, L. (2015). *Fuzzy sets, fuzzy logic, and fuzzy systems.* London: World Scientific Publishing Company.