METHODS FOR THE IDENTIFICATION OF CYBER RISKS: AN ANALYSIS BASED ON PATENT DATA

Lyubov Klapkiv[1], Yurij Klapkiv[2]

Abstract: The problem of fast-rising cyber-risks become very important in the era of the Fourth Industrial Revolution. Cyber-risks cause not only high losses but also break the chain of economic relations between companies and their customers. Besides, cyber risks change their form and structure rapidly, so the tools of risk management must be adequate. That is why the problem of cyber-risk identification and assessment has gotten attention and become so actual. The purpose of this study is to outline new approaches to identifying and estimating cyber-risks based on the dates of the World International Property Organization (WIPO).

In order to conduct our study, we will use various tools and techniques such as: citation analysis, cluster analysis, and visualization. We have analyzed the patent information from the groups of "Electric digital data processing", "Transmission of digital information" and data processing systems or methods, specially adapted for financial purposes. In our findings, we analyze the technical and economic significance of patents.

Our work has led us to conclude that the number of methods of cyber risk identification that were the objects of applications granted by WIPO has a strong connection with the number of cyber-attacks from 2010 to 2017. That is why the innovative methods that were granted have a wide spectrum of influence and could be used in different stages of risk management. We selected patents that based on cyber risk identification and assessment from the data of WIPO and divided these patents into clusters. This helps us in understanding the trends and characters of innovative activities directed to successful management of cyber risks.

JEL Classification Numbers: O31, G32; **DOI:** http://dx.doi.org/10.12955/cbup.v6.1163

Keywords: cyber-attacks, risks, patents, clusters.

Introduction

Over the past decades, the development of the Internet has revolutionized the ways of communication, which became a major factor in worldwide economic growth and a powerful tool for ensuring the Fourth Industrial Revolution. On the one hand, it has made it possible for enterprises and private individuals around the world to benefit from the efficiency, speed and convenience of digital transactions and the exchange of information, but, on the other hand, it has increased the likelihood of financial losses, data leakage and reputational losses due to cybercrime.

The cyber-threat problem has been officially recognized worldwide as one of the five key threats to humanity since 2012. So, in the 2012 Global Economic Forum report cyber-attacks ranked fourth on the scale of threats (2017, p. 4). Furthermore, in a next report of the Global Economic Forum in 2017, a new type of cyber-threat was mentioned - data theft and fraud (2017, p. 4). The annual increase in the number of cyber-attacks and financial losses from these attacks increases the focus on methods for identifying cyber-risk in order to assess the probability of financial losses. It is worth noting that the methodology used by enterprises, including IT companies, is rather confidential. This is due to the fact that hackers can immediately improve their criminal techniques on the basis of such information. Therefore, the industry that's engaged in the development of innovative solutions for assessing cyber-risk is in constant development.

Literature review

In modern economic literature many scientific works are devoted to the issue of evaluating cyber-risk. The amount of scientific research has increased 3 fold from 2010 to 2017, according to data from Google academy [3]. But most papers focus on the core of cyber-risk or cyber-threats from the cyber security point of view. In recent years, the worldwide economic opinion on the issue of cyber-risk has been considered in various ways:

- as systematic risks in the activities of financial institutions and in financial markets by Kopp et al. (2017);

[1] Department of Insurance, Maria Curie-Sklodovska University, pl. M. Curie-Sklodovska 5, 20-031 Lublin, Poland, e-mail: liuba.klapkiv@poczta.umcs.lublin.pl
[2] Department of Insurance, University of Lodz, 90-241, Rewolucji str. 1905 R, 41/43, Lodz, Poland, e-mail: uklapkiv@gmail.com
[3] Own calculation based on the frequency of using the expression "cyber risk assessment" in scientific materials: 6550 times in 2010 and 18800 in 2017 (data of assess 23.08.2018)

- as a component of operational risks of companies by Gereth et al. (2017) and Cebula et al. (2010);
- as the probability of occurrence of events in the field of information assets, computer and communication resources by the Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (2016);
- as probable crimes committed through the Internet by Federal Bureau of Investigation (2016).

One of the most complete theoretical studies is the work of M. Eling (2017), in which 209 literary positions on the subject of cyber-risk are reviewed. In this case, the author identified 7 areas of study of cyber-risks.

There are few studies that analyze the methods of identifying and assessing financial losses from the implementation of cyber-risks in business. One of the reasons for the existence of such a deficit is the interdisciplinary spectrum of the subject of research: the financial evaluation of the effects of cyber-attacks, which combines both the informational and financial spheres. The second reason is the lack of clear boundaries of exposure and the spread of the effects of cyber-risk. The place of the appearance or creation of cyber risk can not coincide geographically with the place of its influence and realization This kind of international character in displaying cyber-risk requires an in-depth study of how the business environments in different countries function.

Important roles in the study of cyber risk assessment play consulting, insurance companies and information and software companies (eg, AON, Pricewaterhausecopers, Deloitte, Earnst and Young, Society of Actuaries, International Association, Allianz). With cyber risks and its adverse financial consequences increasing, more attention is paid to this threat from both public and commercial institutions (eg, Federal Bureau of Investigation, the Bank for International Settlements). Table 1 summarizes key English-language studies on cyber risk assessment.

Table 1: English-language studies in methodology of the assessing of cyber-risks

Authors	Title	Year	The main idea of methodology
Dreyer et al (2018)	Estimating the Global cost of cyber risk	2018	Identifies the value at risk by countries and industries; computes direct and systemic costs of cyber risks between industries.
Cherdantsevaa et al (2016)	A review of cyber security risk assessment methods for SCADA systems	2016	Selected and in-detail examined twenty-four risk assessment methods developed for or applied in the context of a SCADA system.
Patel and Zaveri (2010)	A Risk-Assessment Model for Cyber Attacks on Information Systems	2010	Assessing the impact of cyber-attacks with the model that based on the attack types, manager's financial input and damage probabilities to estimate the corresponding probable financial losses
Alalia et al (2018)	Improving risk assessment model of cyber security using fuzzy logic inference system	2018	Assessing the cyber risk by the Fuzzy Inference Model (FIS) that based on the four risk factors which are: vulnerability, threat, likelihood and impact
Mukhopadhyay et al (2017)	Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance	2017	Calculated the expected loss due to cyber-attacks using collective risk modeling. Classifies the losses due to each of these attacks into four classes using a 2 × 2 matrix based on the probability and severity of attacks

Source: Author

Cybercrime is divided into two groups: cyber-dependent crime and cyber-enabled crime. Cyber-dependent crime refers to crimes committed only with the use of information and communication technology devices, which are both a tool and a purpose of the crime (for example, the development and distribution of malicious software for financial gain, hacking to steal, damaging or destroying data and / or network activity). Cyber-enabled crime is a traditional crime that can be magnified by using a

computer, computer network, or other forms of information technology (for example, cyber-enabled fraud and data theft).

It is worth noting that the concept of cyber-risk can be viewed in a narrow or a broad sense. In the narrow sense, cyber-risk is connected to operational threats to information and technology assets that adversely affect the privacy, availability and integrity of information or information systems. Broadly speaking, cyber-risk is a threat to interactive digital networks used to transmit, modify, and store information (cyber space). In our opinion, cyber risk is an operational risk that involves direct or indirect damage by economic agents as a result of their operation in cyberspace.

Data and Methodology

We used the data of the World International Property Organization to analyze innovative methods for identifying and assessing cyber-risks. This approach to using the number of patents as an indicator of innovation has already been substantiated in the scientific works of Hall, Jaffe, Trajtenberg (2005), Scherer (1965), Schmookler (1966), Griliches (1984), and Lerner (2002). But we must point out that some part of these methods is unknown because the inventors protect their inventions by not patenting them, or the inventions do not pass the qualification requirements of the patent office. To be granted, patents must be: novel, non-obvious, useful.

Part I We identified 197 patents that involve different aspects of cyber risk assessment techniques. The main criterion for first selection was the keywords "cyber risk" in the abstract or title. So we got patents from the subclasses of: H04L – (111), G06F – (102), G06Q – (38), G06N – (6), H04W- (4), G02F – (2), G09B – (2), G09C – (2), A61B – (1), B25J - (1). But this result is not "clean" enough to be used in research, because some patents were repeated twice with a different classification number (IPC). Therefore, we checked our list and eliminated all the duplicates. We determined that there were 33 patents in 2017, 49 patents - in 2016, 21 patents – in 2015, 9 patents – in 2014, 9 patents – in 2013, 4 patents – in 2012, 1 patent – in 2011, 2 patents – in 2010, 1 patent – in 2009, 2 patents – in 2008.

In **Part II**, we explored the financial services patent quality for different types. The methodology is otherwise the same as the Part I methodology described above. We examined whether the patents from the class G06Q with more academic citations are more likely to be litigated.

As mentioned by Hall, Jaffe and Trajtenberg (2005) patent citations enable:

- the quantitative analysis along geographical, institutional dimensions.

- the estimation of "importance" of individual patents (both technological and economic).

Part II also includes the proposition of a cluster structure of the cyber risk assessment activity that is based on the patent dates.

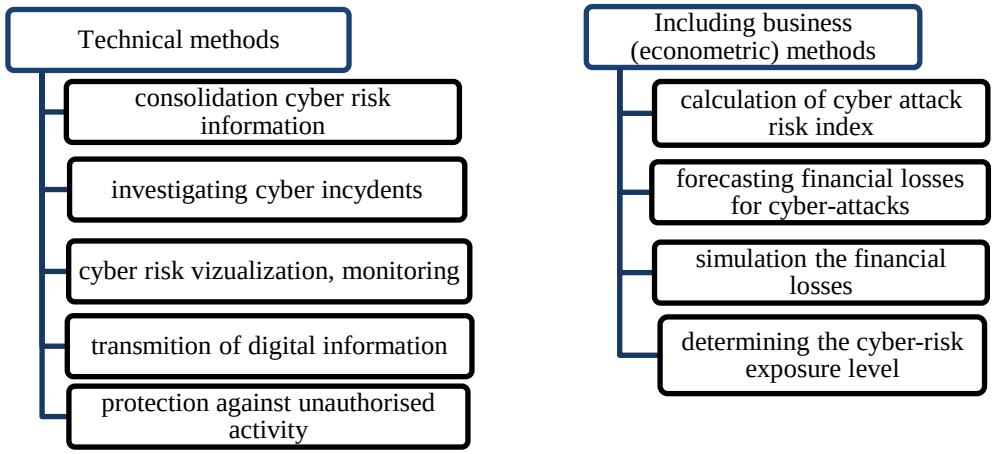
Results and Discussion

The results of the analysis showed that most inventions relate to the technical aspect of cyber-risk (Figure 1). Most patents show the technical aspect of the impact, realization and consequences of cyber threats. Some patents only partly relate to risk assessment, offering auxiliary tools for identifying, fixing and understanding cyber-threats (a likelihood of a cyber-threat, the real-time export of cyber-security risk information, the interface of information about cyber risk).

Business processes that characterize the financial implications of risk implementation are hardly represented in the patents. This confirms the idea that the problem of underwriting cyber-risk is an obstacle to the development of insuring this risk. From the point of view of the probability theory, cyber risk is characterized by significant difficulties of underwriting since it has a very broad sphere of influence and consequences of implementation. In literature, this issue takes a separate niche, since the insurability of risk is the starting point for choosing the method of managing this risk. The main criteria for the insurability of cyber-risk are the ability to determine the maximum losses, average losses for one case, and losses from the "domino effect".

The highest number of citations was noted for patents: the Cybercontinuous Learning Information Feedback (CCLIF): A quantified methodology system to assess the IT architecture and cyber operations risk - 41; Probabilistic model for cyber risk forecasting - 17; Critical / vulnerability / risk logic analysis methodology for business enterprise and cyber security – 39; An online portal for improving cybersecurity risk scores - 12.

Figure 1: Main ideas of patents that includes cyber risk assessment



Source: Author

Based on the patent data, an analysis of their purpose and classification, we have created three clusters that characterize the system of cyber risk assessment (Figure 2). The clusters include the main structural elements that ensure the functioning of the cyber-risk management system. Key clusters include: network security architecture, programs or data against unauthorized activity, and organizational models of risk management.

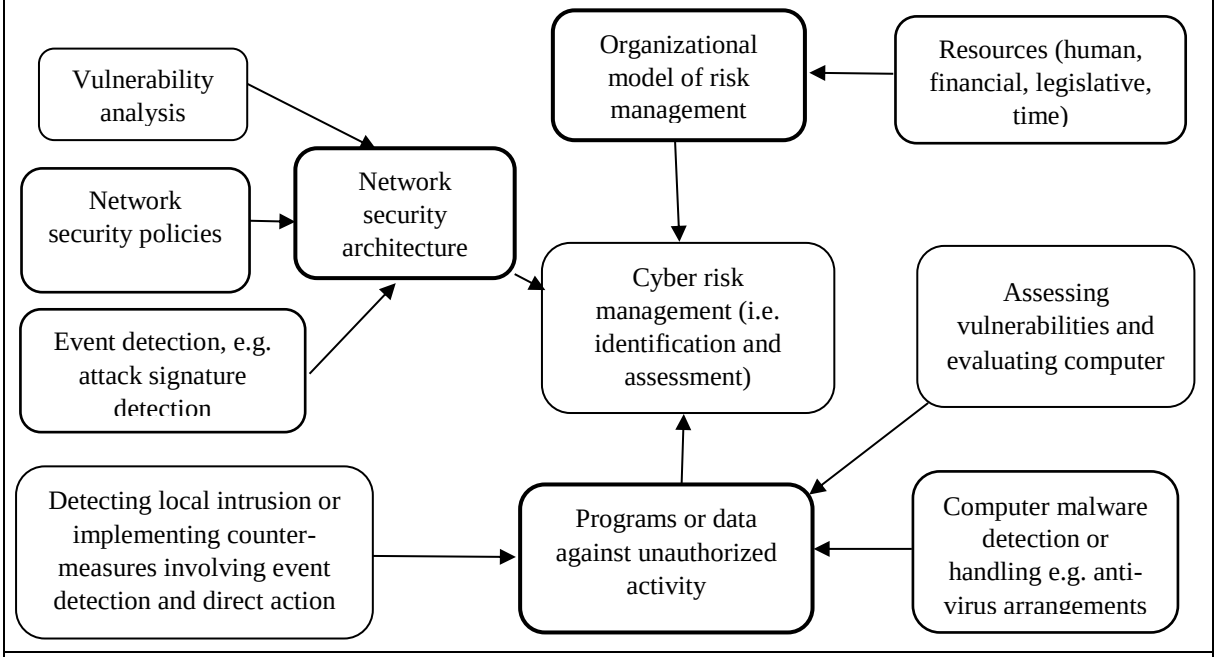
The first patents that included cyber risk assessment methods appeared in 2005. The proposed inventions were not directly aimed at risk assessment, but only partially reflected risk. In most patents, risk assessment is an element of the overall cyber risk management system. Therefore, for an analysis of the modern approaches to assessing cyber-risk, we based our analysis on an accessible description of the patents. We underlined several methods of cyber risk assessment, which was possible to eliminate:

- Cyber risk assessments based on the Monte Carlo methods of estimating the costs for predicting losses and systemic risk. Outputs of the wide variety of simulations that include mitigating actions representing the threat mitigation measures of the organization, for a given moment or period of time, determine a measure of impact of cyber risks to the organization (World Intellectual Property Organization, 2017);
- Cyber risk assessments based on the cyber-attack risk index ("defining a set of cyber risk issues and the value of the degree of risk a corporate entity suffers from the corporate risk issues, an impact score of the corporate risk issue, weighted score from the risk value and the impact score"). This approach enables real-time cyber security risk assessment (World Intellectual Property Organization, 2017a);
- Cyber risk assessments based on a calculated threat intensity and a potential impact on an enterprise or organization. the threat intensity may be calculated based on a subjective evaluation by a cyber threat analyst of one or more threat frequencies, threat likelihood, and threat capability associated with a cyber threat (World Intellectual Property Organization, 2018);
- Cyber risk assessments determining the cyber-risk exposure level for the application based upon the security assessment result sample and a set of parameters; sorting a plurality of risk exposure levels according to an expected loss and a probability of the application being compromised; adjusting the risk exposure levels to account for interconnections and trust relationships between business critical applications, wherein determining the cyber-risk exposure level further comprises the probability of the application being compromised and the expected loss when the application has been compromised (World Intellectual Property Organization, 2016).

Some methods of assessing cyber-risk are based on an analysis of user responses and on the basis of their conclusions (Systems and Methods for Cyber Security Risk Assessment, 2017) or simulating cyber-offender behavior based on real-time feedback from the target network (Synthetic Cyber-risk Model for vulnerability determination, 2016). In 2017, the Probabilistic Model for Cyber Risk Forecast Probabilistic Model for Cybersecurity was patented. This technique defines linear and nonlinear threats for network-dependent systems. In insurance, it is proposed to use an analysis based on data bases (Big

Data), namely Cost-Aware Hierarchical Cyber Incident Analytics. This approach involves designing different scenarios for cyber threats. The main algorithms in CA-HCIA include Monte Carlo Cyber Feature Extraction (MC2FE) or Optimal Cost Balance (OCA) algorithm.

Figure 2: Clusters of cyber risk identification and assessment activity



Source: Author

Conclusions

Patents are not only a method of protecting intellectual property, but also an important source of information for assessing the dynamics of the development of various economic phenomena. We tried to analyze the development of methods for assessing cyber-risk because this is an actual problem. Particularly important is the full identification and assessment of possible negative consequences. The complexity of the solution of this issue is associated with the complex technical and economic nature of cyber-risk. As shown by a cluster analysis, the structure of patents for the period 2008-2017 can be distinguished in three main clusters: network security architecture, programs and date against unauthorized activity, and organizational models of risk management.

A dynamic increase in the number of patents, which includes the description of methods for assessing cyber-risk, is due to the growth of the number and of the costs of cyber-attacks and cyber-incidents. The analysis of the cores of methods shows that the structure and mechanism of evaluation becomes more specialized. This is due to the improvement of the methods of cyber-attacks and the narrowing of their scope.

One of the obstacles to the distribution of innovative methods for assessing cyber-risk is the long time it takes to receive the "granted" status. On average, it's about three years. Given that cyber-threats quickly change their form and effect simultaneously with the introduction of cyber-security, the proposed methods may lose their relevance on the market.

References

Alalia, M., Almogrena, A., Hassana, M., Rassana, lehab A. L., Bhuiyanb, Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security, 74, 323-339.

Cebula, J.J., Young, L.R. (2010). A Taxonomy of Operational Cyber Security Risks, CMU/Software Engeniering Institute, Pittsburg: PA.

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions. (June 2016). Guidance on Cyber Resilience for Financial Market Infrastructures. Retrived from https://www.bis.org/cpmi/publ/d146.htm.

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J.W., Winkelman, Z. (2018). Estimating the Global Cost of Cyber Risks, Methodology and Examples. Retrived April, 14, 2018, from https://www.rand.org/pubs/research_reports/RR2299.html

Eling, M. (2017). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 5, 474-491.

Federal Bureau of Investigation. (2016). Internet Crime Report, Retrived from https://pdf.ic3.gov/2016_IC3Report.pdf

Gereth, P. W., Shevchenko, P.V., Cohen, D. R., Maurice, D. (2017). Understanding Cyber Risk and Cyber Insurance. Retrived March, 2018, from http://dx.doi.org/10.2139/ssrn.3065635

Global Economic Forum. (2017). The Global Risks Report 2017. 12th Edition. Retrived April, 01, 2018, from http://wef.ch/risks2017

Griliches, Z. (1990). Patent Statistics as Economic Indicators: A Survey. Journal of Economic Literature, 28 (4), 1661-1707. Retrived from http://www.jstor.org/fcgi-bin/jstor/listjournal.fcg/00220515/.21-.30

Hall, B., Jaffe, A., & Trajtenberg, M. (2005). Market Value and Patent Citations. The RAND Journal of Economics, 36 (1), 16-38. Retrieved from http://www.jstor.org/stable/1593752

Cherdantseva, Y., Burnapa, P., Blythb, A., Edenb, P., Jonesc, K., Soulsbyc, H., Stoddartd, K. (2016, February). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56, 1-27.

Kopp E., Kaffenberger L., Wilson C., (2017), Cyber Risk, Market Failures, and Financial Stability, (Working Paper of International Monetary Fund). Retrieved March, 2018, from https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104

Lerner, J. (2002). 150 Years Of Patent Protection, American Economic Review, 92, 221-225. Retrived from http://www.nber.org/papers/w8977

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., Shukla, G. K. (2017). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. Information Systems Frontiers. Retrived from https://doi.org/10.1007/s10796-017-9808-5

Patel, S., Zaveri, J. (2010). A Risk-Assessment Model for Cyber Attacks on Information Systems. Journal of computers, 5 (3), 352-359.

Scherer, F.M. (1965). Firm Size, Market Structure, Opportunity, and the Output of Patented Inventions. American Economic Review, 55, 1097-1123.

Schmookler, J. (1966). Invention and Economic Growth. (1st ed.). United States of America: Harvard University Press.

World Intellectual Property Organization. (2016). Patent 2965505. System and method for automatic calculation of cyber-risk in business-critical applications. Retrived from https://patentscope.wipo.int/search/en/detail.jsf?docId=CA196211112&recNum=108&office=&queryString=FP%3A%28cyber+AND+risk%29+&prevFilter=&sortOption=Pub+Date+Desc&maxRec=197

World Intellectual Property Organization. (2017). Patent 20170279843. Probabilistic model for cyber risk forecasting. Retrived from https://patentscope.wipo.int/search/en/detail.jsf?docId=US204154128&recNum=2&office=&queryString=EN_ALLTXT%3A%28of+costs+of+predicted+losses+and+systemic+risk%29+and+cyber+threats&prevFilter=&sortOption=Relevance&maxRec=381

World Intellectual Property Organization. (2017a). Patent 2017268570. Cyber security system and method. Retrived from https://patentscope.wipo.int/search/en/detail.jsf?docId=AU208388013&recNum=6&office=&queryString=FP%3A%28cyber+AND+risk%29+&prevFilter=&sortOption=Pub+Date+Desc&maxRec=197

World Intellectual Property Organization. (2018). Patent 20180069891. System and Method of Mitigating Cyber Attack Risks. Retrived from https://patentscope.wipo.int/search/en/detail.jsf?docId=US213383205&recNum=3&office=&queryString=FP%3A%28cyber+AND+risk%29+&prevFilter=&sortOption=Pub+Date+Desc&maxRec=197