The Issue of Cyber-Risk Insurance from the Point of View of the Valuation of the Information System in the Organization

Lukas Pavlik
Department of Safety Engineering
Tomas Bata University in Zlin
Zlin, Czech republic
lpavlik@fai.utb.cz

Tomas Klima
Department of System Analysis
University of Economics
Prague, Czech republic
the.book@seznam.cz

Krerk Piromsopa
Department of Computer Engineering
Chulalongkorn University
Bangkok, Thailand
krerk@cp.eng.chula.ac.th

***Abstract*— In recent years, we could see that a lot of world organizations are contested by different ways, which we are called as cyber threats or cyber risks. Many of organizations are well secured, but the most of them admitted that they are not able to successfully prevent these attacks and they tried to find other ways to mitigate the risk. The insurance market began to respond to this fact, which began offering insurance against cyber risks. 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. In this article, authors propose scoring model for cyber insurance that is based on the results of internal and external audits and compliance with mandatory and voluntary standards and presented some main factors, which are most likely to affected the price of organization.**

Keywords*— *cyber risk, factors, scoring model, price, information system

I. 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.

This approach abandons the focus (only) on investments into internal security controls and suggests the use of cyber security insurance. Cyber insurance is a risk transfer mechanism, by which an organization can exchange uncertain loss for a fixed yearly loss (i.e. premium) [4]. Basic idea is the same for that of travel insurance – you pay the insurance company some amount of money (premium) and if the adverse event occurs, you receive the appropriate payment (in case you meet all the requirements). As stated in cyber insurance is a promising remedy to many risk-related problems because it facilitates risk diversification; however, structural consequences of networked systems can also affect insurers [5]. The biggest difference between the travel insurance and cybersecurity insurance is the fact that insurance company should have at least basic overview of the state of the organization security controls (to mitigate the information asymmetry). This fact brings the cyber insurance closer to the problematics of the financial loans, where also the financial company needs to conduct basic background check and employs a scoring model which determines if the client is able to apply for a loan and if yes, what should be the cost (Pricing of insurance products traditionally relies on actuarial tables constructed from voluminous historical records. Since the Internet is relatively new, extensive histories of e-crimes and related losses do not exist. The repositories of information security breaches that do exist (see www.cert.org) do not cover many years, and suffer from the fact that firms often will not reveal details concerning a security breach).

Main benefit of a scoring model is fairness of the price calculation which is a prerequisite for an effective cyber insurance market and transparency for both insurance company and client. In case the cost is calculated without the model (unfair), the result is un-optimal which means either the demand for cyber insurance is too low because of the inadequate price or there is a significant risk that the insurance companies will go bankrupt if they are not able to cover their losses from premiums. Recent research works on cyber-insurance have mathematically shown the existence of inefficient insurance markets (Intuitively, an efficient market is one where all

stakeholders (market elements) mutually satisfy their interests [6]). Secondary benefit is the fact that if the premium is calculated according the proposed model, the client has an incentive to continuously develop his internal security controls (premium is lower if the results from audits suggest responsible approach to IT security).

When providing the insurance against cyber risk, the methodical process of quoting the price of such an information system is the key area. This issue is also the subject of my dissertation. It is not easy to specify the factors that directly affect the price of the information system. A large number of influences enter the assessment process and these must be included in the methodology of the assessment process. However, it is necessary to consider only those factors that are essential for an objective assessment of the information system and eliminate the redundant ones. From the research that has been carried out so far, it is possible to develop the following procedure for determining the price of the information system which can be used as a platform for developing the methodical procedure.

The construction and employment of scoring model for the domain of cyber insurance is discussed in the rest of this article. In the first part current approaches, basic prerequisites and assumptions are discussed, followed by a description for constructing such a scoring model. In the second part, newly developed scoring model is presented on a use case (in order to explain practical use of the model).

II. 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 information 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. Alternatively, proposes assigning a level of due care, in which following a security incident, a user is penalized only if its level of investment is lower than a pre-specified threshold. Finally, users can be incentivized to invest in security if they are assigned bonuses/penalties based on their security outcome (e.g. users get a reward if their security has not been breached). It should be noted that in all the aforementioned incentive mechanisms, there is a need for either auditing users, monitoring their actual investment, or accurately observing their security outcome [4]. It´s also connected with a problem that the success of an organization in management of its information security risks hinges on its efficient deployment of information security controls.

In order to make the right decision, decision makers need appropriate tools to assess the alternative actions based on the relevant information, which is widely dispersed. Currently, decision makers rely on a number of traditional approaches such as consulting experts, appointing teams for qualitative and/or quantitative risk analysis, to improve their decisions.

Especially the aforementioned methods for qualitative and quantitative risk analysis such as CRAMM, OCTAVE, DREAD are very helpful for internal audits and internal risk management, but have limitations for the use in calculating the fair premium price. Since these methods usually work with an expert estimation, which is very subjective and in connection with an information asymmetry between client and insurance company can be very inaccurate, there is a need for new methods to help the decision makers [9].

III. Scoring model

In this section, the scoring model based on results of external and internal security assessment as well as compliance with mandatory and other standards is described. This model is a baseline for decision making if a specific client should be insured and what should be the premium (price of the insurance). The goal of this model is to work with relevant factors with respect to client's privacy. When the insurance company has a possibility to gain information from a third party (independent audit company) about the level of client´s security controls (which also contains compliance information), the information asymmetry is lower and also the problem of adverse selection is partly mitigated. The model also aims to be as simple as possible without employing pure theoretical approaches (This model works with several assumptions – firstly we assume that company which fails to comply with a mandatory standard or law is not able to claim an insurance. Secondly we assume that there are companies that can be regarded as accredited external auditors. For example in UK there is an CREST (http://crest-approved.org/) which organizes approved IT security audit vendors. If the accredited vendor is not available then we can choose any of the top vendors on the market). The scoring model is based on following:

1) Compliance with mandatory standards and laws (eg. SOX, HIPAA, Basel, PCI DSS).

This is a key factor, which means that if client is not compliant, then a firm is not able to apply for a cyber insurance.

2) Compliance with other standards (eg. ISO 27001)

If compliant, then the client is awarded with a score. Exact calculation is a topic for further discussion.

3) Results of a security assessment (audit) conducted by an accredited company

Based on the results of the audit, the client is awarded with a score. The company which conducts the audit must be accredited (which means that must be recognized as a professional organization – similar to CREST in the UK).

4) Results of other security assessments (audits) (eg. results from internal audits)

Based on the results of the audit the client is awarded with a score.

At first the client has to prove that he has either no obligation to comply with any mandatory standard or law or is compliant. For an insurance company, noncompliance is a reasonable cause for declining the clients' demand as it suggests an inferior security practices (the client will probably also face some penalty for the noncompliance). This is a key factor - in case of noncompliance the final score equals zero, thus the assessment process ends.

Then the client submits the documents which prove the compliance with other (voluntary) standards. These documents are reviewed by analyst of insurance company and score is awarded according the expert opinion (possible ways how to exactly determine the score are discussed in paragraph Discussion and further research). The value of corresponding weight a is recommended to be 0.25, see calculation below.

Results of a security audit by accredited company are the most important factor in the decision making process (thus the value of b is recommended to be 0.65, see calculation below). They help the analyst to responsibly assess the level of IT security controls in client organization and score is calculated in cooperation with security analyst who is able to translate the technical details from an audit report into business terms. Other possible way is that if the auditing company prepares the report on demand for this scoring process the score can be awarded directly by this company (For experienced audit company it´s easy to benchmark the level of IT security controls of client organization).

Results of other security assessments are considered as auxiliary materials as they can be possibly spoofed by client in order to obtain lower premium (or be able to claim the insurance). If client has any other documents that prove the level of IT security controls (security budget, invoices from IT security vendors etc.) they can be also used. The value of corresponding weight c is recommended to be 0.25.

Overall score is then calculated:

$$\boldsymbol{SCORE = \alpha(a \times \beta + b \times \gamma + c \times \delta)}$$

α - Compliance with mandatory standards and laws {0,1}
β - Compliance with other standards <0,1)
γ - Results of a security assessment (audit) conducted by an accredited company <0,1)
δ - Results of other security assessments (audits) <0,1)
a,b,c – weights (0,1) *(their values are subject of further discussion and should be set by the insurance company analyst)*

For further calculations we propose following values:

a=0.25
b=0.65
c=0.1

Because the calculation is straightforward, for the practical use we propose also the description in pseudocode:

SCORE <0, 1) Decimal
THRESHOLD (0, 1) Decimal
PREMIUM Decimal
INSURABLE Boolean
TARGET_VALUE Integer
PRICE_COEFFICIENT Decimal

If SCORE >= THRESHOLD and α=1 then
INSURABLE=TRUE
SCORE = 0.25 × β + 0.65 × γ + 0.1 × δ
PREMIUM= PRICE_COEFFICIENT × TARGET_VALUE / SCORE
Else
INSURABLE=FALSE
EndIf

A. Use case

In order to achieve better understanding of the proposed scoring model, one example on how the process could look like is described in this paragraph. Let´s assume the following client:

1) Client wants to insure losses up to €10 mil.
2) Client has no obligations to comply with mandatory standards.
3) Client is certified with ISO 27001.
4) Client has been audited by a sound external audit company (e.g. Ernst & Young).
5) Client did not submit the result of internal IT security audit.

In order to calculate the premium, we need a values of threshold, price_coefficient and values of variables α, β,γ,δ. Threshold is set by an insurance company and depends on risk that the company is willing to take (where the divide between secure and insecure companies should be).

Threshold is connected with a value of price_coefficient which directly determines the premium. Let´s assume that insurance company has set these variables:

THRESHOLD = 0.6
PRICE_COEFFICIENT = 0.03

These values tell us that company that has a score at least 0.6 is able to apply for an insurance. Next we need a values of variables α, β,γ,δ:

- α has value of 1 because the client does not have to comply with any mandatory standard.
- β is calculated by an insurance company analyst. Let´s assume that an expert opinion is that if the company complies to ISO 27001, this variable should be a value of 0.7.
- γ is also calculated by an insurance company analyst in cooperation with security analyst. Let´s assume that the client has very good results from an audit and therefore the value set by analyst is 0.8.
- The value of δ is zero, because the client was not able to submit result of internal audit (or any prove of level of IT security controls).

Based on the given values, the calculation is:

$$SCORE = 0.25 \times 0.7 + 0.65 \times 0.8 = 0.695$$

$$SCORE > THRESHOLD$$

$$PREMIUM = 0.03 \times 10\,000\,000 / 0.695 = 431654{,}6762589928$$

PREMIUM = € 431 655

Result from the calculation is that if the client wants to insure losses up to €10 mil, the premium of this insurance will be € 431 655. Exact calculation depends heavily on the variables set by an insurance company (threshold, price_coefficient). So there is a possibility to fine tune this model to accordingly respect the requested risk profile for a portfolio of clients of a specific insurance company. Also if the analyst of the insurance company has expert opinion that the values of β,γ,δ should be different it´s very easy to alter the calculation. It is worth clarifying that our main focus is the scoring model. The premium price is just an example.

IV. ATTRIBUTES OF NA ORGANIZATION

The areas which are directly associated with determining the amount of insurance coverage need to be included in the group concerning the organization complexity. This amount, based on the analysis of this group, should cover the main costs for the system recovery and financial compensation for the value of lost or damaged data. The main areas of this issue include:

- **turnover,**
- **hardware,**
- **empoyees,**
- **software,**
- **fines,**
- **the cost of data reconstruction,**
- **the damage to reputation.**

a) Turnover

The turnover can be defined as the amount of funds that are adopted by the economic entity for a specific period. For a merchant, for example, it is a summary of what customers have paid for the goods. According to the turnover amount for a certain period, the sum of money the company would lose in case of the information system failure which would thus mean the inability to produce goods and generate profit can be estimated. According to this amount, the approximate value for the insurance coverage of the information system can therefore be determined. [5]

b) Hardware

In this case, not only computers and their accessories, but also any mechanical and technical equipment related to the information system of the organization can be included in the hardware area. In this group, the lost revenue can be calculated which is the indicator of the value the organization has lost for a specific time period. The loss of revenue can occur e.g. due to the inactivity or disruption of the information system for a certain time. During this time when the information system does not work, the production capacity can be disrupted, which can lead to a loss in the company.

c) Employees

In the employees group, we need to consider the actual number of employees available in the organization. It is very difficult to use the relevant data when determining the input value of each employee working with each document. The result should be a value that comes as close as possible to the actual value that the employee put in their work with the document. One option that can be used as an initial procedure for determining this criterion is the following formula:

The value the employees put in the document production

t * CZ * PZ

t .....….the time spent by employees on the production of documents

CZ .....avarage labour costs of employees

PZ .....….the number of employees involved in drafting the document

The time spent by employees on the production of documents

The determination of the time spent by employees on creating the documents is usually set for a period of five years. The reason is that five years is the most common retention period for documents in the organization. [5]

Average labour costs of employees

This is the hourly wage which is designed for employees in the company.

From the formula proposed above, it is possible to determine the approximate price that indicates the value of information and documents the employees were working with for the elapsed time in the organization. The information value is thus relative to a certain extent, however, it is possible to use this way of assets valuation in the organization so as to reach the value which can be used for further work.

The number of employees involved in drafting the document

This is the actual number of employees who take part in forming the document price with their added value.

c) Software

All the software that can be deleted or irreversibly modified due to the disruption of the information system function can be included in the category of software. The software area is relatively easy to assess due to acquisition costs which serve as the basis for assessing this category. [5,7]

d) Fines

Fines can be issued on the basis of a failure to meet certain requirements. These requirements are set for each type of organization separately. In case of state institutions, a situation can occur that the failure of the organization information system can cause inability to provide the information that was due to be published. This means e.g. the publication of information on the electronic notice board, which can be sanctioned under the Act on Municipalities No. 128/200 Coll. It also depends on the type of information that was not published within a certain time interval. If it were the documents concerning e.g. a municipal budget, then this issue would be related to the legislation of the Amendment No. 477/2008 Coll., in the provision of the Act No. 250/2000 Coll. [1]

If it were a second type of organization, i.e. manufacturing companies, then this could lead to sanctions due to the fact that the company did not manufacture a number of products within a specified time plan. In the event of disruption of the function of the company information system, the main function of which is to ensure the operation of production machinery and production lines, the required number of products for a specified time unit would therefore not be made, which would result in a large company loss. Such fines can be imposed either by the main headquarters of the company if it is a failure of the information system in a branch office, or the fine can also be imposed by the supplier of the material who loses a potential product from his material and thus revenue. [1]

e) The cost of data reconstruction

The cost of data reconstruction can be defined as reasonable costs of restoration and recovery of data from the hardware and software resources. The data loss can occur if the source or carrier where the data are stored or backed up is disrupted. This disruption can be divided into two groups, namely:

1) A mechanical or electronic damage to the disk or memory

2) A software data loss from disk or memory [10]

f) The damage to reputation

The damage to reputation should also be included in the pricing of the company information system. It is primarily for this reason that any security incident in an organization (meaning the cyber risk) can do harm to other entities (companies, suppliers, customers). This harm can be expressed by the loss of existing and future business contacts and ties. When determining the amount that will reflect the damage to reputation, the base should be derived from the defrayed costs of promotion and networking in the business field for a specific time period.

V. Discussion and Further Research

To validate the model, an empirical study is required. We initially discussed with insurance agents and and according our findings most of them fail to understand cyber security. With good preparation (compliance to standards, thorough security audits), certain types of cyber threats can be mitigated. Though some risks still exist, the insurance company should lower the premium for customers with standard compliance. This will encourage more cyber insurance. The analogy is good driver should obtain a better rate for insurance.

VI. Conclusion

We bridged a gap between security standards and cyber insurance by proposing a scoring model for cyber insurance. Our scoring model allows insurance company to intuitively incorporate security standards into the calculation of the premium. When companies are compliant with security standards, they should have a better rate for cyber insurance. As was mentioned before the main benefit of a scoring model is fairness of the price calculation which is a prerequisite for an effective cyber insurance market and transparency for both insurance company and client. Nowadays the calculation of the premium is based on traditional approaches which results in inadequately high price without taking the real level of client´s IT security controls into account.

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. 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.

For example, we can use fuzzy logic for further modelling. Given that this area is not yet designed a uniform methodology for valuing information system is to use pareto analysis, one of the ways to keep their effective decisions backed by scientific method. Identification, analysis and valuation of the assets of the organization is a key activity of the entire methodical process of valuation, since the assets of the organization determine the total cost of the information system. The final amount is then used as a basis for establishing fair amount of coverage in case of realization of cyber risks in the organization

In conclusion, we 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. Our 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.

Acknowledgment

This paper was supported by the TBU IGA project: *Design methodology for determination of prices also of the information system organization in terms of cyber risks*, registred under IGA/FAI/2017/008.

References

[1] Check Point. Check Point 2013 security report. Israel, 2013.

[2] Verizon. 2013 Data breach investigations report. New York, 2013.

[3] Verizon. 2015 Data breach investigations report. New York, 2015.

[4] Naghizadeh, P.; Mingyan Liu, "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

[5] Johnson, B.; Laszka, A.; Grossklags, J., "The Complexity of Estimating Systematic Risk in Networks," Computer Security Foundations Symposium (CSF), 2014 IEEE 27th, vol., no., pp.325, 336, 19-22 July 2014

[6] Pal, R.; Golubchik, L.; Psounis, K.; Pan Hui, "On a way to improve cyber-insurer profits when a security vendor becomes the cyber-insurer," IFIP Networking Conference, 2013, vol., no., pp.1,9, 22-24 May 2013

[7] Schwartz, G.; Shetty, N.; Walrand, J., "Why cyber-insurance contracts fail to reflect cyber-risks,", 2013 51st Annual Allerton Conference on Communication, Control, and Computing, vol., no., pp.781,787, 2-4 Oct. 2013

[8] Sadhukhan, S.K., "Insuring Big Losses Due to Security Breaches through Insurance: A Business Model," System Sciences, 2007. 40th Annual Hawaii International Conference on System Sciences (HICSS'07), vol., no., pp.158a,158a, Jan. 2007

[9] Pandey, P.; Snekkenes, E.A., "Applicability of Prediction Markets in Information Security Risk Management", 2014 25th International Workshop on Database and Expert Systems Applications (DEXA), vol., no., pp.296,300, 1-5 Sept. 2014