Ekonomika Economics
Management Management
Inovace Innovation

EMI, Vol. 10, Issue 3, 2018
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

MODELING THE IMPACT OF SELECTED CYBER THREATS IN THE FIELD OF CYBER RISK INSURANCE

Lukáš Pavlík

Lukáš Pavlík, Department of Informatics and Applied Mathematics, Moravian Business College Olomouc, Tř. Kosmonautů 1, 779 00 Olomouc, Czech Republic, e-mail: lukas.pavlik@mvso.cz

Abstract:
This paper describes a possible approach to modeling the impact of selected cyber threats in the field of providing cyber-risk insurance. Basic problem is then how the cost of insurance should be calculated and how to assess the level of client's IT security controls and related risk. It compares predefined organizational parameters in relation to cyber threats scenarios. The results show how the insurance company can approach the issue of organizational insurance and protect its information systems against cyber threats. Finally, there is a discussion that sums up the problems with an outline of possible future developments.

Key words:
cyber risk, information, model, threat, insurance, economic

JEL: L53, L86

1 Introduction

These days, many existing organizations do not have sufficient security system protecting them against cyber attacks. Many research papers and monographs have been published dealing with the area of cyber risk insurance and the establishment of optimum financial investments in important parameters of the organization (Pal 2013, Srinidhi 2015, Woods 2017). Parameters may thus have both financial and non-financial character. In the case of information systems can be eg. hardware, software, damage reputation etc. (Schwartz 2013, Lawrence 2003, Kuru 2017). But there can be parameters that may not be directly related to the organization's information system. These parameters are in the final price information system, however, directly involved. However, only a few publications focus on the methodology of valuing important parameter of an organization that should be covered by cyber risk insurance (Fiedler 2016, Johnosn 2014). The aim of the presented paper is to investigate the magnitude of the risk between the cyber threat scenarios and selected parameters, the importance of which is significant to the organization's information system.

Current approaches mainly deal with a problem of creating the efficient cyber insurance market based on a game theory and creating maximal social welfare. In current works, the cyber-insurance premiums usually depend only on general client features (ex. employee number, sales volume), i.e., premiums reflect no client security practices. This is connected with a fact that cyber insurance is affected by the classic insurance problems of adverse selection (higher risk users seek more protection) and moral hazard (users lower their investment in self-protection after being insured). Therefore, the insurance companies need to somehow mitigate the informtion asymmetry and calculate the premium fees with these considerations in mind (Gordon 2011, Hiscox 2011, Danchey 2009).

The information asymmetry can be mitigated in many ways - for example the certifying authority can classify clients based on whether or not they have made security investments, and ensures that certified users get adequate compensation in case of a security incident. Another theoretically attractive incentive mechanism that may result in optimal levels of investment is the liability rule, where users are

EMI, Vol. 10, Issue 3, 2018
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

required to compensate others for the damages caused by their under-investment in security. However, these mechanisms are costly in that it is difficult to accurately determine the cause of a damage.

When calculating the price information system organization, which is important for determining the amount of insurance coverage, it is necessary to analyze, identify and measure selected parameters. Parameters are now an integral part of the company structure. The simplest definition of the term parameter is property that its owner brings revenue, or is expected for corporate, that he will bring in the future.

Parameters may thus have both financial and non-financial character. In the case of information systems can be eg. hardware, software, etc. But also parameters that may not be directly related to the organization's information system. These parameters are in the final price information system, however, directly involved. It can be eg. a production machine, reputation of company. In the case of the analysis and identification of parameters, we can use several analytical tools. If we have a larger amount of parameters is required of them to choose only those that have a certain weight and influence on the price information system.

2 Methods

To determine the impact of cyber threats on the organization's information system, selected risk analysis methods were used. A scale of 1 to 5 was used to determine the significance of parameters that are considered here. The value 1 represents the least meaningful parameter and 5 the most important parameter. Parameters were selected on the basis of a questionnaire survey conducted in 12 organizations in the Czech Republic (Pavlík 2016). In this questionnaire survey, questions were raised especially concerning the data security of possible cybernetic threats that have already occurred in the organization or assets that may be threatened by the impact of these threats. Based on the results of this survey, organization parameters have been compiled, representing areas that can be affected by the impact of individual cyber threats. These areas (parameters) can result in large financial losses and costs that can significantly impair the organization and its functioning. Restoring some parameters (such as Good Organization Name) can be a very challenging process.

In addition, seven types of cybernetic threats were identified, the significance of which was reassigned according to the scale from 1 to 5. A risk matrix has been developed from the available data to illustrate the degree of cyber risk of the identified parameters. The final step was to create the following risk analysis table which illustrates the probability of a cyber threat to the asset and the impact of that threat on the parameter. These results were obtained on the basis of the following mathematical calculation.

The risk analysis methods presented here are based on ISO 27001, which defines an information security management system. In this standard it is possible to find the individual steps of risk analysis that are applied in a shortened form in this paper. The calculation of the required risk is also defined in ISO 27005. The relationship between threat, vulnerability and impact is proposed on the basis of Decree No. 316/2014 Coll. on security measures, cyber security incidents, reactive measures, and cyber security reporting requirements (Cyber Security Regulation).

$$R = PI \times T \times H$$

R……risk
PI……probability
T……value parameter
H……vulnerability of the parameter against cyber threat

EMI, Vol. 10, Issue 3, 2018
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

3 Results

The aim of the analyses was to determine the vulnerability of individual parametres to selected cybernetic threats. For this purpose, seven most common cyber threats with which organizations are threatened were selected.

Tab. 1 Identification of cyber threats and their values

Cyber threat	Probability of the threat
Ransomware	3
Hacking	5
Unauthorized access	3
Malware	3
Data leak due to employee negligence	5
DDoS attack	2
Pretending fraud	1

The following numerical scale is used to express the threat probability.

Tab. 2 Numerical scale of probability

Probability of the threat	Numerical Scale
1	0 – 0,25
2	0,3 – 0,45
3	0,5 – 0,65
4	0,7 – 0,85
5	0,9 - 1

Within this research, six parametres (areas) of the organization were also identified to which the implementation of some of the threats has a significant impact. To illustrate the vulnerability, the risk rating scale mentioned bellow were used.

EMI, Vol. 10, Issue 3, 2018
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

Table 3. Identify organization parameters and determine their significance

Parameter	Parameter value
Hardware	3
Fines	4
Lost yield on unprocessed products	5
Software	4
Cost of data reconstruction and recovery	4
Damage reputation	5

Table 4. Expression of relationship between threats and defined parameters

Expression of relationship	Parameter	Hardware	Fines	Lost yield on unprocessed products	Software	Cost of data reconstruction and recovery	Damage reputation
	Parameter value	**3**	**4**	**5**	**4**	**4**	**5**
Cyber threat	**Probability of the threat**						
Ransomware	**3**	**2**			**4**	**4**	
Hacking	**5**	**5**	**3**	**3**	**4**	**4**	**3**
Unauthorized access	**3**	**3**			**4**	**4**	**5**
Malware	**3**	**4**	**4**	**5**	**4**	**3**	**3**
Data leak due to employee negligence	**5**		**4**			**5**	**5**
DDoS attack	**2**	**3**	**5**		**3**	**3**	**3**
Pretending fraud	**1**						**5**

EMI, Vol. 10, Issue 3, 2018
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

Table 5. Vulnerability matrix

Vulnerability matrix	Parameter	Hardware	Fines	Lost yield on unprocessed products	Software	Cost of data reconstruction and recovery	Damage reputation
	Parameter value	**3**	**4**	5	4	4	5
Cyber threat	**Probability of the threat**						
Ransomware	**3**	**18**			**48**	**48**	
Hacking	**5**	**75**	**70**	**75**	**80**	**80**	**75**
Unauthorized access	**3**	**27**			**48**	**48**	**75**
Malware	**3**	**36**	**48**	**75**	**48**	**36**	**45**
Data leak due to employee negligence	**5**		**80**			**100**	**100**
DDoS attack	**2**	**18**	**40**		**24**	**24**	**25**
Pretending fraud	**1**						**25**

Table 5. Risk rating scales

Risk	**Value range**	**Colour**
Low risk	1 to 30	
Moderate risk	31 to 65	
High risk	66 or more	

Table 4 shows the level of vulnerability of particular organizational parametres and individual cyber threats. As can be seen, hacking and data leak due to employee negligence are the threats to which the organizational parametres are the most vulnerable. It should be noted that these two threats are among the most common problems in organizations that are associated with data leakage or

EMI, Vol. 10, Issue 3, 2018
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

disruption. On the contrary, the selected areas are the least vulnerable to the organization's ransomware, DDoS attack, and fraud pretensions. This is also due to the fact that these cyber threats are the least frequent and do not pose a great threat to the organization. Other organizational parametres show a moderate level of vulnerability to cyber threats.

4 Discussion

The purpose of this paper was to design an algorithm for determining insurance coverage in the framework of cyber threat insurance. The results obtained follow on previous research and analysis (Arunabha 2017, Bojan and Jerman-Blažič 2008, Pandey 2014). It was found that in order to determine the level of insurance cover more precisely, it is necessary to determine the parameters (assets) of the organization. These parameters can be represented by indicators for modeling the impact of selected cyber threats to an organization's information system as reported in. Based on parameters that are valued at the beginning of the entire algorithm, it is necessary to model the interaction between the parameter and the cyber threats (Drounin 2004, Winn 2009). Overall, the modeling and depiction of the impact of individual cyber threats, with consequent influence on the price of the parameters, are the results of this process. Depending on the impact of the most likely cyber threat, an optimal level of insurance cover should be set. However, it is important to note that the proposed procedure does not provide information about the final amount to be covered by the insurance contract (Bandyopadhay 2009, Böhme 2006). Clearly, more research is needed to clarify the impact and cost of parameters. A more accurate interaction between cyber threat and the impact on selected organization parameters (assets) is one of the challenges for future research.

Pricing information system and information that are inserted into it, is a very complex process. Determination of the key factors with subsequent assignment of values is to some extent subjective. But one can say that the information is equally measurable quantity, such as. The laws of physics, and therefore it is possible to objectively determine their value (Šatava 2015, Jarkovský 2014). This value should serve as a basis not only for the organization itself, but also for insurance companies that have chosen to provide the insurance company against cyber risk. Pricing information system, they are usually used so. Methodologies in-house. These are the methods that have been developed by specific companies and whose application is designed exclusively for this organization. These methodologies are usually a combination of existing tools and procedures that can provide relevant data information system (Naghizadeh 2014, Rabin 1989, Ishiguro 2006). This is e.g. the metric type COBIT in combination with the framework NIST, which was developed for the assessment of critical infrastructure, in terms of cyber security in the USA. In conclusion we can say that the issue of insurance information systems against cyber risk is a trend that is due to the increasingly frequent cyber attacks becoming increasingly important field. From my previous research shows that most companies and institutions is more focused on prevention rather than dealing with the consequences and harm arising from the implementation risks (Carly 2015, Leigh 2014, Salter 2016).

On the one hand it is good that prevention is considered as one of the main pillars to prevent undesirable events associated with the information system of the organization. On the other hand, you also need to reckon with the fact that prevention may be inadequate and may compromise the information system and information that are inserted into it. This area can be effectively resolved with the cyber insurance against risk, through which the organization can bridge the gap between the crisis, caused by the disruption of operations information system and restoring the balance that makes the information system is again stable and secure (Kříž 2014, Pavlík 2016).

5 Conclusion

This article was primarily focused on designing possible approaches to modeling the possible impacts of selected cyber threats on the organization's information environment. Based on the findings,

EMI, Vol. 10, Issue 3, 2018
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

it can be stated that the interaction between the cyber threat and the identified parameters is one of the key parts of the process for setting the optimal level of insurance cover for the organization. Parameters that are designed here represent areas of the information environment of an organization whose can negatively affect the organization and its function. The method that has been applied here is part of the Cyber Security Act (Jarkovský 2014), and it is possible to find out which of the above threats can have the greatest impact on these parameters. Based on this analysis, it was found out that the biggest insecurity for the particular organization is hacking. This threat has the greatest number of interactions with the parameters, and therefore the insurance should be counted primarily on the implementation of this threat.

Overall it can be stated that a very important function in the process of modeling the impact of selected cyber threats is the number of interactions with the given parameters. As we can see, not all cyber threats can impact on these parameters. e.g. hacking and malware have interactions with all parameters. On the other hand, the smallest number of interactions has the pretending fraud or ransomware. Further research in this area should include the identification of potential financial damages that may occur in the event of any of the above threats. This assumption should be supported by the valuation of selected organizational parameters and the determination of financial damages on the basis of the organization's risk.

6 Bibliography

[1] MUKHOPADHAY et al. (2017). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. Information Systems Frontiers [online]. pp. 1-22.
[2] BANDYOPADHYAY, Tridib, Vijay MOOKERJEE a Ram RAO (2009). Why IT managers don't go for cyber-insurance products [online]. pp 68-73
[3] BÖHME, Rainer and Gaurav KATARIA (2006). Trust and privacy in digital business[online].Berlin, Heidelberg: Springer Berlin Heidelberg. pp 31-40.
[4] BOJANC, Rok and Borka JERMAN-BLAŽIČ (2008). An economic modelling approach to information seurity risk management. International Journal of Information Management. pp 413-422.
[5] Damla Kuru and Sema Bayraktar (2017). The effect of cyber-risk insurance to social welfare. Journal of Financial Crime [online]. pp. 329-346.
[6] FIELDER, Andrew et al. (2016). Decision support approaches for cyber security investment. Decision Support Systems. pp 13-23.
[7] JOHNSON. et al. (2014). The Complexity of Estimating Systematic Risk in Networks, Computer Security Foundations Symposium (CSF). pp 325-336
[8] LAWRENCE John et al. (2003). A Framework for Using Insurance for Cyber-risk Management. Management [online]. pp 223-229.
[9] PAL, R et al. (2013). On a way to improve cyber-insurer profits when a security vendor becomes the cyber-insurer, IFIP Networking Conference. pp. 1-9.
[10] PANDEY, Paul and E.A. SNEKKENES (2014). Applicability of Prediction Markets in Information Security Risk Management, 2014 25th International Workshop on Database and Expert Systems Applications (DEXA). pp. 296-300.
[11] SCHWARTZ, Galina, Nikhil SHETTY and Jean WALRAND (2013). Why cyber-insurance contracts fail to reflect cyber-risks [online]. pp 781-787.
[12] SRINIDHI, Bin, Jia YAN and Giri Kumar TAYI (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. Decision Support Systems [online]. pp 49-62.
[13] WOODS, D. et al. (2017). Mapping the coverage of security controls in cyber insurance proposal forms. Journal of Internet Services and Applications [online].

EMI, Vol. 10, Issue 3, 2018
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

[14] ŠATAVA, Jiří. The implementation of the directive governs the physical security of the computer network in the state administration environment. Zlín, 2015. Bachelor thesis. Tomas Bata University in Zlín. Supervisor: Lubomír Macků, Ph.D.

[15] JARKOVSKÝ, Aleš. Cyber Risk Insurance. Online System [online]. Prague, 2014, (2), 3 pp. [Cit. 2018-04-21]. Available from: http://www.systemonline.cz/it-security/pojisteni-kybernetickych-rizik.htm

[16] CARLY, Jim. 10 key facts you need to know about cyber insurance. We live security [online]. USA, 2015, , 3 s. [cit. 2018-04-18]. Dostupné z: http://www.welivesecurity.com/2015/10/14/10-key-facts-need-know-cyber-insurance/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+eset%2Fblog+%28ESET+Blog%3A+We+Live+Security%29

[17] LEIGH, Thomas a Jim FINKLE. Insurers struggle to get grip on burgeoning cyber risk market. Reuters [online]. USA, Boston, 2014 [cit. 2018-04-11]. Dostupné z: http://www.reuters.com/article/us-insurance-cybersecurity-idUSKBN0FJ0B820140714

[18] SALTER, Josh. THE RISK MANAGEMENT SOCIETY. RIMS Release Cyber Survey [online]. [cit. 2018-06-02]. Dostupné z: https://www.rims.org/aboutRIMS/Newsroom/News/Pages/cybersurvey15.aspx

[19] KŘÍŽ, Lukáš. CIO BUSINESS WORLD. The cost of cyber-attacks has risen again [online]. Prague, 2014 [cit. 2016-06-03]. Available from: http://businessworld.com/analyzy/naklady-na-reseni-kybernetickych-utoku-opet-vzrostly-11889

[20] NAGHIZADEH, P et al. Closing the price of anarchy gap in the interdependent security game, Information Theory and Applications Workshop (ITA), 2014, vol., no., pp.1,8, 9-14 Feb.2014

[21] PAVLÍK, Lukáš a Roman JAŠEK. Possibilities Pricing of the Information System by Providng Insurance against Cyber Risk: International Scientific Conference: Knowledge for Market Use 2016 [online]. Univerzita Palackého, Olomouc, 2016, 8 s. [cit. 2018-06-26]. ISBN 978-80-87533-14-7

[22] RABIN, M.O.: Efficient dispersal of information for security, load balancing and fault tolerance. *Journal of the ACM* 32 (1989) 335–348

[23] ISHIGURO, M. et al. The effect of information security incidents on corporate values in the Japanese stock market. Retrieved November 28, 2011, Available from: http://wesii.econinfosec.org/draft.php?paper_id=23

[24] DROUNIN, D. (2004). Cyber risk insurance: A discourse and preparátory guide, 2004, Bethesda, MD: SANS Institute.

[25] WINN, J., & GOVEM, K. (2009). Identity theft: Risks and challenges to business of data compromise. Temple Journal of Science, Technology, & Environmental Law, 28(1), 49—63

[26] GORDON, L. A et al. (2011). The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security, 19(1), 33—56

[27] HISCOX. (2011). Safeonline launches Internet security insurance. Retrieved November 23, 2011,Available from: http://www.hiscox.com/news/press-releases/archive/2000/18-10-00.aspx

[28] DANCHEY, D. (2009). Conficker's estimated economic cost? $9.1 billion. Retrieved November 23, 2011, Available from: http://www.zdnet.com/blog/