Manažment rizika informačných a komunikačných systémov
Risk management of information and communication systems

Zuzana Krátka, Lucia Baková

Abstrakt: Bezpečnosť informačných a komunikačných systémov je pre každý ekonomický subjekt veľmi významná. Cieľom tohto príspevku je analýza rizík informačných a komunikačných systémov a ich manažmentu v súčasnom období.

Abstract: The security of information and communication systems for each economic entity is very significant. The aim of this paper is the analysis of risks to information and communication systems and their management in the current period.

Kľúčové slová: manažment rizika, riziko informačných a komunikačných systémov, kyber poistenie
Keywords: risk management, risk of information and communication systems, cyber insurance

JEL classification: G22, G32

1. Introduction

The value and importance of the information is steadily growing. Information – the knowledge and skills derived from them – are currently the engine of the world economy. With the development of a global network of the internet, the transmission of information over short and long distances became a simple activity. The development has caused a huge amount of information available today, with a relatively low-cost almost anywhere and to anyone. The violent expansion of quantity of information and its availability prompted the development of systems for processing, so called information and communication systems, whose complexity and sophistication is constantly increasing. Information and communication systems use in their operations the information and communication technologies and in terms of security and risks they create linked entity. Information and communication systems we understand as a set of people, technical means and methods, providing collection, transmission, storage and processing of data for the purpose of the creation and presentation of information to meet the needs of users engaged in systems management. Information is data enriched with the relevance and practicality. The concept of information and communication technologies is a set of hardware and software, network elements, and recordable media for the collection, storage, processing and transmission of information (data, text, sound recordings, and images, etc.). To put it simply, the concept of information technology we refer to all of the technical, software and organizational means to work with the information and means of communication between them.

As a result of the rapid development of information technology and digital communications, and also other relevant factors, in particular advances in the process of globalisation, there is a fundamental change in society and its economy. The core of the new economy is made up of just the information and communication systems based on sophisticated information-communication technologies. The economy, which is characterised by intensive usage of global information and communication systems, is referred to in different contexts, as "information", "Internet", "network", "electronic", "digital", "knowledge", "innovative", or "post-industrial" economy. Quite often also referred to as "e-

economy". Economic growth and structural changes here do not primarily depend on raw materials, machinery and methods of their use, but the ability of people to interact with information. Gain a competitive advantage increasingly depends on investments in modern electronic systems, because the speed, quantity and transaction interdependence are incomparably greater than ever before in the history of human society. For this economy, global technology infrastructure is essential, with an emphasis on the application of computer and telecommunications technology, advanced computer and digital literacy, but also appropriate legislative environment.

The introduction and development of sophisticated information and communication systems usually means a substantial increase in the efficiency of that entity. In the era of knowledge-based economies often just the information and the means of processing are the most important assets, of which individual economic operators have and therefore have an interest in their protection.

2. The risk of information and communication systems

Information and communication system is a set of technical (hardware) and software equipment, recordable media, data and personnel used by the entity to manage and transfer information. These tangible and intangible objects are specifically selected and interrelated to each other for the purpose of the collection, processing and storage, generation and distribution, exchange of information and data in a predefined structure and time, for the purpose of the enforcement of decisions, decision support, information and communication. The substantive elements of the information and communication systems are technology, especially computing user forms (PCS, servers, disk arrays) and communications technology (cabling, active and passive network elements). The value of these assets is determined as a general rule of their acquisition value. The intangible elements of the information and communication systems is the software and data. This includes, in particular, operating systems, application programs and programming tools for the Administration and management of the information and communication systems. The most significant value of intangible assets is the data base.

In connection with the information and communication systems and their safety, information-communication asset is an important concept. It is a tangible or intangible object that participates in the functioning and development of the information and communication system. ICT assets can be divided into three main groups:

- data and documentation assets, i.e. databases and data files, data and information, system documentation, user manuals, operating procedures, the agreements on the replacement procedures to be used in the event of failure of the service or system, and the archived information. Data structures represent the greatest value of the information and communication system. Their loss is difficult to be quantified, their value can significantly change, depending on the time;
- software assets, i.e., application software, system software, development tools and utilities, resource libraries and the library executable programs;
- physical assets, i.e., computer equipment (CPUs, monitors, modems, laptops, etc.), communication equipment (routers, fax devices, etc.), magnetic media (tapes, floppy, HDD), other technical equipment (power supplies, air conditioning units, UPS), furniture and the like.

The Risk of information and communication system can be understood as a function of the probability with which occurs through the action of a specific threat to disrupt the confidentiality, integrity and availability of information within the information and communication system as a result of damage to or destruction of the information and communication assets and the amount of potential damage. The threat (Thread) is a fact or an event, which may cause damage to or destruction of the information-communications assets. This threat may be a person (employee, external or temporary worker, hacker, etc.), natural disaster (water, fire, earthquake, etc.), the impact of technology (equipment failure, failure or fluctuation of electrical power, roads, communication, etc.), and others. Damages arising from errors of techniques or natural disasters can be detected quite easily. More complicated situation arises during illegal leak of information, which is hard to prove and the operator of information and communication system is not interested in negative publicity. Such revelations usually do not get to the public.

The security of information and communication systems can be defined with three essential requirements:

- confidentiality, i.e. protection against disclosure of information
- integrity, i.e. protection against unauthorized modification
- availability, i.e. protection against unauthorized refusal or inability to provide information services.

These essential requirements are the same for all information and communication systems. Their mutual balance is, however, dependent on the requirements defined for a specific system. For example, confidentiality will prevail over the integrity of military systems, the integrity of the data will take precedence in large-scale information libraries, and so on.

Vulnerability of the information and communication system is the lack, a weak spot all over the security of the system, which can be exploited by a threat in such a way that will cause a damage to or destruction of the information and communication assets. Major damages can cause disruption of the confidentiality, integrity, or availability of the so called sensitive data and information, therefore, they require special protection. It is all about personal information (phone numbers, addresses, etc.), data protected according to the law on the State and professional secrecy and confidential commercial information – data about accounts, concluded contracts, the database of clients, etc.

In terms of the literature, some authors distinguish two separate groups in risks of information and communication systems. The first are the risks resulting from the programming and technical equipment and the increasing dependence on these systems. The second form is called Cyber risks, linked to the use of the Internet and include, in particular, damage, modification or theft of data by unauthorized persons. This kind of risk is closely linked to the so-called security holes in systems. A security hole is a tear or weakness in the design and implementation of hardware and software, network equipment or computer systems. Security holes can be intentionally or unintentionally used to influence the operational activities of the economic entity, assets or personnel. Cyber risk is then a combination of the likelihood that the security hole will be in the system, either intentionally or unintentionally, exploited by the attackers, and according to the extent of the injury made within the framework of the company assets or personnel may result in loss of credibility, integrity and performance. The main perpetrators of these crimes are called the hackers, who may act as individuals, or be integrated in organised crime or terrorist organizations. To carry

out such acts generally so called malicious software are used, namely, computer viruses, worms, Trojan horses and the like, which can infect your hard drive and cause enormous losses.

In addition to the above risks in the context of globalization, the growing interconnection of the economic operators and their dependence on information and communication systems, failure of computer networks seems like a huge risk. Their consequences can be devastating, including damage to the trading on the stock exchanges, the collapse of the internet banking, the collapse of email communications, the unavailability of the online shops, portals, the unavailability of public administration, and so on. Although it is possible to redirect the connection in case of failure, the large volume of transmitted data may lead to deterioration in quality, or complete interruption of services.

3. Risk management of information and communication systems

With the rapid development of information and communication systems increases the possibility of their misuse. The more accelerated developments in this area, the more aggressive competitive environment, and the shorter time the failure of information and communication systems may cause irreparable damage. Companies are missing out on great resources, whether as a result of random failures of the information and communication systems, loss of data or other random incidents. There are also considerable damages as a result of deliberate action by employees, or third parties, in order to undermine or cause harm to information and communication system.

Risk management of information and communication systems is to be understood as a purposeful process of selection and application of control and remedial measures based on the assessed risks, taking into account economic, technical, political, and social opportunities and, where appropriate, taking into account the effects of other solutions. Very important is the right decision on financial risk coverage, thus ensuring the financing of any commitments arising from the risk assessment carried out. In general, the least recommended form of financial risk coverage is relying on ex post obtained foreign sources, which can be in case of need very expensive or entirely unavailable.

The aim of active risk management of economic operator is to reduce the risk and its impact on the economic stability of this entity. A prerequisite for any action in the context of risk management is being aware of the existence of the risk and to recognize it in a timely manner. Risk management of information and communication systems is the process by which it is possible to determine, control and limit the impact of random events – threats. It contains of the identification, analysis and assessment of risk, or the implementation, testing and operation of safety. Risk Assessment is the process of evaluation of the risks involved in the information and communication system in order to reflect the level of risk to which the system is exposed. The correct assessment of risk information and communication systems ascertains whether there are adequate security measures.

Dangers and threats to information and communication systems and the risks associated with them can be managed effectively, in order to reduce the likelihood of their occurrence, and mitigate the impact of serious damage and losses to entities using information and communication systems.The need to address the issue of the security of information and communications technologies and systems is becoming more urgent. There is a relatively new discipline in the field of management which is constantly developing faster – information security management. Information security means protecting information during their creation, processing, storage, transmission and disposal of, and through logical, technical,

physical and organizational measures that counteract the loss of confidentiality, integrity and availability.

The main factors on which to focus attention in the context of information security are:

- persons interested in systems, including users, administrators, managers and staff of technical and programme support,
- technical equipment, including work stations, servers, input-output devices and mobile computing devices,
- network, including local and global networks, communication channels,
- software, including operating systems, corporate applications and specialized applications,
- management system, including procedures, processes, activities, and ethical principles.

It is not possible to completely ensure the security of information and communication systems, and the effort to advance towards a high security is disproportionately costly. In combination with the appropriate insurance it is possible to eliminate optimally the potential risks from information and communication systems.

Offer of insurance products providing a partial transfer of the financial consequences of the implementation of the ICS is constantly expanding. There is another term "cyber insurance", which is also used. The aim of the insurance is to reduce risk by providing advanced ICS cyber insurance coverage compared with traditional insurance products. This extended coverage insurance covers the financial consequences of the attacks of viruses, interruption to business caused by the attacks on the security of ICS, penetration into the enterprise network, damage and loss of integrity and confidentiality of the data, and other violations of company security policies with respect to information and communication technologies. Insurance protection in cyber insurance covers accidental damage to the insured ICS and the resulting financial losses, the deliberate damage caused by insured by a third party or your own employees, and also to the liability for damage caused by its own ICS to a third person.

Demand in the market for insurance coverage of risk-up ICS

- ICS, users who are especially interested in coverage of losses incurred by the interruption of services and costs for data security, etc.,
- service providers (software companies, systems integrators, and service organizations, outsourcing companies) who are interested in coverage for damage caused by the trading partner and the client in respect of the liability for the services provided, etc.,
- service providers on their own servers, who are interested in both the cover
- own damage, the coverage for damage, both on third parties (clients) in respect of the liability.

Cyber insurance is a very young industry insurance- there is a sharp development, which is taking place with sudden and radical changes. Therefore, the acquisition of cyber insurance is currently a fairly complicated affair. Insurance with the insurer that has entered into a contract for cyber insurance, is derived from its levels of activity on the Internet, of the type and nature of its assets and a range of online Internet transactions, which wishes to secure.

The main barriers for the development of cyber insurance are currently in particular:

- lack of historical data necessary for the exact calculation of risk level derived therefrom premium rates,
- the lack of coverage for this type of risk premiums,
- the reluctance of companies to publish information about security incidents,
- undefined and ambiguous terminology in this field,
- legislative resolution of a level of responsibility in dealing with complex hierarchical stages of fault in the ICS are quite common,
- the absence of a standardized form of insurance policies for this type of risk,
- the amount of insurance exclusions that insurers can apply in insurance contracts.

ICS insurance risks can be for a variety of businesses very elegant solution to the problem of security of information assets, but the world is not yet very advanced, and it should be seen as a trend, which is likely to be a significant development starting in the next few years. There are several factors driving the growth of the demand for insurance cover ICS risks:

- management of the whole production, economic and logistical processes of economic operators through ICS,
- acceleration of production processes, where still shorter interrupt causes great harm to the operator and his partner,
- a huge competition, as a result of power failure causes the company will lose many clients,
- electronic data interchange gives the possibility of their misuse or theft during the transmission,
- professional and technical equipment of potential pests,
- as a result of outsourcing, company provides part of their information to other entities.

4. Conclusion

Operators in the various sectors of the economy are increasingly investing in its information and communications assets. However, there also is constantly increasing the number of security threats and the constant attacks on the ICT assets. It is therefore very important to pay attention to the risk management of information and communication systems.

To quantify the risk associated with information and communication systems is very complicated. The success of the implementation of the management of the security of information systems and the management of the risks associated with their operation in the first place is given to the degree of understanding of the risks that threaten their correct identification and assessment and of course the choice of the correct methods of reduction.

Although the initial experience with the introduction of insurance risk into practice have been associated with a number of complications of ICS, many of which still are not fully resolved, the insurance industry holds huge potential. Insurance companies are already aware that insurance is not only a theoretical concept of cyber that was formed in the minds of IT specialists and actuaries, but it is a product that is requested by the economic reality. The insurance industry has enormous potential, and therefore the insurance companies hold

an intense effort to be able to manage and resolve problems with the ICS insurance risk as quickly as possible.

Literature

MOLNÁR, Z. 1992. *Moderní metody řízení informačních systému*. Praha : Grada. 347 s. ISBN 80-85623-07-2.

STRNÁD, O. 2002. *Manažment bezpečnosti IT*. Bratislava: Vydavateľstvo STU v Bratislave. ISBN: 80-227-1696-0.

THE WORLD BANK GROUP. 2002. *Information and Communication Technologies – A world bank group strategy*. [citované dňa 2. 11. 2014]. [online]. Dostupné z <http://siteresources.worldbank.org/INTINFNETWORK/Resources/ict.pdf>.

WILLIAM YURCIK, W. – DOSS, D. 2002. *Cyberinsurance: A market solution to the internet security market failure*. In WEIS, Berkeley, CA. Dostupné online: http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurit%y/

Author's address:

Mgr. Ing. Zuzana KRÁTKA, PhD.
Institute of Management of the Slovak University of Technology
Vazovova 5, 812 43 Bratislava
e-mail: zuzana.kratka@stuba.sk

Ing. Lucia BAKOVÁ, MB.
Institute of Industrial Engineering and Management, Faculty of Materials Science and Technology of the Slovak University of Technology
Paulínska 16, 917 24 Trnava
e-mail: lucia.bakova@stuba.sk