UDC 368.025.31

Ryszard Pukala
PhD (Economics), Director, Institute of Economy and Management,
State Higher School of Technology and Economics, Jaroslaw, Poland
16 Czarnieckiego Str., Jaroslaw, 37-500, Poland
ryszard.pukala@interia.pl

INSURANCE AS A TOOL TO LIMIT CORPORATE FINANCIAL LOSSES RESULTED BY IT RISK MATERIALIZATION

Abstract. The issues discussed in this article concern the usage of insurance as a tool for limiting corporate financial losses arising from IT risk materialization. The article presents possible threats for the security of IT systems used by enterprises. Quantitative and qualitative methods for estimating IT risk have been presented, as well as insurance products have been selected that can be applied by the enterprises to enhance protection against losses resulted by IT risk. The article also draws attention to benefits which arise from efficient tools for the management of IT systems' security implementation and usage of insurance as a tool for limiting risk in the enterprises development under volatile market conditions.
Keywords: IT risk; cyber-attack; risk transfer; insurance; financial losses.
JEL Classification: G22, G32

Ryszard Pukala
Dr. (ekonomia), Dyrektor Instytutu Ekonomii i Zarządzania,
Państwowa Wyższa Szkoła Techniczno-Ekonomiczna w Jarosławiu, Polska
UBEZPIECZENIE JAKO NARZĘDZIE OGRANICZENIA STRAT FINANSOWYCH PRZEDSIĘBIORSTWA, POWSTAŁYCH W WYNIKU MATERIALIZACJI RYZYKA INFORMATYCZNEGO
Streszczenie. Problematyka omawiana w artykule dotyczy wykorzystania ubezpieczeń jako narzędzia ograniczenia strat finansowych przedsiębiorstw powstałych w wyniku wystąpienia ryzyka informatycznego. Zostały przedstawione możliwe zagrożenia dla bezpieczeństwa systemów informatycznych wykorzystywanych przez przedsiębiorstwa. Zaprezentowano wybrane ilościowe i jakościowe metody oszacowania ryzyka informatycznego. Zostały także przedstawione wybrane produkty ubezpieczeniowe, które mogą być wykorzystywane przez przedsiębiorstwa w przypadku ochrony przed stratami wynikającymi z ryzyka IT. Zwrócono także uwagę na korzyści, jakie stwarza wykorzystanie skutecznych narzędzi zarządzania ryzykiem bezpieczeństwa systemów IT i wykorzystania ubezpieczeń jako narzędzia jego ograniczenia w rozwoju przedsiębiorstw w zmieniających się warunkach rynkowych.
Słowa kluczowe: ryzyko informatyczne; cyberatak; transfer ryzyka; ubezpieczenie; straty finansowe.

Ришард Пукала
PhD (экон.), директор, Институт экономики и менеджмента,
Государственная Высшая технико-экономическая школа им. о.Бронислава Маркевича, Ярослав, Польша
СТРАХОВАНИЕ КАК ИНСТРУМЕНТ СНИЖЕНИЯ ФИНАНСОВЫХ ПОТЕРЬ ПРЕДПРИЯТИЯ, ВОЗНИКШИХ В РЕЗУЛЬТАТЕ МАТЕРИАЛИЗАЦИИ ИНФОРМАЦИОННОГО РИСКА
Аннотация. В данной статье раскрывается тема использования страхования как инструмента сокращения финансовых потерь предприятия, возникших в результате IT-риска. Описаны возможные виды рисков безопасности информационных систем, раскрыты количественные и качественные методы оценки информационного риска. Автором также представлены отдельные страховые продукты, которыми могут пользоваться предприятия для защиты от возможных убытков, связанных с IT-рисками. Должное внимание уделено анализу преимуществ, которые получают предприятия за счет внедрения эффективных инструментов управления рисками для безопасности IT-систем и использования страхования как инструмента уменьшения финансовых потерь в изменяющихся рыночных условиях.
Ключевые слова: информационный риск, кибератака, передача риска, страхование, финансовые убытки.

Ришард Пукала
PhD (екон.), директор, Інститут економіки та менеджменту,
Державна Вища техніко-економічна школа ім. о.Броніслава Маркевича, Ярослав, Польща
СТРАХУВАННЯ ЯК ІНСТРУМЕНТ ЗНИЖЕННЯ КОРПОРАТИВНИХ ФІНАНСОВИХ ЗБИТКІВ, СПРИЧИНЕНИХ МАТЕРІАЛІЗАЦІЄЮ ІНФОРМАЦІЙНОГО РИЗИКУ
Анотація. У статті розкривається тема використання страхування як інструменту зменшення фінансових втрат підприємства, що виникли внаслідок IT-ризику. Окреслено можливі види ризиків безпеки інформаційних систем, розкрито кількісні та якісні методи оцінки інформаційного ризику. Автором представлено окремі страхові продукти, якими можуть послуговуватися підприємства для захисту від імовірних збитків, пов'язаних з інформаційними ризиками. Приділено також належну увагу аналізу переваг, які отримують підприємства завдяки впровадженню ефективних інструментів управління ризиками для безпеки IT-систем і використанню страхування як інструменту скорочення фінансових втрат підприємств у мінливих ринкових умовах.
Ключові слова: IT-ризик, кібератака, передача ризику, страхування, фінансові втрати.

Introduction. Provision of IT security is one of the key tasks for each enterprise under today's extremely competitive economic conditions. It is particularly significant in the times of rapid development of information and telecommunication systems and growing acceptance for using these media as distribution channels for products and services, which poses new challenges as regards the development of own data processing systems and, in particular, their robustness and resiliency. Following Grzebyk M. (2010) [1], we need to stress that as part of intensified globalization and consolidation processes more and more enterprises perform their operational activity not only on local and regional markets, but also on the global scale. Ever larger territorial networks, an expanding assortment of products and operational innovativeness bring about increased risks arising from possible actions aimed at destabilizing IT systems in stock, which can result in reputation damage and

considerable financial losses. In this context we need to emphasize a growing significance of risk management in enterprises, which is aimed at limiting losses related to events that disorganize the company's work. Risk transfer tools used by enterprises, particularly an insurance policy, gain significance in this perspective. However, it is worth mentioning that insurance should not substitute a corporate risk management process. It can only be an element that supplements or optimizes actions undertaken with a goal to minimize losses that can arise from an event that threatens the effectiveness of IT systems' operation. The selection of a method that will protect these systems from IT risks should be justified by economic balance, since only then it can fulfil its optimization roles and constitute an efficient risk limiting tool.

Brief Literature Review. Efficient IT risk management in enterprises as well as the utilization of insurance as a risk limiting tool are subjects of analyses in many countries. One of the first scientists to deal with these issues was Courtney R. H. (1980), who as early as in 1980s worked out a complete methodology for designing security solutions for IT systems. These solutions were later modified and modernized by, among others, Fisher M. (1994) [2] and Parker D. B. (1981) [3]. In Poland, we have important publications describing the issue of risk by, among others, Jajuga K. (2008) [4], Kreft K. (2013) [5] and Szczepankiewicz P. (2006) [6] as well as studies related to the use of insurances in the field of optimizing corporate activity by Monkiewicz J. & Hadyniak B. (2010) [7], and Gasiorkiewicz L. (2010) [8].

The purpose of the article is to analyze the possibility of using a range of insurances available on the market as a tool for limiting corporate financial losses that occur as a result of IT risk materialization.

Results. According to most recent Global Risk 2014 report prepared by the World Economic Forum [9], the following global risks have been recognized as most probable in five key areas (economic, environmental, geopolitical, social and technological):

- financial crisis (economic),
- extreme weather conditions (environmental),
- global authority crisis (geopolitical),
- food crisis (social),
- disruptions of IT infrastructure (technological).

The following risks are enumerated as the ones having the greatest impact on the economy:

- fiscal crisis (economic),
- climate change (environmental),
- water crisis (environmental),
- unemployment and underemployment (economic),
- IT systems failures (technological).

We need to note here that technological risks, particularly IT infrastructure disruptions, massive-scale cyber attacks and massive-scale data thefts represent a very important aspect of providing operational security to entities and market infrastructure. It is clear that every organization that stores client data, performs online sale and provides online services or even promotes itself online, is exposed to cyber-risks. Here it is worth defining a cyber-risk, which means a risk that stems from the use and transmission of electronic data. The risk includes physical damage caused by cyber-attacks, data loss or damage and ensuing financial results, frauds resulting from data abuse as well as obligations resulting from the failure to observe availability, integrity and confidentiality of digital information storage. A precise definition of IT risk is extremely important in the context of determining enterprise's operational areas where actions aimed at risk limitation are possible to undertake. Until recently cyber-area was relatively immune to attacks, however the progress in the field of information and communication technologies as well as their broader use in all segments of operation has made a possible threat of attacks more tangible. Suffice to look at Figure 1 below to see how many areas are prone to potential attacks.

It is known to all enterprises interested in limiting operational risk that such a broad spectrum of multi-layer threats increases the significance of protection against cyber-attacks by implementing risk management tools that take account of such threats. We need to bear in mind though, that every entity may create its own risk management methodology adapted to the needs and specificity of operations [10]. Depending on the scale and complexity of operations, the risk management process in the IT area can be: formal or informal, objectively measurable or subjective, intrinsic to a given entity or centrally managed at the organisation's strategic level.

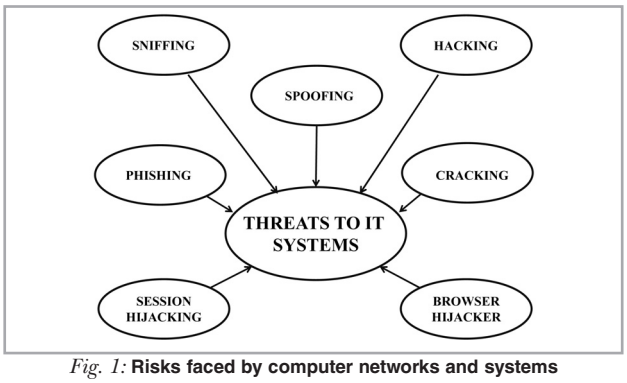

Fig. 1: **Risks faced by computer networks and systems**
Source: Own research

Despite a multitude of solutions, this process should correspond to an entity's culture, management methods and objectives. The tasks of managerial staff or persons responsible for risk management mechanisms include checking whether the selected methodology takes account of all aspects, is sufficient as far as a type of operation is concerned and to what extent it is understood by key groups or particular employees involved. When it comes to risk management in the field of computer networks and systems used by an enterprise, it consists in creating: a security policy for IT systems, rules of access to resources, norms, recommendations and good practices concerning security, analysis procedures related to threats to security, procedures for responding to events of security violation.

An important group of factors directly related to operational security of computer systems includes: determination of security classes for IT systems, monitoring of protection status, monitoring of transmitted data, updating of operating systems and applications, defining authentication mechanisms and authorisation of services and users.

Estimation of risks for IT systems is indispensable to make efficient decisions concerning security, including a potential risk transfer. To this end, we can make use of a quantitative or a qualitative method. As regards the quantitative method, the value of risk is expressed as a foreseeable volume of losses related to a given type of risk, in monetary terms. Here we can utilize Courtney's concept basing on integrity, confidentiality and availability in IT systems, presented by Federal Information Processing Standards Publication «FIPS65 – Guideline for Automatic Data Processing Risk Analysis» [11], according to which the volume of risk for a given IT system can be expressed as an Annual Loss Exposure (ALE, 1):

$$ALE = SLE * ARO, \quad (1)$$

where SLE – Single Loss Expectancy, which is a volume of foreseeable loss resulting from a single loss event, expressed in monetary terms; ARO – Annualized Rate of Occurrence, which is an estimated frequency of a loss event.

Popularity of risk estimation based on Courtney's method regarding IT systems results from the simplicity of approach and a certain degree of intuition at calculating ALE. According to this method, groups of risks that make potential losses calculable include: accidental data disclosure, accidental data modification, and accidental data removal, and deliberate data disclosure, deliberate data modification, deliberate data removal.

We need to emphasize that it is very difficult to precisely estimate risk for IT systems due to the impossibility to obtain all accurate data. Some of them are very hard to parameterize, e.g. loss of data confidentiality. In this case it is legitimate to

determine the impact of information on the execution of a given business process and its significance to an enterprise. It is equally hard to express the loss of good image or credibility among clients of a given enterprise in monetary terms.

Qualitative IT risk analysis methods are based on such information security criteria, as: confidentiality, availability, integrity.

A complete risk analysis can be performed separately for each of the abovementioned categories, while it is crucial to determine incidence for every single risk by using a predefined scale that can be different for every information group. We need to allocate numerical values to each adopted scale and, following the formula (2), we can calculate a qualitative risk value [7]:

$$R = W * F * V, \quad (2)$$

where R – qualitative risk value; W – information loss value; F – risk incidence; V – vulnerability of a given IT resource to a given risk.

On the basis of quantitative and qualitative IT risk volume analysis we can determine an economic efficiency of risk management. It is analysed from the angle of minimizing security costs and risk expressed in monetary terms – see Figure 2.

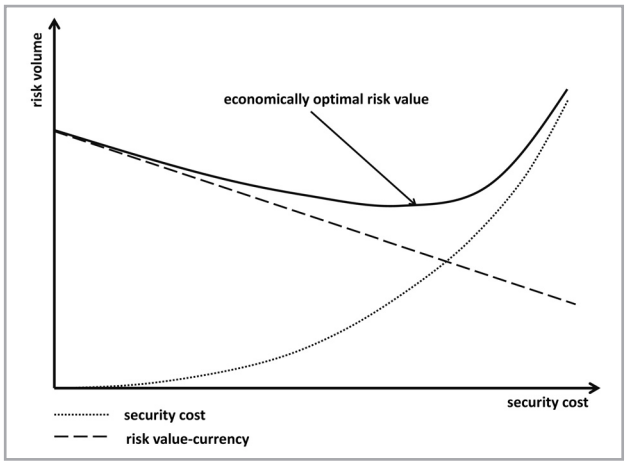

Fig. 2: **Interdependence of security cost and risk expressed in currency unit**
Source: Kreft K. Zarzadzanie ryzykiem IT [5]

Economically optimal risk volume can be determined on the basis of marginal security cost and marginal risk. Marginal security cost can be determined according to the formula below (3) [7]:

$$MSC(i) = SC(i+1) - SC(i), \quad (3)$$

where MSC – Marginal Safeguard Cost; $SC(i)$ – security cost.

On the other hand, Marginal Risk Value-Currency can be determined on the basis of this correlation (4) [7]:

$$MRVC(i) = RVC(i) - RVC(i+1), \quad (4)$$

where $MRVC$ – Marginal Risk Value-Currency; $RVC(i)$ – Risk Value-Currency.

Economically optimal risk value for an IT system can thus be determined on the basis of this correlation (5) [7]:

$$MSC(i) = MRVC(i). \quad (5)$$

This condition is consistent with the assumption of minimizing security cost and risk value-currency.

Despite its complexity, risk analysis for an IT system should answer the question to what extent the tools that serve the purpose of protecting an enterprise from IT risk materialization are efficient and optimal as regards costs. It is extremely important when deciding on a potential risk transfer, e.g. in the form of an insurance policy, as it is justified only if it generates smaller costs compared to costs of implementing and maintaining a security measure.

We need to stress that by making use of an insurance instrument enterprises transfer the risk of expenditure related to counteracting the effects of losses, thus gaining more operational stability in this way. It is important for all types of enterprises, since owing to insurance they can concentrate on the execution of their main objectives. By transferring risk by means of insurance, they do not need to worry that operational activity they undertake will not be executed due to materialization of insured IT risk [12]. Moreover, by eliminating the need to tie-up capital to cover potential losses, insurance allows a broader scope of investing, a more confident execution of innovative investment undertakings, implementation of innovative solutions, optimization of operations, i.e. a more diverse development. Having the feeling of financial security resulting from concluded insurance contracts, company management board is also more willing to make risky decisions, which can bring about additional financial profits or strengthen the company's competitive advantage [13]. Making use of insurance tools has one more very important value: development of a company requires a constant inflow of financial resources allocated to its operational activities and further development. Own funds are often insufficient to finance executed undertakings and it is often necessary to make use of external funding [14]. It is easier and often cheaper to obtain such external funding in the case of an enterprise whose operational risk, including risks related to the use of IT systems, has been insured.

A decision to retain or transfer the risk depends on a number of strategic decisions related to company management, the most important of which are the following: legal, economic and social limitations, level of risk control applied, value and quality of an insurance service, tax burdens, and alternative methods of limiting and transferring risk.

Therefore, a decision concerning the selection of a specific type of insurance derives from the demand for protection and from specificity of operations. Insurance companies offer a broad range of diverse products or packages that can be adjusted to individual needs of a company – see Table.

IT system protection programmes offered by insurance companies can form a basis for a comprehensive protection of corporate interests in the face of risks. Their main aim is to minimize potential financial losses arising from an event. The range of protection is very broad here, particularly in the framework of CEI programme. However, we need to emphasize that due to each enterprise's specificity, the selection of insurance protection should be preceded by internal analysis of its costs and risk. We also need to bear in mind that the insurances offered often provide for exclusion of liability, which can make protection illusory for an enterprise that has failed to verify the degree of protection before an event. Therefore, insurance should constitute one of the many elements of the risk management process concerning corporate IT systems.

Conclusions. When analyzing the use of insurances as a tool for limiting risk for corporate IT systems security, it is optimal to use both quantitative and qualitative risk evaluation tools. Such approach enables us to precisely determine IT risk level for a given entity and, in consequence, to perform effective risk management. It is also important to elaborate clear risk management procedures, which certainly leads to a better use of resources and enhances employee, client and society's trust in a given enterprise. Another issue is to skilfully use insurance as an IT risk transfer tool, since many entities utilize them to an insufficient degree, which in turn considerably limits optimization possibilities.

Taking a closer look at the issue of corporate IT risk management and insurance application as a tool for limiting financial losses, it becomes evident that these tools are very efficient when it comes to the optimization of corporate operational activity of an enterprise. Application of these instruments is extremely important under intensified market competition and in the reality of growing innovation of business activities. To gain market advantage, companies should be foresighted, dynamic

Tab. : **Selected insurance programmes that protect corporate interests in case of IT risk materialization**

Insurance	Scope of insurance protection
Cyber Edge Insurance	Allows limiting severe consequences of data security violation. Personal or commercial data spill or loss can result in financial penalties and can contribute to the damage of reputation. Cyber-attacks can lead to the disability of servers and consequently to the loss of client trust and financial losses. The following insurance options can be distinguished:
	1. Responsibility for personal data and commercial information Coverage of financial consequences of a loss or illegal use of client or employee data or commercial information spill.
	2. Crisis management Coverage of crisis management costs related to a cyber-attack, including services provided by IT specialists who manage a cyber-risk, remuneration for lawyers and PR consultants, whose task is to reconstruct the image of a company or an individual. The insurance also covers the costs of an IT investigation after the data security violation as well as necessary notification costs related to persons whose data may have been disclosed as a result of a spill.
	3. Administrative proceedings Coverage of legal counselling costs related to proceedings carried out by an authority competent for data security and storage oversight (Inspector General for Personal Data Protection) as well as administrative penalties imposed by a competent authority.
	4. Electronic data Coverage of costs of electronic data recovery or reconstruction.
	5. Network disruptions Coverage of costs of the loss of income due to the Insured Party's network disruption as a result of data security violation.
	6. Multimedia activity Coverage of damages and costs of legal defence due to violation of third party's intellectual property, in relation to digitally transmitted content.
	7. Blackmail attempt Coverage of costs of independent advisers in order to determine blackmail circumstances and the amount of ransom for the third party who threatens to reveal confidential information illegally obtained from the Insured Party's databases.
Computer Crime Policy	The insurance covers risks related to electronic collection, storage, processing and transfer of information, the loss of which could lead to company's losses.
Business Interruption Insurance	The scope of insurance covers losses resulting from temporary suspension of activities caused by a fortuitous event, which in consequence leads to a turnover decline and cost increase, both of which disorganize a proper functioning of a company.
Professional Indemnity Insurance	The insurance covers third party claims (mostly clients) related to workers' errors and mistakes that occurred during the provision of a service to a contracting entity. Usually, the insurance also covers a loss, damage or theft of client data or documents as well as money belonging to clients.

Source: Own research

and optimally use available optimization measures. IT risk management and protection in the form of an optimally tailored policy can become an important source of support for a company that is translatable into market success.

References

1. Grzebyk, M. (2010). Determinants influencing the competitiveness of local government units. *Economic Development and Management of Regions* (pp. 95-98). Hradec Kralove, Czech Republic.
2. Baskerville, R. (1994). Information Systems Security Design Methods: Implications for Information Systems Development. *Computing Surveys, 25*(4), 375-414.
3. Parker, D. B. (1981). *Computer Security Management.* Reston, VA: Reston Publishing Company Inc.
4. Jajuga, K. (2008). *Zarzadzanie ryzykiem.* Warsaw: Wydawnictwo Naukowe PWN (in Polish).
5. Kreft, K. (2013). *Zarzadzanie ryzykiem IT.* Gdansk: Uniwersytet Gdanski, Studia i Materialy Instytutu Transportu i Handlu Morskiego. Retrieved from http://studiaimaterialy.pl/wp-content/uploads/ 2013/07/ZN-2012-ITiHM-KKreft.pdf (in Polish).
6. Szczepankiewicz, P. (2006). Analiza ryzyka w srodowisku informatycznym do celow zarzadzania ryzykiem operacyjnym. *Monitor Rachunkowosci i Finansow, 6.* Retrieved from http://www.mrf.pl/index.php?mod=m_artykuly&cid=89&id=3 (in Polish).
7. Hadyniak, B., & Monkiewicz, J. (2010). *Ubezpieczenia w zarzadzaniu ryzykiem przedsiebiorstwa* Tom 1: Podstawy. Warsaw: Poltext (in Polish).
8. Gasiorkiewicz, L., & Monkiewicz, J. (2010). *Ubezpieczenia w zarzadzaniu ryzykiem przedsiebiorstwa* Tom 2: Zastosowania. Warsaw: Poltext (in Polish).
9. World Economic Forum, Committed to Improving the State of the World (2014). *Global Risks 2014.* Retrieved from http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf
10. Grzebyk, M. (2012). Clusters-new possibilities of development of enterprises. *Economic Development and Management of Regions.* Part II (pp. 71-76). Hradec Kralove, Czech Republic.
11. U.S. Department of Commerce, National Bureau of Standards (1979). *Federal Information Processing Standards Publication 65: Guideline for Automatic Data Processing Risk Analysis.* Retrieved from https://www.ncjrs.gov/pdffiles1/Digitization/68759NCJRS.pdf
12. Pukala, R. (2012). Risk and Insurance Management in an Enterprise. In A. Malina, R. Oczkowska, & T. Rojek (Eds.). *Knowledge Economy Society. Dilemmas of the contemporary management* (pp. 527-544). Cracow: University of Economics, Foundation of the Cracow University of Economics.
13. Williams, A. C. Jr., Smith, M. L., & Young, P. C. (2002). *Zarzadzanie ryzykiem a ubezpieczenia* (Trans. from Eng.). Warsaw: Wydawnictwo Naukowe PWN (in Polish).
14. Pukala, R. (2013). Efficient insurance protection management as a determinant of micro and small enterprises operation risk limiting. *Ekonomicnij Casopis-XXI (Economic Annals-XXI), 9-10*(1), 67-70.

Received 04.05.2014