Modeling the Impact of Selected Cyber Threats on the Organization's Parameters in the Framework of Cyber Risk Insurance

LUKÁŠ PAVLÍK
Department of Security Engineering
Tomas Bata University in Zlin, Faculty of Applied Informatics
Nad Stráněmi 4511, 760 05, Zlín
Czech Republic
lpavlik@utb.cz

Abstract: - Many small and medium-sized organizations face very frequent attacks on their information systems and valuable assets. One of the ways to face and prevent the occurrence of damage from these undesirable events is to insure information systems against cyber-risk. This paper presents the possibilities of modeling the impact of cyber threats on selected organizational parameters. The main results, which are based on the interaction of cyber threats and identified parameters, can then be intercepted in the context of cyber-risk insurance. The main findings can be used as a platform for setting optimal insurance coverage for the organization.

Key-Words: - information system, risk, cyber threat, parameter, modeling, impact, costs

1 Introduction

In the recent years, we could see many examples of data breaches amongst the high profile companies such as RSA, Global Payments, Sony or LinkedIn that resulted in a significant financial loss [1,2,3]. In spite of the fact that these organizations had probably all state of the art security controls in place, the intruders were able to breach them and steal the data that were mission critical for some of these companies. Because many of today's businesses are dependent on the confidence of their customers and on their goodwill, they are aware of the fact that just a single occurrence of the data breach could put them out of the business. In order to protect their investments, they therefore look for a new approach to risk management which could bring them some kind of payout in case that all the internal security controls fail. [11, 12].

Cyber risk insurance is a relatively new issue in the field of insurance and information security. It is a transdisciplinary area of scientific interest that combines many different disciplines, such as economics, informatics, security and law. In recent years, the number of cyber attacks on major information systems worldwide has grown considerably. This rise is due to the fact that information is a very valuable asset, and attacks on organizations are moving into the cyberspace these days. Moreover, 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 assets of the organization [4,6,13]. However, only a few publications focus on the methodology of valuing important assets of an organization that should be covered by cyber risk insurance. [4,5] The aim of the presented paper is to investigate the magnitude of the risk between the cyber threat scenarios and selected assets, the importance of which is significant to the organization's information system. [12].

1.2 Current approaches to cyber insurance

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 [7]. 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. [8].

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 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. [9,10,11].

2 Problem Formulation

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 parametr that are considered here. The value 1 represents the least meaningful parameter and 5 the most important parameter.

For the purpose of modeling cyber threats, 10 possible cyber threats have been identified that can cover cyber-threat insurance. These scenarios were determined on the basis of AIG insurance statistics. Parameters that may be affected by the impact of cyber-threatened risks were determined by the article author's research, which was conducted in thirteen organizations in Czech Republic. These organizations include both insurance companies, manufacturing companies and state institutions.

A risk matrix has been developed from the available data to illustrate the degree of cyber risk of the identified assets. 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 asset. These results were obtained on the basis of the following mathematical calculation.

$$\mathbf{R = PI \times T \times H} \quad (1)$$

R…….risk
PI……probability
T…….value parameter
H……parameter vulnerability

2.1 Characteristics of selected parameters

The most important parameters in the organization related to cyber-threat insurance include:

a) Hardware
b) Fines
c) Lost yield on unprocessed products

Ad a) The hardware area includes not only computers and their accessories, but also any technical equipment that is related to the organization's information system.

Calculation: This category is valued based on two possible solution approaches.

1) The first one is the award option if the hardware has a cost of less than 40,000 CZK.

Valuation at acquisition cost - in the case of assets acquired in return for payment (also included in the price are related costs - for example, transportation and installation, licenses and patents, exploration, geological and other work ... the cost of the purchase price may also include interest on the loan, definitely).

Repurchase Valuation Award - the price at which the assets would be acquired at the time they are accounted for – tangible assets received by the donation, newly discovered and not yet recorded in the bookkeeping, the tangible assets deposit, provided that this deposit according to the Memorandum of Association is not otherwise assessed; tangible assets acquired free of charge on the basis of a finance lease; in cases where it is not possible to identify the own costs of creating the property.

Own costs – tangible assets created by own business. These are direct costs incurred for production or other activity and indirect costs that are related to production or other activities.

2) Another possibility of evaluating hardware is based on its current residual value, which arises from the depreciation of long-term tangible assets with a price higher than CZK 40,000. For the purpose of measuring this type of asset, an

accelerated depreciation method was chosen according to the formula:

In the first year: $\boldsymbol{D_n = \frac{PP}{c}}$ (2)

Next year: $\boldsymbol{D_n = \frac{(2*NBV)}{(C-yd)}}$ (3)

D_n = depreciation

PP = purchase price

C = coefficient

NBV = net book value

C = coefficient valid in the coming years

yd = year of depreciation

Ad b) If this was the type of organization where the main business is the production, then there could be penalties for not doing a certain number of products in a given schedule. In the event of a breach of the information system function of the company, whose main function is to ensure the operation of production machines and production line, the required number of products would not be fulfilled at a given time unit, which would result in large losses of the company. These fines can be awarded either by the headquarters of the firm if it is a failure of an information system at a branch of a firm, or a fine may also be imposed by the supplier of the material that comes from a potential product from its material and thus also from the profit.

Another subject that can sanction an institution that does not meet certain requirements is the Office for Personal Data Protection. This issue is followed by the General Data Protection Regulation (GDPR). Sanctions can also be included in the category of fines by suppliers and customers. In some cases, fines may be imposed, for example, for failure to meet delivery dates, materials, services, etc. These penalties may be imposed by purchasers. Contractors may include, for example, fines for unprocessed products. Suppliers provide material to the organization, and if products from this material are not produced, potential supplier and manufacturer profits may be lost.

Calcuation: No predefined formula can be used to evaluate this category. The amount of fines is an individual matter and depends on supplier-customer relations. In the case of GDPR issues, the amount of fines is set in the range of 10,000,000 € to 20,000,000 € or 4 % of the total turnover of the company. According to current information from the Office for Personal Data Protection, fines will be awarded at the lowest threshold, therefore10,000,000 €. This amount of fines also includes the price of data that may be lost or misused due to a cyber threat.

Ad c) This can happen if the organization has a set of products that it has to produce for a specified time unit. In the event of a disablement or disruption of the information system, production functions are also undermined. This can result in a lost profit, which is also an important item, when determining the total value of the lost profit.

Calcuation: Methods and approaches to determine the lost profit of an organization are large. For the purpose of research is designed a formula for the determination of lost profits.

$$\boldsymbol{LP = PP_h * H_p} \quad (4)$$

LP = lost yield on unprocessed products

PP_h = the price of a normal number of products made in one hour

H_p = the number of hours when the products are not produce

3 Problem Solution

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

Table 1. Identify organization parameters and determine their significance

Parameter	**Parameter value**
Hardware	3
Fines	4
Lost yield on unprocessed products	5

Within this research, three parameters (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 above were used.

Table 2. Identification of cyber threats and their values

Cyber threat	**Probability of the threat**
Ransomware	3
Hacking	5
Unauthorized access	2
Malware	2
Data leak due to employee negligence	5
DDoS attack	2
Pretending fraud	1
Physical loss of data carrier	3
Lightning strike	2
System failure	1

The following decimal scale is used for more accurate probability.

Table 3. Decimal scale of probability

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

Table 3. Parameter matrix, threats and impact

Vulnerability matrix	Parameter	Hardware	Fines	Lost yield on unprocessed products
	Parameter value	3	4	5
Cyber threat	Probability of the threat			
Ransomware	3	**4**		
Hacking	5	**5**	**5**	**3**
Pretending fraud	1			**1**
Malware	2	**5**	**5**	**1**
Data leak due to empl. neg	5		**4**	
DDoS attack	2	**4**	**4**	
Physical loss of data carrier	3	**5**	**5**	
Lightning strike	4	**4**		**5**

System failure	1	**5**		**5**
Unautho rized access	2	**2**	**4**	
Lightning strike	4	**48**		**100**
System failure	3	**15**		**25**
Unautho rized access	2	**12**	**32**	

Table 4. Vulnerability matrix

Vulnerability matrix	Parameter	Hardware	Fines	Lost yield on unprocessed products
	Parameter value	3	4	5
Cyber threat	Probability of the threat			
Ransom ware	3	**36**		
Hacking	4	**75**	**100**	**75**
Pretending fraud	3			**5**
Malware	2	**30**	**40**	**10**
Data leak due to empl. neg	5		**80**	
DDoS attack	2	**24**	**32**	
Physical loss of data carrier	3	**45**	**60**	

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 5 shows the level of vulnerability of particular organizational factors and individual cyber threats. As can be seen, hacking and data leak due to employee negligence are the threats to which the organizational factors 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 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 factors show a moderate level of vulnerability to cyber threats.

On the basis of the analyzes performed, it is possible to predict the impacts of the most likely threats to the organization and its information system. Each of these parameters should have a financial statement on the basis of which potential financial damage could be caused. This financial statement can serve as a basis for determining optimal coverage. According to available studies, it can be said that the algorithm for determining the optimal level of insurance against cybernetic threats is still absent. The main objective of the author's research is to design and validate this algorithm on

the general model of the organization. This work is the subject of further research in the field. [13]

4 Conclusion

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 [6,7]. 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 [8,9,10]. 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.

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. 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 the information system and information that is inserted into it is a very complex process. The determination of the key factors with subsequent assignment of values is subjective to some extent. But it is possible to say that the information as such is an equally measurable quantity. It follows physical laws so it becomes possible to objectively determine its value. This value should serve as a basis not only for the organization itself, but also for insurance companies that have chosen to provide the company insurance against cyber risk. The in-house methodologies are usually used for pricing the information system. These are the methods that have been developed by specific companies and the application of which is designed exclusively for this organization.

In conclusion, I can say that the issue of the insurance of information systems against cyber risk is a trend that has become an increasingly important field due to the increasingly frequent cyber attacks. My previous research shows that most companies and institutions are more focused on prevention rather than dealing with the consequences and harm arising from the implementation risks. On the one hand, it is good that prevention is considered one of the main pillars to prevent undesirable situations associated with the information system of the organization. On the other hand, you also need to reckon with the fact that prevention can be inadequate and can compromise the information system and information that is 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 the information system operations and restoring the balance that makes the information system stable and secure again. [10,13].

These methodologies are usually a combination of existing tools and procedures that can provide relevant data on the information system. This is e.g. the metric type COBIT in combination with the framework NIST which was developed in the USA for assessing the critical infrastructure in terms of cyber security. The current methods for determining the optimum level of insurance coverage are based on pure actuarial mathematics. [9,10] This is not the case for information technology or security. Based on this fact, determining the amount of insurance cover can not reflect all interactions and influences that should be included in the process of calculating insurance for the organization. In practice, this is reflected in the insufficient setting of the insurance limit. [8]. If research in this field is to continue, it should focus precisely on the implementation of IT and security in the optimal insurance calculation process for each organization.

References:

[1] T. Bandyopadhyay, Organizational Adoption of Cyber Insurance Instruments in it Security Risk Management, in: SAIS 2012 Proceedings, pp. 348 – 361.

[2] S. Mansfield-Devine, Security guarantees: building credibility for security vendors, Netw. Secur. 2016, Vol. 2, pp. 14–18.

[3] P. Naghizadeh, M. Liu, Voluntary participation in cyber-insurance markets, in: Proceedings of the 2014 Annual Workshop on Economics in Information Security, 2014, pp. 251 – 262.

[4] D.K. Saini, I. Azad, N.B. Raut, L.A. Hadimani, Utility implementation for cyber risk insurance modeling, in: Proceedings of

the World Congress on Engineering, Vol. 1, 2011, pp. 346 – 358.

[5] G. Schwartz, N. Shetty, J.C. Walrand, Why cyber-insurance contracts fail to reflect cyber-risks, in: Proceeding Sof the 51st Annual Allerton Conference, 2013, pp. 781–787.

[6] S. Chaisiri, R.K.L. Ko, D. Niyato, A joint optimization approach to security-asa-service allocation and cyber insurance management, in: Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Vol. 1, 2015, pp. 426–433.

[7] F. Martinelli, A. Yautsiukhin, Security by insurance for services, in: Proceedings of the 1st International Workshop on Cyber Resilience Economics, 2016, pp. 25 – 36.

[8] B. Johnson, A. Laszka, J. Grossklags, The complexity of estimating systematic risk in networks, in: Proceedings of the 27th IEEE Computer Security Foundations Symposium, CSF, 2014.

[9] L. Krautsevich, F. Martinelli, A. Yautsiukhin, Formal analysis of security metrics and risk, in: Proceedings of the IFIP Workshop on Information Security Theory and Practice, in: Lecture Notes in Computer Science, vol. 6633, 2011, pp. 304–319.

[10] A. Mukhopadhyay, G.K. Shukla, P. Kirs, K.K. Bagchi, Quntifying e-risk for cyber-insurance using logit anf probit models, in: Proceedings of the 8th Annual Symposium on Information Assurance, 2013, pp. 425 – 436.

[11] B. Johnson, J. Grossklags, N. Christin, J. Chuang, Are security experts useful? Bayesian nash equilibria for network security games with limited information, in: D. Gritzalis, B. Preneel, M. Theoharidou (Eds.), Proceedings of the 15th European Symposium on Research in Computer Security, Springer, 2010, pp. 588–606.

[12] G.E. Rejda, Principles of Risk Management and Insurance, 10th edition Pearson Publication, 2010.

[13] J. Yan, G.K. Tayi, Allocation of resources to cyber-security: the effect of misalignment of interest between managers and investors, Decis. Support. Syst. 75, (2015) pp. 49–62.