Risk Assessment and Verification of Insurability

David Nicolas Bartolini[1], César Benavente-Peces[2] and Andreas Ahrens[3]
[1]*Metafinanz Informationssysteme GmbH, Leopoldstraße 146, 80804 München, Germany*
[2]*Universidad Politécnica de Madrid, Ctra. Valencia. km. 7, 28031 Madrid, Spain*
[3]*Hochschule Wirmar, University of Technology Business and Design, Philipp-Müller-Straße 14, 23966 Wismar, Germany*

Keywords: Cyber Risk Management, Cyber Insurance, Information Security, Data Protection.

Abstract: Nowadays, cyber-risks are an important aspect on the business agenda in every company, but they are difficult to analyze. Cyber-insurance is considered as appropriate means to absorb financial losses caused by computer security breaches. This article explains how a customer and his risks are assessed by an insurance company. It shows which funds the insurer has available to make the risk assessment and thus to check the insurability.

1 INTRODUCTION

Although many cyber insurers are knowing their customers and various insurance contracts have existed for several years, the cyber risk management of the companies to be insured is not well known. This situation is not different for new customers. For this reason, different methods are used in the context of the risk identification in the interaction with the customer to analyze both the risk and the need for protection.

Against this background, the focus of this paper is the presentation of the risk assessment process of a leading insurance company. Which this assessment the insurer can analyse the individual cyber risk.

The remaining part of this paper is structured as follows: In Section 2 the 3 Phases of Risk Assessment is explained, which include the questionnaire about the customer company and the conduct of the insurability test by the security experts in cooperation with, for example, the underwriters of the insurers. The questionnaire used is often based on the ISO/IEC 27001 standard (ISO/IEC 2013). Section 3 introduces to the evaluation of the risk assessment questionnaire results and the insurers risk evaluation methods. This includes the final report. Finally, some concluding remarks are provided in Section 4.

2 THE 3 PHASES OF RISK ASSESSMENTS

First, a workshop is organized at the customer company. The focus is on the customer's advice and less on the sale of the insurance product. This workshop`s intention is customer sensitization to cyber risk management.

This workshop enables the insurer and his underwriters to make a risk and price assessment, which is in the interest and within the framework of the insurance customers, thus enabling a healthy risk portfolio. In return, the prospective customer company receives an objective overview of its cyber risks, which is included in the workshop catalog and presented in the final risk assessment dialogue. By doing so, the customer has an indication of how these risks can be adequately treated.

A questionnaire as well as checklists are called a collection method for risk identification. On the other hand, Delphi methods for the method of creativity and Failure Mode and Effects Analysis (FMEA) belong to the analytical methods (Rausand et al., 2004).

The workshop is part of the risk identification in the context of the insurer's cyber insurance, since it has been established that more complex customer companies can be investigated in more detail and that the underwriter can make a better decision.

This also applies as a valid approach since the cyber risk of a company changes with every change

Bartolini, D., Benavente-Peces, C. and Ahrens, A.
Risk Assessment and Verification of Insurability.
DOI: 10.5220/0006485101050108
In *Proceedings of the 7th International Joint Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2017)*, pages 105-108
ISBN: 978-989-758-266-0

in the business model or business process, as well as with advancing technological development. Furthermore, this is because cyber risk is heavily dependent on soft and hard IT and security management factors (Anderson, 2001).

The workshop`s approach works in two directions. On the one hand, the insurer must know and understand his risk to offer the customer the best possible premium. On the other hand, the insurer is interested in the fact that the customer himself understands his risk and can use it sensibly.

The cyber risk depends on many factors. Therefore, it is important to know the value of the customer. What are these values and what information they contain, plays a key role for the insurer. Therefore, many business units are investigated. It must be ascertained how the control of the IT operation works, since this is an elementary prerequisite for reliable Information Technology.

Furthermore, the company's safety measures must be ascertained. In this case, questioned how segments are arranged and separated from one another, or what possibilities are used to monitor the networks. It is also questioned, for example, whether the data centers are physically and adequately equipped by the supply devices.

The company is also asked about its preparation against cyber-attacks. Therefore, contact persons from business and industrial IT, management reporting, contract management, risk management, business continuity management, information security management, and IT service management will be interviewed to assess the overall risk.

Furthermore, it is essential that the participants of the customer company come from different departments, since cyber-risks are cross-departmental risks (Aguilar, 2014). The Chief Financial Officer is particularly important as she is involved in the management of information security from the business point of view and she is usually responsible for corporate risk management.

Next, the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO) are needed as part of the risk management at the operational level, as they must implement most of the measures.

Since the dependency on suppliers and service providers is sufficient, the head of purchasing department is also an important partner in this workshop.

In this context, the legal department is often involved. This is usually also the point of contact when dealing with questions of the liability of the company in the context of cyber incidents against customers.

During the workshop, the questionnaire is developed in cooperation with the responsible customer. The questionnaire contains questions about the company and closes with the instruction on the precontractual obligation to provide information.

Such a questionnaire was developed by the insurer Cyber Risk Management Team (experts) and is based on the ISO/IEC 27001 standard.

The questionnaire includes the following areas:

The company, its business areas and the company's key figures are dealt with in several points to obtain a quantitative risk approach.

Within a further section, corporate guidelines and procedures are highlighted, and the impact of these guidelines on the company employees.

The specialist also questions whether the company allows cashless payments. This has, inter alia, an impact on possible claims under the payment card industry data security standard (PCI-DSS, 2016) requirements.

A next area of concern is the company's cooperation with external service providers. Furthermore, the customer company is asked if a crisis management plan exists and how the company behaves in case of a crisis.

The next question group deals with questions about pre-claims within the scope of insurance protection and whether known facts have been made available to the customers representative.

Finally, after the company’s data are summarized, the desired insurance sums, deductibles and sublimit are treated.

The customers know that cyber risk is of concern for every business. Thus, they have also agreed to the workshop and have provided their own investments in the form of several resources conducting the workshop.

Therefore, the companies appreciate professional exchange with the experts. The workshops are helpful to understand their own cyber risks and to further perform more effective action. Corporate management is given transparency over cyber risks. This, in turn, helps the IT to gain the necessary attention and acceptance as an important department in the fight against cyber-risks and not to be considered any longer as a cost center.

The evaluation of the customer portfolio and the conduct of the insurability test are carried out by the experts in conjunction with the underwriters of the insurer after the workshop.

3 RISK EVALUATION

The threatened objects are identified, such as the values that affect infrastructure, hardware, buildings as well as software and information. This includes intangible assets, such as the reputation of the company, its employees and, in turn, their knowledge of the threatened objects must also be recorded. With this complete risk knowledge, the value analysis can be done (Turner, 2003).

The values to be protected are evaluated in the value analysis. For this purpose, it is important to measure the interdependencies between the objects. The individual assessment is carried out on both quantitative and qualitative levels. The value of the assets is as much important as the classification (low, medium, high) of it (Schneier et al., 1998).

The threat analysis considers the threats that could affect the objects to be protected. For this purpose, entrance probabilities and damage, which can occur in an event must be estimated. Threats can be caused by technical failure, force majeure, human error, or precautionary action. Organizational deficiencies are also a major part of threat analysis (RFC 2828, 2000).

In classic risk analysis, the individual values should be assessed and a meticulous and comprehensive assessment is to be presented (Rausand, 2011). For each individual object, a strength, weaknesses, opportunity, threat analysis (SWOT analysis) must be conducted. It is necessary to determine who the attackers are and which motives they have. The value or the potential quantitative impact must then be estimated. An assessment (low, medium, high) helps to find an adequately way to protect the most important resources.

The vulnerabilities are like objects. Both have a natural interdependence, and vulnerabilities thus impact objects. Therefore, the objects must be protected because a vulnerability of the input channel is a threat (Foreman, 2010).

For an insurance, quantifiability is a key premise to calculate the insurance premiums (Rokski, 2011). Therefore, an insurance company needs more stochastic values than other companies. For this reason, the questionnaire is oriented to the international standard ISO / IEC 27000 not only as already mentioned, but also by its insurance factors.

The analysis also identifies the current insurance situation. It is important for the insurer that there was no reason for another insurer to neglect the cyber insurance. The information technology incident history is also investigated. Whether business interruption occurred during the last five years. It could be an interesting for the insurer, for example, whether the customer experiences a major disruption incident twice a year, for example in the context of Storage System (RAID 5) failures and limitations of the solid-state disk availability or if information technology failures and cyber-attack occurred. The risk management structure, including the threat and risk modeling and vulnerability management of the customer company, based on the answered questions as well on the public annual reports is carried out.

In addition, the company will be analyzed by means of specific questions as to how the company is positioned within the framework of the Business Continuity Plan. If systems are identified as bottle necks, the experts must check whether the customer can counteract a possible failure, for example by clusters and high availability platforms.

It is also important for the risk assessment to ascertain whether the customer has certified his company according to standards such as ISO 20000, ISO/IEC 27001 or PCI DSS.

As human factor in IT security is a key factor, questions about this area are also important and form the end of the evaluation of the questionnaire. For example, the customer is asked whether awareness training and security training are implemented annually.

4 CONCLUSIONS AND OUTLOOK

Through the risk assessments described, an insurance company can prepare an assessment of cyber risk and then price-setting using premium and risk tables. The premiums for the future require further adjustments to the risk assessment. Demand for cyber insurance is growing steadily in Germany (PWC, 2015). These are glorious prospects for the insurance industry. However, the effects of digitization and the permanent growth of Internet of Things and Cloud Computing, as well as the European General Data Protection Regulation (General Data Protection Regulation, 2016), which will come into force in May 2018, must consider how future damage levels will affect the customers and the insurance companies - this is the roadmap of the future of cyber insurance. Therefore, premiums calculation in context of probable future risk models

and dependencies will be investigated by the team during the further development of the Phd thesis.

REFERENCES

Aguilar, L. A., 2014. *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus,* Cyber-Risks and the Boardroom Conference New York Stock Exchange.

Anderson, R., 2001. *Why information security is hard - an economic perspective,* Computer Security Applications Conference (ACSAC) 2001, Proceedings of the 17th annual computer security applications conference, 358 - 365.

Foreman, P., 2010. *Vulnerability Management,* Taylor & Francis Group.

General Data Protection Regulation, 2016. Final Version http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

Internet Security Glossary, 2000. Internet Engineering Task Force, RFC 2828.

ISO, 2013. ISO/IEC 27001: 2013 Information technology - Security techniques - Information security management systems – Requirements.

Moore, T., 2010. *The economics of cybersecurity: Principles and policy options,* International Journal of Critical Infrastructure Protection, 3 (3-4), 103-117.

PCI/DSS, 2016. Payment Card Industry (PCI) Data Security Standard, v3.2.

PWC, 2015. Insurance 2020 & beyond: Reaping the dividends of cyber resilience.

Rausand, M., 2011. *Risk Assessment: Theory, Methods, and Applications.*

Rausand, M., Hoyal A., Series, W., 2004. *System Reliability Theory: Models, Statistical Methods, and Applications in probability and statistics—second edition, 88.*

Rokski, T., et al., 1999. *Stochastic Processes for Insurance and Finance, 79-94.*

Schneier, B., et al., 1998. *Toward A Secure System Engineering Methodology. National Security Agency*: Washington, 1-11.

Turner, B., et al., 2003. Science and Technology for Sustainable Development Special Feature: *A framework for vulnerability analysis in sustainability science.* Proceedings of the National Academy of Sciences. 100 (14): 8074–8079.

Wallner, J., 2008. Cyber-Risk management, in: *Melnick, E. und B. Everitt: Encyclopedia of quantitative risk analysis and assessment, 429-440, New York.*