DOI: 10.5604/01.3001.0012.5274

INSTRUMENT DESIGN FOR CYBER RISK ASSESSMENT IN INSURABILITY VERIFICATION

David Nicolas Bartolini[1], Andreas Ahrens[2], Jelena Zascerinska[2]
[1]Universidad Politécnica de Madrid, [2]Hochschule Wismar, University of Applied Sciences, Technology, Business and Design

Abstract. *Cyber risk assessment for insurability verification has been paid a lot of research interest as cyber insurance represents a new dynamic segment of market with considerable growth potential for insurers. As customer's practices and processes consistently lead to the final overall result, customer's behaviour has to be described in detail. The aim of the present paper is to design an instrument (questionnaire) for customer's cyber risk assessment in insurability verification. The method for building an instrument (questionnaire) is empirical research. Empirical research is based on use of empirical evidence. A questionnaire with 11 questions is proposed.*

Keywords: cyber risk management, cyber insurance, information security, data protection

PROJEKTOWANIE INSTRUMENTÓW PRZEZNACZONYCH DO OCENY ZAGROŻENIA RYZYKA CYBERNETYCZNEGO W WERYFIKACJI UBEZPIECZALNOŚCI

Streszczenie. *Ocena ryzyka związana z bezpieczeństwem cybernetycznym jest przedmiotem dużego zainteresowania badawczego, ze względu na to, że bezpieczeństwo cybernetyczne stanowi nowy, dynamiczny segment rynku o znacznym potencjale wzrostu dla ubezpieczycieli. Ponieważ praktyki i procesy klienta w ciągły sposób wpływają na końcową ocenę, zachowanie klienta musi być szczegółowo opisane. Celem niniejszego artykułu jest opracowanie instrumentu (kwestionariusza) do oceny ryzyka cybernetycznego klienta w ramach weryfikacji ubezpieczenia. Metoda budowy instrumentu (kwestionariusz) to badania empiryczne. Badania empiryczne opierają się na wykorzystaniu dowodów empirycznych. Zaproponowano kwestionariusz składający się z 11 pytań.*

Słowa kluczowe: zarządzenie ryzykiem cybernetycznym, ubezpieczenie cybernetyczne, bezpieczeństwo informacji, ochrona danych

Introduction

Cyber risk assessment for insurability verification has been paid a lot of research interest as cyber insurance represents a new dynamic segment of market with considerable growth potential for insurers. Companies estimate a premium potential of at least 700 million euros in Germany by the end of 2018. Many companies, especially small and medium-sized ones, continue to underestimate risks associated with using the Internet. In large companies, safety management is in general better trained in comparison to medium-sized companies. But further challenges for companies are regulatory challenges in the context of General Data Protection Regulation (GDPR) and requirements of the IT 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. Attacks on Sony, Google, Amazon and German Bundestag show the dimensions. Thus, a number of approaches, methods, tools and instruments have been developed for organisation's cyber risk assessment in insurability verification. However, as customer's practices and processes in an organisation consistently lead to the final overall result, customer's behavior has to be described in detail. Assessment combines information security relevant standards such as ISO 27001, NIST, BSI Standard, Cobit, etc. and enables cyber security assessment. Cybersecurity is "the process of protecting information through prevention" [10]. 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, PR campaigns, legal fees and court fees, consumer credit monitoring, technology changes and comprehensive recovery measures [2]. 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 have separate roles within the security group (or outsourced) or may be part of broader roles in an organisation. As IT security experts point out that it has become impossible to prevent data breaches, each organisation is considered to be unique that demands on an individual approach. For these purposes, Cyber Risk Dialogue to identify jointly insurance-relevant customer risks was elaborated [1]. According to Cyber Risk Dialogue [1], a dialogue cannot represent a risk assessment and should also be conducted openly and serve as an exchange between clients and insurers. Cyber Risk Dialogue [1] is based on such an instrument as questionnaire.

The aim of the present paper is to design an instrument (questionnaire) for customer's cyber risk assessment in insurability verification. The method, an instrument (questionnaire) for customer's cyber risk assessment in insurability verification is built, is identified as empirical research. Empirical research employs the use of empirical evidence, namely gaining knowledge by means of direct and indirect observation or experience.

1. Questionnaire design

The questionnaire is structured according to such domains and maturity levels of the respective customer as Existing certifications, IT security Organisation (IT security and risk management), Awareness for information security, Use of external service providers and contract management, Protection of IT systems, Network protection, Detection of attacks, Data management and storage, Access and access protection, and Physical security.

Each domain and maturity level have characteristics that are classified according to valuation factors. Statements are categorized to assess customer's situation and track common areas across all maturity levels. Components are groups of similar statements to facilitate or comprehensively organize the handling of assessment. Based on a total of 38 questions (according to [5–11]), the questionnaire could be filled in with the findings from the risk dialogue by the risk engineer. This questionnaire is assessed by the Cyber Risk Engineer. This assessment provides the insurer, and risk engineer, with a repeatable, reproducible and measurable process to inform underwriters of client's risks and to assist in verifying insurability of cyber security. Cybersecurity maturity level includes domains, valuation factors, components and individual implementations of measures across four levels of responsiveness to identify specific controls and practices. Each maturity level contains a descriptive characteristic or a characteristic. Each of the questions contains four different answer options, which correspond to the respective risk situation of customer. Risk Engineer determines which category client's current practices best suit. All statements in each domain and in all included levels must be answered and classified qualitatively to achieve a best possible maturity of this domain. Risk Engineer can determine a maturity level of customer in each area, but 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 which do not apply to the respective customer must be excluded, 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 specific insurance capability.

In principle, an equivalent quantification of rating can be made from 38 questions. Questionnaire is logically staggered so that a rating can be made based on the respective maturity of answers (between 1 = weak maturity and 4 = strong maturity). This can be calculated using the arithmetic mean formula:

$$\bar{x}_{\text{arithm}} = \frac{1}{n}\sum_{i=1}^{n} x_i = \frac{x_1 + x_2 + \cdots + x_n}{n} \tag{1}$$

If the minimum rating value (> 2.00) is reached, the company is generally insurable.

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

Inherent risk profile and company's maturity may change over time as threats, vulnerabilities and operating environments change. However, fundamental domains and maturity's levels are a prerequisite for company's cybersecurity, categorized as a show stopper.

2. Show stopper description

The present part of the paper clarifies the choice of 11 questions classified as show stoppers and requirements to their minimum degree of maturity per area:

Does a security organization with defined roles and responsibilities exist?

Table 1. Showstopper

Showstopper / Questions	Minimum rating value
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 own information security?	2
Have password quality requirements been implemented?	2
Have physical security zones been defined?	2

Since customer must take a holistic approach to cyber security, identification of basic roles within a security organization is important.

The entrepreneur is therefore responsible for the organization of IT security in his/her company, but s/he cannot manage the task alone: the development of an IT security organization is necessary [4]. Depending on the company's size, there are distinctive characteristics to be considered. In a small company between 10 to 20 employees, it is difficult to create jobs that deal exclusively with the topic of IT security. Medium-sized companies may have 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 decisions, set precise targets and of course, set a good example for implementation. In addition, IT security must be carried to all company's areas, 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. 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. Responsible employee must be given a necessary freedom to perform his/her duties adequately. Separation of functions is essential. For example, IT administrator may not be responsible for creating IT security policies at the same time [6]. All employees and executives (including management) must be regularly informed of the importance of compliance with the guidelines (e.g. SOX 2002, COSO 1992). This can be done through training, but better through advanced training or even small IT security competitions.

Do employees succeed in raising awareness and training on information security and cyber-security?

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 [14]. For example, phishing mails are a widespread form of social engineering, detection of the fake website, USB sticks left lying on the company's car park or in publicly accessible areas of the company [4], documents such as alleged salary list of the Executive Board or candidates for an upcoming wave of redundancies. There are many technical measures, but ultimately the user remains the weakest link in the chain.

Probably every user has already found such an email in 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 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. 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.

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.

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 systems or system components, on which they are based, and respective application

to be secured are not sufficiently robust and built on a system environment that is secured in principle [2, 8]. For example, it is not sufficient to protect a database against unauthorized access if the operating system allows "anonymous" access at any time. Customers need to know and secure concrete operating system architectures as well as the general system and basic services they use.

Is malware protection implemented in your company?

As malicious code is one of the most important tools used by attackers [12], customer must take appropriate countermeasures and reach the minimum maturity level.

Because malicious code is one of the most important tools used by attackers, 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. 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 defense 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.

Are there any procedures for patch and vulnerability management?

Since vulnerable software is a risk, a controlled process for patch management must be in place at customer's premises. Patch management is the process that evaluates, controls and installs software updates during operations. This ensures the functionality of used software components, eliminates security gaps and thus increases the stability of the production environment. Use of outdated software and resulting adverse effects on system security can have a negative impact on interruption of business-critical infrastructures, data theft and data integrity, etc. In addition to hardware and software specifications, these include dependencies among each other. By means of a patch management process, company ensures the best possible security process and reduces risk.

Are backups regularly performed and tested?

Regular data backups must be performed to avoid data loss. In most computer systems, these can be largely automated. Rules must be set to determine which data is backed up by whom and when. All users should be informed about the rules for data backup to be able to point out any shortcomings (e. g. too little time interval for their needs) or to be able to make individual additions (e. g. mirroring important data on their own disk). Confidential data should be encrypted before the backup to ensure decryption even after a longer period.

How are external accesses secured?

Remote maintenance of IT systems involves security risks. In case of remote maintenance, a distinction must be made between internal and external maintenance personnel accessing the IT systems [1].

Are data transfers over unsecured networks protected?

In the age of digitalization, data are constantly in motion. They are transferred from one point to the next via different devices. End-to-end encryption is an effective protection measure for communication via e-mail.

Does the processing of information in the public cloud take place according to the requirements of your own information security?

Various alternatives for cloud computing must be developed on a broad scale and subjected to a security analysis adapted to customer's organization. Distinguishing features of the alternatives include, among other things, localities of the data centers, options for restricting the public cloud to specific regions, control options for the data flow and service levels offered [3, 7]. Contracts and service level agreements (SLAs) describe a complete and controllable service to guarantee quality and information security in the public cloud. It is also important to have own audit rights, key figures, migration and above all the regulations for terminating the contractual relationship.

Have password quality requirements been implemented?

Insecure passwords can be found quickly by crackers via simply trying them out (e. g. brute force attack, dictionary attack). The risk of becoming a victim of such an attack can be significantly reduced by users' changing their passwords on a regular basis, paying attention to the security of passwords [6, 9, 10, 11, 13]. A formal management process for the authentication information is required [7].

Have physical security zones been defined?

The Physical Security monitoring area deals with all aspects of secure organizational environment. The monitoring area is divided into two fields, namely Securing Areas, such as Entrance Areas and Rooms, and Securing the Equipment from Theft, Misuse, etc. Entrance controls ensure access to sensitive organizational areas. Technically based solutions are available in the form of terminals up to contactless detection. Earthquakes, tsunami, war or a fire can also have devastating effects. As a result, data and data media should be stored securely, the data center should be securely equipped, and all backup media should be stored at different (but also secured) location [1]. Equally important are various cable connections (power, fiber optic and copper cables for data transmission). The equipment required in a data center, such as air conditioning, emergency generators, UPS, ventilation, water supply, sewage, fire alarm system (incl. smoke detector, fire extinguisher and sprinkler system) and telecommunications must be checked and maintained [4]. Depending on the need for security, replacement systems should also be available. The most important protection against unauthorized persons is the sensitization of employees. To achieve the best level in the maturity model, the lifecycle model (Plan-Do-Check-Act) requires ongoing monitoring and maintenance. Insurability can already be reached (minimum 2) beforehand.

3. Remarks and conclusion

Instrument (questionnaire with 11 questions) has been designed. Depending on the customer's needs and wishes, 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. Customer can initiate improvements based on the identified gaps. Any organizational or technical weakness can necessitate many strategies and processes that have an enterprise-wide impact. For example, risk engineers' feedback on individual domains that do not reach yet a required maturity can provide insight into new policies, processes, procedures and controls to 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's. 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

[1] Bartolini D., Ahrens A., Benavente-Peces, C.: Risk Assessment and Verification of Insurability. In: International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS), Madrid (Spanien). 2017, 24–26.
[2] Eckert C.: IT Security – Concepts, Procedures and Protocols. De Gruyter Oldenbourg, 2014.
[3] Official Journal of the European Union: General Data Protection Regulation. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf, 2016.
[4] Meyers M., Harris S., a Campo Rössing: CISSP: Certified Information Systems Security Professional (mitp Professional) Broschiert, 9 März 2009.
[5] ISACA, 2012, Cobit 5 Framework.
[6] ISO 2013. ISO/IEC 27001: 2013. Information technology – Security techniques – Information security management systems – Requirements.
[7] ISO 2015. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud security services.
[8] NIST 2008. NIST 800-123: Guide to General Server Security.
[9] NIST 2013. NIST 800-40: Guide to Enterprise Patch Management Technologies.
[10] NIST 2013. NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations.
[11] NIST 2013. NIST 500-291: NIST Cloud Computing Standards Roadmap.
[12] Open Web Application Security Project (OWASP), 2017.
[13] PCI/DSS, 2016. Payment Card Industry (PCI) Data Security Standard, v3.2.
[14] Warren C., et. al.: Enterprise Information Security and Privacy, 2009, 193–199.

M.Sc. David Nicolas Bartolini
e-mail: davidnicolas.bartolini@alumnos.upm.es

David Nicolas Bartolini received the Master of Science degree in Business Informatics from University of Wismar, Germany, in 2017. Currently, he is a Ph.D. student at the Polytechnic University of Madrid, Spain. His main field of interest include Cyber Risk Management, Cyber Insurance and Machine Learning.

Prof. Dr.-Ing. habil. Andreas Ahrens
e-mail: andreas.ahrens@hs-wismar.de

Andreas Ahrens received the Dr.-Ing. and Dr.-Ing. habil. degree from the University of Rostock in 2000 and 2003, respectively. In 2008, he became a Professor for Signal and System theory at the Hochschule Wismar, University of Technology, Business and Design, Germany. His main field of interest includes error correcting codes, multiple-input multiple-output systems, iterative detection for both wireline and wireless communication as well as social computing.

Dr. Jelena Zascerinska
e-mail: knezna@inbox.lv

Jeļena Zaščerinska was awarded Dr. Degree from University of Latvia in 2011. In 2012 she became a leading researcher at Centre for Education and Innovation Research, Latvia. She received research grants. In 2012 she was bestowed expert rights by Latvian Council of Science, in 2013 – by Horizon 2020, in 2017 – by National Science Centre, Krakow, Poland. Since 2013 she has been actively acting as Editorial Board Member and Reviewer in international scientific journals.

otrzymano/received: 1.08.2018 *przyjęto do druku/accepted: 15.09.2018*