Cyber Risk Assessment for Insurability Verification

David Nicolas Bartolini[1], César Benavente-Peces[1] and Andreas Ahrens[2]
[1]*Universidad Politécnica de Madrid, Ctra. Valencia. Km. 7, 28031 Madrid, Spain*
[2]*Hochschule Wismar, University of Applied Sciences - Technology, Business and Design, Philipp-Müller-Straße 14, 23966 Wismar, Germany*

Keywords: Risk Assessment, Information Security, Customer Analysis, Bayes Theorem.

Abstract: Nowadays, cyber-risks are an important aspect on the business agenda in every company, but they are difficult to analyse. Cyber-insurance is considered as appropriate means to absorb financial losses caused by computer security breaches. Cyber security management in a company requires the inter-action of all corporate divisions. To ensure security of wide level at an enterprise, decision-makers must take the necessary measures to avert the dangers of cyber-attacks or, following an attack, take the right steps to manage a damage at the lowest possible level. Within the scope of insurability assessments, Risk Engineers must analyse these measures to perform a cyber insurance acceptance test.

1 INTRODUCTION

Cyber insurance represents a new dynamic segment and a market with considerable potential growth for insurers. Companies estimate that there is a premium potential of at least 700 million euros in Germany by the end of 2018. Many companies, especially small and medium-sized (SME) ones, continue to underestimate the risks associated with using the Internet. In large companies, safety management is in general better trained than in medium-sized companies. However, further challenges for companies are the regulatory challenges in the context of the General Data Protection Regulation (GDPR) and the requirements of the IT (Information Technologies) security law, among others for operators of critical infrastructures. The global network creates problems that have gained significance under the term “cyber risks”. Any company connected to the Internet is vulnerable to intrusions. Attacks on Sony, Google, Amazon and the German Bundestag are few examples which show the dimensions. IT security experts point out that it has become impossible to prevent data breaches. An additional protection is thus a Cyber Police. The focus of this paper is to present a risk-related approach in customer analysis, which helps to assess the question of insurability. The Cyber Risk Dialogue (Bartolini et al., 2017) served to jointly develop the insurance-relevant customer risk. According to the name, a dialogue cannot represent a risk assessment and should also be conducted openly and serve as an exchange between clients and insurers. However, to subsequently implement the insurability check, the findings must be recorded in a structured manner. To guarantee this, an own-used question board is used, which sorts in the respective question categories.

The remaining part of this paper is structured as follows: In Section 2 the cyber risk questionnaire is introduced. In Section 3 the 11 showstopper questions of Risk Assessment are explained, which include the minimum maturity level for each of these questions. These questions used are based on the ISO/IEC 27001 standard (ISO, 2013) and contain elementary security features that a company must meet - other-wise it is not insurable. Finally, some concluding remarks are provided in Section 5.

2 CYBER RISK QUESTIONNAIRE

In general, the questionnaire is structured according to several domains and maturity levels of the respective customer. Each domain and maturity level have many characteristics that are classified according to valuation factors. Statements are categorized to better assess the customer's situation and track common areas across all maturity levels.

Bartolini, D., Benavente-Peces, C. and Ahrens, A.
Cyber Risk Assessment for Insurability Verification.
DOI: 10.5220/0006870900930097
In *Proceedings of the 8th International Joint Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2018)*, pages 93-97
ISBN: 978-989-758-322-3

The components are groups of similar statements to facilitate or comprehensively organize the handling of the assessment. Based on a total of 38 questions (NIST, 2007; NIST, 2008; NIST, 2013a; NIST, 2013b; NIST, 2013c; ISO, 2011; ISO, 2013; ISO, 2015; ISACA, 2012), the findings from the risk dialogue can be systematically entered in the questionnaire by risk assessment engineers. This questionnaire is evaluated by the Cyber Risk Engineer as an assessment. This assessment provides the insurer, and the risk engineer, with a repeatable, reproducible and measurable process to inform underwriters of the client's risks and to assist in verifying the insurability of cyber security. The cybersecurity maturity level includes domains, valuation factors, components and individual implementations of measures across the four levels of responsiveness to identify specific controls and practices. Each maturity level contains a descriptive characteristic or just a characteristic describing the customer's behaviour. The practices and processes of a customer consistently lead to the final overall result. The assessment combines information regarding security relevant standards such as ISO 27001, NIST, BSI Standard, Cobit, etc., and thus enables cyber security assessment. NIST (NIST, 2013c) defines cybersecurity as "the process of protecting information through prevention". Cyber events can have financial, operational, legal and reputational implications. Cyber incidents can have a significant impact on corporate capital. Costs may include forensic investigations, Public Relation campaigns, legal fees and court fees, consumer credit monitoring, technology changes and comprehensive recovery measures (Eckert, 2014; AGCS, 2016) Cybersecurity therefore needs to be integrated across the enterprise as part of corporate governance processes, information security, business continuity and third-party risk management. Cybersecurity roles and processes referred to in the assessment may be separate roles within the security group (or outsourced) or may be part of broader roles within the institution. Each question contains four different answer options, which correspond to the respective risk situation of the customer. The Risk Engineer determines which category best suits the client's current practices. All statements in each domain and in all included levels must be answered and classified qualitatively to achieve the best possible maturity of this domain. The Risk Engineer can determine the maturity level of the customer in each area, but the assessment is not intended to determine a general maturity level of cyber security only based on these 38 questions in an equally weighted form. On the one hand, domains must be excluded which do not apply to the respective customer, for example if outsourcing is not carried out. Questions or domains that are not applicable to the respective customer have no influence on the determination of the specific insurance capability. In principle, however, an equivalent quantification of the rating can be made from 38 of the above-mentioned questions. The questionnaire is logically staggered so that a rating can be made based on the respective maturity of the answers (between 1 = weak maturity and 4 = strong maturity). This can be calculated using the arithmetic mean. If the minimum rating value (> 2.00) is reached, the company is generally insurable.

However, the risk engineers have incorporated an exception to this fundamental weighting in the risk assessment, since there are 11 show stopper topics (Table 1) within the questions or domains, which must be considered separately.

Table 1: Showstoppers.

Showstopper	Minimum
Does a security organization with defined roles and responsibilities exist?	2
Do employees succeed in raising awareness and training on information security and cyber-security?	3
Are there any specifications for the secure basic configuration (hardening) of IT systems?	2
Is malware protection implemented in your company?	2
Are there any procedures for patch and vulnerability management?	3
Are backups regularly performed and tested?	3
How are external accesses secured?	3
Are data transfers over unsecured networks protected?	2
Does the processing of information in the public cloud take place according to the requirements of your information security?	2
Have password quality requirements been implemented?	2
Have physical security zones been defined?	2

The inherent risk profile and maturity of a company may change over time as threats, vulnerabilities and operating environments change, but fundamental domains and levels of maturity are a prerequisite for a company's cybersecurity, which is categorized as a show stopper.

3 SHOWSTOPPERS

Why these 11 questions are classified as so-called showstoppers and why a minimum degree of maturity per area is necessary is explained in the following four showstopper explanations.

3.1 Does a Security Organization with Defined Roles and Responsibilities Exist?

Since the customer must take a holistic approach to cyber security, it is necessary that basic roles within a security organization must be named. The entrepreneur is therefore responsible for the organization of IT security in his company, but he cannot manage the task alone: the development of an IT security organization is necessary (Harris and Maymi, 2016). Depending on the size of the company, there are distinctive characteristics that can be considered. In a small company with 10 to 20 employees, it is hardly possible to create jobs that deal exclusively with the topic of IT security. Medium-sized companies may have the financial means and the need for one or two full-time IT security jobs. International corporations cannot do without an extensive IT security organization. In general, IT security must be exemplified. Management must make the decisions, set precise targets and, of course, set a good example for implementation. In addition, IT security must be carried to all areas of the company, and it must be made clear that every employee is part of the IT security organization. An IT security officer should be appointed, even if not required by law (BSI, 2017). This can be an own employee or an external service provider.

For core tasks, suitable employees must be appointed and equipped with sufficient skills. This is the only way to enforce the guidelines. It goes without saying that the responsible employee must be given the necessary freedom to perform his or her duties adequately. Separation of functions is essential. For example, the IT administrator may not be responsible for creating IT security policies at the same time (ISO, 2013). All employees and executives (including management staff) must be regularly updated of the importance of compliance with the established guidelines (e.g. COSO, 1992). This can be done through training, but better through advanced training or even small IT security competitions.

3.2 Do Employees Succeed in Raising Awareness and Training on Information Security and Cyber-security?

Adverse behaviour is the most common cause of damage. Human beings continue to be the greatest vulnerability in IT and non-digital information security. Whether out of good faith, ignorance or bad faith - confidential company data quickly falls into the wrong hands or the network is infected (Warren and Bayuk, 2009). For example, phishing e-mail addresses are a widespread form of social engineering. Probably every user has already found such an email in his/her inbox. They can be used to pretend that you have completed a transaction on eBay, Amazon or PayPal with errors. You should correct this by visiting the site. If users follow this call, they will come across a website that looks very similar to the original. There they are asked to enter passwords or Transaction Authentication Numbers (TANs). If now actually functioning Account-data is revealed, the theft starts on the real account.

Detection of the fake website is usually easy, indications are, for example, security certificates expired, faulty or not available at all. URL or domain of the website seem strange, like amazon.tv. There are spelling mistakes in the e-mail and on the website. Also, not to be despised are USB sticks that seem to have been left lying on the company car park or in publicly accessible areas of the company (Harris and Maymi, 2016). If the curious finder connects such a stick to the computer, she will catch a sophisticated Malware or Ransomware and possibly infect a large part of the company network. Finally, tempting are the documents contained therein, such as the alleged salary list of the Executive Board or the candidates for an upcoming wave of redundancies. It is assumed that the state-contracted malware Stuxnet also entered the Iranian atomic plant Natanz via USB stick (Kushner, 2014).

However, no matter how an attack takes place or how you assess the threat situation: it is important that companies take themselves out of liability as far as possible and if they have established a comprehensive training and awareness-raising program, claims for damages can be passed on directly to the perpetrator. Incidentally, this is also the only sensible method of protecting oneself against any form of social engineering. There are many technical measures to filter e-mails or control accessed websites, but ultimately the user remains the weakest link in the chain. It is therefore important that companies achieve the required maturity level in risk assessment.

3.3 Are There Any Specifications for the Secure Basic Configuration (Hardening) of IT Systems?

All measures taken in individual cases can only be effective to a fraction of their effectiveness as long as the systems or system components on which they are

based and the respective application to be secured are not sufficiently robust and based on a system environment that is secured in principle (Eckert, 2014; NIST, 2008). For example, it is not sufficient to protect a database against unauthorized access if the operating system allows "anonymous" access at any time. The attacker/hacker will initially gain access to the relevant machines via the operating system and will try to gain access to the database contents from there. In a large UNIX installation, SSH is used for terminal access to the machines. The machines are protected by a firewall, both externally (outside the company) and in the direction of the internal LAN. Access to the machines is mainly necessary for administrative tasks, also from the company or from outside. Each access must be explicitly requested and activated at the Firewall Administration. By default, both SSH and the "r" commands (rsh, rexec, rcp, rlogin) are applied for with each new access - and unlocked by mistake. The configuration of the SSH servers is often superficial - the authentication mechanisms required in the standard distribution are optionally configured, and users are also allowed to use. Cases such as these are avoided with an existing basic coverage or hardening. Customers need to know and secure concrete operating system architectures as well as the general system and basic services they use - a firewall without con-figuration also offers no protection, just as systems without hardening. Initial hardening of the systems must be carried out to achieve the necessary maturity level.

3.4 Is Malware Protection Implemented in Your Company?

Because malicious code is one of the most important tools used by attackers (OWASP, 2017), the customer must take appropriate countermeasures and reach the minimum maturity level. Every company should put together appropriate preventive measures against malware and regulate how it should be handled in the event of a malware infection. In addition to the classic computer viruses, malware also includes Trojan horses, computer worms and malicious software causing Ransomware (Eckert, 2014). A security concept against malware should be developed as a basis for preventing the intrusion of malware into IT systems. Aware of the residual risk, measures must be taken to prevent the intrusion of malicious programs. If a preventive defence is not successful, the intrusion of malware should be detected as early as possible. The consistent application of the measures and constant updating of the technical methods used are essential. This requirement is due to the daily occurrence of new malware or new variations of known malware. The further development of operating systems, programming languages and application programs regularly leads to new attack potential for malware, so that appropriate counter-measures must be initiated.

4 CONCLUSIONS AND OUTLOOK

Depending on the customer's needs and wishes, the Risk Engineer can formulate improvements for each domain or across domains. A gap analysis can be created between the current and the target maturity level. Based on this, the customer can initiate improvements based on the gaps. Any organizational or technical weakness can necessitate many strategies and processes that have an enterprise-wide impact. For example, feedback from risk engineers on individual domains that do not yet reach the maturity required can provide insight into new policies, processes, procedures and controls that can improve risk management about a risk or the customer's overall cyber-security readiness.

Further work will focus, on the one hand, on the development potential of loss probabilities in selected industries. This includes possible data mining strategies on collected data breach information. On the other hand, future cyber insurance products will also have to focus more on the effects of the GDPR. For this reason, data privacy and information security requirements will also be addressed in the further work and the challenges will be worked out, as well as additional and necessary showstopper questions will be developed.

REFERENCES

Allianz Global Corporate and Speciality (AGCS), 2016. *Allianz Risk Barometer*. Retrieved on May 30, 2018 from http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2016/.

Bartolini, D., Ahrens, A., Benavente-Peces, C., 2017. Risk Assessment and Verification of Insurability. In Proceedings of the 7th International Joint Conference on *Pervasive and Embedded Computing and Communication Systems* - Volume 1: SPCS, 105-108, 2017, Madrid, Spain.

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017. *Leitfaden zur Basis-Absicherung nach IT-Grundschutz*. Retrieved on May 30, 2018 from

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3.

COSO, 1992. *The Committee of Sponsoring Organizations of the Treadway Commission*. Retrieved on May 30, 2018 from https://www.coso.org/Pages/erm-integratedframework.aspx.

Eckert, C., 2014. *IT Security – Concepts, Procedures and Protocols*. DE GRUYTER OLDENBOURG.

Harris, S., Maymi, F., 2016. *Certified Information System Security Professional.* New-York: McGraw – Hill Education.

ISACA, 2012. *Cobit 5 Framework*. Retrieved on May 30, 2018 from https://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx.

ISO, 2011. ISO/IEC 20000-1:2011. Information technology – Service Management. Retrieved on May 30, 2018 from https://www.iso.org/standard/51986.html.

ISO, 2013. ISO/IEC 27001: 2013. Information technology - Security techniques - Information security management systems – Requirements. Retrieved on May 30, 2018 from https://www.iso.org/standard/54534.html.

ISO, 2015. ISO/IEC 27017: 2015. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud security services. Retrieved on May 30, 2018 from https://www.iso.org/standard/43757.html.

Kushner, D., 2014. The Real Story of Stuxnet, *IEEE Spectrum*.

NIST, 2007. NIST 800-45: Guideline on Electronic Mail Security. Retrieved on May 30, 2018 from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-45ver2.pdf.

NIST, 2008. NIST 800-123: Guide to General Server Security. Retrieved on May 30, 2018 from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf.

NIST, 2013a. NIST 500-291: NIST Cloud Computing Standards Roadmap. Retrieved on May 30, 2018 from https://www.nist.gov/publications/nist-sp-500-291-nist-cloud-computing-standards-roadmap.

NIST, 2013b. NIST 800-40: Guide to Enterprise Patch Management Technologies. Retrieved on May 30, 2018 from https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final

NIST, 2013c. NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. Retrieved on May 30, 2018 from https://nvd.nist.gov/800-53

Open Web Application Security Project (OWASP), 2017. Retrieved on May 30, 2018 from https://www.owasp.org/index.php/Main_Page

Warren, C., Bayuk, J.L., Schutzer, D., 2009. Enterprise Information Security and Privacy. *Artech House, Inc. Norwood*, MA, USA ©2009.