FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

RECHTS- UND WIRTSCHAFTS-
WISSENSCHAFTLICHE FAKULTÄT

Components and Challenges of Integrated Cyber Risk Management

Thomas Kosub

Working Paper

Department of Insurance Economics and Risk Management
Friedrich-Alexander University Erlangen-Nürnberg (FAU)

Version: April 2015

COMPONENTS AND CHALLENGES OF INTEGRATED CYBER RISK MANAGEMENT

Thomas Kosub*

This version: April 3, 2015

ABSTRACT

Cyber risk has become increasingly important as the severity and frequency of cyber incidents is steadily on the rise. Cyber risk management is thus a necessity for businesses to ensure firms' stability and operability, which is partially even required by law. Therefore, this paper focuses on the major components of an effective cyber risk management process. This is done based on a comprehensive review of the academic literature and relevant frameworks (ISO/IEC 27000 series) and by outlining the cyber risk management process step by step. In addition, we discuss existing challenges and problems of cyber risk management. The study emphasizes that a comprehensive management of cyber risks needs well-designed internal risk management structures as well as adequate awareness for such threats.

1. INTRODUCTION

Cyber risks are amongst the most underestimated business risks for 2013, according to the global Allianz survey of 500 Allianz corporate insurance experts, even though cyber risks can result in serious business risks, leading, e.g., to business interruption or major reputational damage.[1] This may consequently cause even larger losses than traditional industrial risks.[2] The current underestimation of cyber risks appears questionable, as cyber risks were first mentioned as early as 1995, when Internet growth began with the release of the Internet Explorer 1.0.[3]

In this regard, risk transfer solutions such as "hacker insurance" policies as a particular risk management tool were already being offered in the US insurance market in 1998 by ICSA TruSecure, Cigna Corp/Cisco Systems/NetSolve, or J. S. Wurzler Underwriting, for instance.[4]

* Thomas Kosub is at the Friedrich-Alexander University Erlangen-Nürnberg (FAU), Germany, Department of Insurance Economics and Risk Management, Lange Gasse 20, D-90403 Nürnberg. thomas.kosub@fau.de.

1 See http://www.agcs.allianz.com, access 06/18/2013.

2 See Behrends (2013, p. 25), Sinanaj and Muntermann (2013, p. 88).

3 See Njegomir and Marović (2012, p. 140).

4 See Majuca, Yurcik, and Kesan (2006, p. 5).

However, technological growth, as well as the increasing number of private and business Internet users, seems to not have yet entirely adapted to this major risk factor. This is also confirmed by a study among 200 German Chief Information Officers and Chief Technology Officers, in which 45 % of the respondents did not prioritize cyber security due to the lack of an immediate threat and 18 % lacked understanding of cyber risks.[5] In addition, Biener et al. (2015, pp. 82, 93) conduct two surveys among various firms (16 employees from the financial sector, 22 employees from small and medium-sized enterprises) and find that cyber risks are identified as major threats by businesses, but that most businesses feel well protected against cyber risks and do not require cyber insurance protection. Based on a third survey among four insurance providers offering cyber insurance in Switzerland, the authors find that for many businesses, the management of cyber risks requires considerable improvement and that a blend of preventative measures and risk transfer risk is considered as the most effective way of cyber risk management.

The relevance of cyber risks and adequate cyber risk management is also of increasing relevance for policymakers.[6] Recently, the German Federal Ministry of the Interior announced the implementation of an IT Security Law (IT-Sicherheitsgesetz), aiming to significantly improve confidentiality, integrity and availability of data processing IT systems.[7] In addition, many countries (more than 50) have published strategic proposals on cyber security and cyber risks as well.[8] The importance of cyber risk management is additionally promoted by regulatory changes and tightened laws, e.g., on data privacy protection. In the particular case of Germany, criminal acts involving alteration of data or sabotage of computers are cited in the German criminal code (Strafgesetzbuch §202a, 202b, 202c (“*hackerparagraph”*), 303a, 303b). Furthermore, privacy protection is regulated by the German Federal Data Protection Act (Bundesdatenschutzgesetz). Therein, Article §43 (3) states that monetary fines can be imposed of up to 300,000 Euros for deliberate or negligent privacy protection violation.[9] With the planned implementation of the European General Data Protection Regulation expected in 2015, penalty levels will generally increase; for example, the monetary fine will be up to one million Euros or 2 %[10] of the worldwide annual turnover of the company responsible for the

---

5 See http://www.roberthalf.de/id/PR-04055/cyber-security-unterschaetzt, access 01/27/2015.

6 See Dowdy (2012, p. 129).

7 See Federal Ministry of the Interior (2014, p. 1).

8 See von Solms and van Niekerk (2013, p. 97).

9 See German Federal Data Protection Act (2009), Haas and Hofmann (2014).

10 See European General Data Protection Regulation. With the first unofficial consolidated version of the European General Data Protection Regulation, the European Commission is adjusting the fine up to 5 % of annual worldwide turnover, or up to 100,000,000 Euros, whichever is the larger value (see http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf, access 03/04/2014).

violation.[11] In addition, any privacy data violations will have to be reported, if feasible, to the supervisory authority within 24 hours of detection.[12] Such regulatory restrictions will certainly support the further development of cyber risk management frameworks and encourage companies to transfer risks towards insurers via cyber insurance, as cyber risks may harm company values and thus directly influence the company's reputation.[13] The increasing severity and frequency of cyber incidents thus induces a strong need for a sound and integrated cyber risk management as one vital part of a holistic enterprise risk management framework.

In the literature, cyber risk management as well as cyber insurance as a particular risk transfer tool have been analyzed, focusing particularly on the correct pricing of cyber insurance (e.g., Herath and Herath, 2011) and the adequate loss valuation of cyber crime (e.g., Smith, 2004), general risk management approaches (e.g., Gordon, Loeb and Sohail, 2003), correlation of cyber risk-classes and interdependencies (e.g., Böhme, 2005; Böhme and Kataria, 2006; Wang and Kim, 2009) as well as, e.g., the reactions on the capital market after the announcement of such cyber incidents (e.g., Campbell et al., 2003; Cavusoglu, Mishra, and Raghunathan, 2004b; Hovay and D'Arcy, 2003). Empirical findings reveal that security breaches directly show negative market reactions for the firm's stock market valuations. Cavusoglu, Mishra, and Raghunathan (2004b) state that costs among the different types of security breaches do not differ and find that market value drops by 2.1 % over two days after the announcement of the security breach. Campbell et al. (2003) only find significant negative market reactions for particular security breaches, in which access to confidential data has been granted. Focusing on insurance for the management of cyber risks, Biener, Eling, and Wirfs (2015) provide an empirical analysis of the insurability of cyber risks. With regard to risk management of cyber risks in general, Tuttle and Vandervelde (2007), for example, empirically examine the COBIT framework as an internal control instance for IT. Siegel, Sagalow and Serritella (2002) also focus on cyber risk management and present a risk management approach, and also consider cyber insurance as well as technical controls to manage risks. In addition, Bodin, Gordon and Loeb (2008) introduce a new risk metric as a decision-making tool for, e.g., IT security management. A comprehensive tabular overview of findings from the literature is presented in Table A.1 (see Appendix).[14] This paper aims to contribute to the

---

[11] See European Commission (2012, pp. 92-93).

[12] According to the European General Data Protection Regulation, see European Commission (2012, p. 28).. With the current data protection laws, only personal data violations have to be reported immediately (see §42a German Federal Data Protection Act; Behrends, 2013, p. 25).

[13] See Behrends (2013, p. 25), IBM (2012, p. 3). See also Gatzert, Schmit, and Kolb (2013) for specific information on reputation risks.

[14] Table A.1a (see Appendix) shows selected findings from the academic literature focusing on cyber risk management and cyber insurance, briefly summarizing the main findings and risk management approaches among different researchers. Table A.1b further summarizes practical literature and industry studies on cyber risks.

literature by providing a structured review of the academic literature and the relevant components of an integrated cyber risk management (based on the ISO/IEC 27000 series). In comparison to Biener et al. (2015), for instance, who focus on the risk management and the insurability of cyber risks, this paper primarily focuses on the cyber risk management process and links the different cyber risk management steps with findings from the academic literature and the ISO/IEC 27000 series of standards. We further discuss existing challenges associated with cyber risk management.

The remainder of this paper is structured as follows. Section 2 focuses on the definitions, the cyber terminology and the different types of cyber risk. In Section 3, the main components of a holistic risk management process with a specific focus on cyber risk management are presented, by combining the findings from the literature and current frameworks (focusing on the ISO/IEC 27000 series). Challenges associated with cyber risk management are discussed in Section 4, and Section 5 concludes.

2. Definition, Growth and Threats of Cyber Risks

One definition of the term *cyber* (an abbreviation for *cyber space*) encompasses all digital networks required for storage, modification and communication of information.[15] The National Institute of Standards and Technology (NIST) defines cyber space as "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[16]

Returning to the actual definition of *cyber risks*, one can treat them in a narrow or broader sense.[17] For instance, Öğüt, Raghunathan, and Menon (2011) use information security as a synonym for cyber risks, while Mukhopadhyay et al. (2013) define the involvement of malicious electronic events (as a cause of disruption to business and financial losses) as a cyber risk. For the categorization of cyber risks, an operational clustering approach is used by Biener, Eling, and Wirfs (2015) (based on Cebula and Young, 2010) whereby the authors empirically study cyber risks based on operational risk data. The authors classify operational cyber threats into four cyber security risks, which comprise (1) actions of people, (2) systems and technology failures, (3) failed internal processes and (4) external events.[18]

---

[15] See Biener, Eling, and Wirfs (2015, p. 132), Cabinet Office (2011, p. 11).

[16] See NIST (2013, p. 58).

[17] See Biener, Eling, and Wirfs (2015, p. 132), Hult and Sivanesan (2013, p. 97).

[18] See Biener, Eling, and Wirfs (2015, p. 133), Cebula and Young (2010, p. 2).

In terms of defining *cyber risks*, the separation between the terms *cyber risk* and *cyber crime* appears relevant for a clear understanding. According to the German Federal Office for Information Security (2012), cyber crime consists of criminal acts against the Internet or other data networks, IT systems or their data, and criminal acts that are committed via these information technologies.[19] Whereas *cyber risk* comprises *attacks* and *disruptions*, the term *cyber crime* is hereby solely limited to *cyber attacks*, the intended and target-oriented kinds of cyber incidents.[20] Such *cyber attacks* can further be categorized into *espionage*, e.g., illegitimate information retrieval or *sabotage* such as intentional damage to IT systems.[21] Such cyber crime incidents can have diverse forms, as the examples in Table 1 illustrate. The extent of cyber crime can thereby vary between, e.g., Google Inc. in 2013, where privacy rights were harmed, and examples such as Maroochy Water Services, where a physical system was harmed by a cyber attack.

Table 1: Selected cyber crime examples

Company	*Date*	*Element of crime*	*Estimated loss (excl. reputational losses)*
Maroochy Water Services[22]	January 2000	Unauthorized access to and control of SCADA wastewater system	-
Sony Corp.[23]	April 2011	Unauthorized access to customer data (77 million customers) on Sony PlayStation Network	171 million USD - 1.5 billion USD
Google Inc.[24]	February 2012	Violation of privacy protection settings in Apple's Safari browser	22.5 million USD
Google Inc.[25]	April 2013	Privacy violation through picking up data from unsecured wireless networks with Google Street View Car	145,000 Euros

One of the distinctive threats of cyber crime in contrast to other forms of crime is the capability of just a small group of activists or individuals to cause large damages and losses to businesses and governmental institutions.[26] This is particularly the case with c*yber-physical systems*, i.e., electronic components monitoring and controlling physical entities such as, e.g.,

[19] See Bundeskriminalamt (2012, p. 3).

[20] See BMI (2011, pp. 14-15), BSI (2013, p. 3).

[21] See BSI (2013, pp. 19, 41 (category G0.41)).

[22] See Slay and Miller (2008, pp. 73-75).

[23] See http://www.zeit.de/digital/datenschutz/2011-04/sony-playstation-kundendaten-hack, access 11/05/2013.

[24] See http://www.heise.de/newsticker/meldung/Google-zahlt-Rekordbusse-fuer-Cookie-Trick-im-Safari-Browser-1664559.html, access 11/05/2013.

[25] See http://www.telegraph.co.uk/technology/google/10010228/Germany-fines-Google-for-unprecedented-privacy-violations.html, access 11/05/2013.

[26] See Munich Re (2012, p. 39), Slay and Miller (2008, p. 80).

embedded systems in trains or airplanes, but also control systems for, e.g., water pumps.[27] For example, in 2000 the Australian Maroochy Water Services were attacked by a single person who managed to control the wastewater system with its 150 sewage pumping stations. The perpetrator then affected the local waterways by releasing untreated sewage water over three months.[28] The vulnerability of such Supervisory Control and Data Acquisition (SCADA) systems has often been discussed, but in practice, however, SCADA systems are still often in use for controlling infrastructure facilities.[29] The main threat caused by such attacks on cyber-physical systems is the direct impact on physical objects. In particular, such an attack on cyber-physical systems of critical infrastructure with a considerable extent of damage can be classified as a major threat. Critical infrastructure, which often has high importance for the national community and public security, includes the following objects: telecommunications, traffic control systems (roads, waterways and air traffic), supply infrastructure (water, wastewater and energy supply), medical care infrastructure, and further control systems.[30] Such vulnerable critical infrastructures often show a high level of dependency, either physical, by IT methods, or geographical, which means that the interdependency of information systems and physical infrastructures expose socially relevant physical structures to cyber threats.[31]

With regard of *cyber security*, Hult and Sivanesan (2013), for instance, determine a blending of protection of IT systems (IT security) and information security.[32] Von Solms and van Niekerk (2013), furthermore, explicitly distinguish between the terms *information security*, *information and communication technology security* and *cyber security*: i) *information and communication technology* defines the actual information technology infrastructure as the valuable asset ("infrastructure that processes, stores and communicates information"), ii) *information security* determines information (either analogue or digital) as the valuable and protectable asset, thereby including the digital information and communication technology where the information is stored and finally, iii) *cyber security* requires a broader definition, comprising cyber space, any electronic information, the information and communication technology that it depends on, as well as the users of cyber space in a personal, societal and national level and their interests of a tangible and intangible nature.[33] In this regard, the ISO/IEC 27001 defines abstract protection goals and security requirements for information

---

[27] For more information on cyber-physical systems and embedded systems, see acatech (2011) or BITKOM (2010).

[28] See Slay and Miller (2008, pp. 73-75).

[29] See Fernandez and Fernandez (2005, pp. 162-164), Rinaldi, Peerenboom, and Kelly (2001).

[30] See, e.g., Hult and Sivanesan (2013, p. 99), Lenz (2009, pp. 17-18).

[31] See Lenz (2009, pp. 24-25).

[32] See Hult and Sivanesan (2013, p. 99).

[33] See von Solms and van Niekerk (2013, pp. 100-101).

security. These include the *confidentiality*, *integrity* and *availability* of information, often described as the *CIA triad*. *Confidentiality* describes cyber risks in terms of unauthorized access to confidential information. *Integrity* means the correctness and completeness of digital information. Finally, *availability* defines the steady availability of access to authorized information. This approach can be extended by the following criteria: *authenticity*, *authentication*, *accountability*, *non-repudiation*, *reliability* and *access control*.[34] In terms of a holistic risk identification process, the actual impact of cyber risks on the respective CIA triad category needs to be clearly identified to provide information on the consequences of cyber risks for the general protection goals of a firm.[35]

Development of losses resulting from cyber risk

Key drivers for the steady growth of cyber risks include the technological progress and increasing complexity and interconnectedness of economy, state and society.[36] By the continuous development of new technologies, e.g., faster processors (CPUs) and larger data storage, the modern enterprise is capable of storing large sets of data and information. In addition, the amount of Internet users worldwide has grown continuously since 2000, thus also increasing the potential amount of vulnerable targets for cyber risk.[37] Due to faster Internet connections and the worldwide accessibility of private and corporate information through smartphones, tablets and PCs, private and corporate Internet users can store their data and information in the cloud, leading to benefits in terms of accessibility of data, but also, however, increasing data vulnerability and consequently altering cyber risks and particularly cyber crime.[38] Additionally, recent developments such as, e.g., workplace flexibility in the form of offsite working and corporate "bring your own device" (BYOD) or "corporate owned, personally enabled" (COPE) arrangements are multiplying the current risk exposures.[39]

Furthermore, as shown in the Ponemon Institute's *2013 Cost of Data Breach Study*, the organizational costs of data breaches[40] amounted to 5.40 million USD for 2013 in the US (4.83 million USD in Germany), leading to a cost per capita (per data set) of approximately 136

---

[34] See Brenner et al. (2011, pp. 3-5), Dinger and Hartenstein (2008, pp. 189-190), Posthumus and von Solms (2004, pp. 639-640).

[35] See Brenner et al. (2011, p. 39).

[36] See, e.g., AWK Group (2013, p. 1).

[37] See Gordon, Loeb, and Sohail (2003, p. 81).

[38] See, e.g., Haas and Hofmann (2014), or Alali and Yeh (2012), for risks associated with cloud computing.

[39] BYOD describes the usage of private hardware for business purposes. In contrast, with COPE, the actual device (such as a laptop or smartphone) is owned by the business, but employees are allowed to use the hardware for private purposes. See Federal Office for Information Security (2012, p. 3), Harvard Business Review (2013, p. 2).

[40] Ponemon Institute (2013) includes direct (e.g., forensic experts) and indirect (e.g., extrapolated value of customer loss resulting from turnover) expenses (see Ponemon Institute, 2013, p. 3).

USD.[41] Further, McAfee (2013) expects estimated costs of global cyber activity to be somewhere between 300 billion USD and 1 trillion USD.[42] According to a Corporate Trust (2012 and 2014) study, industrial espionage led in 2012 to losses of 4.2 billion Euros and in 2014 to losses of 11.8 billion Euros in the German economy, mainly affecting medium-sized businesses.[43] In addition, the World Economic Forum (2012) estimates the costs for cyber crime in 2009 in the US to be approximately 550 million USD and places *cyber attacks* in fourth place among the Top Five global risks in terms of likelihood – and after being unmentioned in the Top Five for 2013, *cyber attacks* is once again rated in fifth place in the 2014 World Economic Forum (2014) report.[44]

Additionally, Biener, Eling, and Wirfs (2015) analyze loss data using the SAS OpRisk Global Data database, showing that, for instance, the average and maximum losses from cyber risk are significantly smaller than for other operational risk categories.[45] Based on an in-depth analysis, the authors find the majority of measured cyber risk incidents are based on *actions of people* (903 incidents), followed by *failed internal processes* (41 incidents), *system and technical failure* (37 incidents) and *external events* (13 incidents).[46] Regarding geographical distribution, Biener, Eling, and Wirfs (2015) show that while the vast majority of cyber incidents occur in North America, the mean loss amount per cyber incident varies among the lowest of all analyzed regions.[47]

3. CYBER RISK MANAGEMENT

Regulatory requirements

Against the background of the increasing risk of cyber crime and the severe consequences for businesses, an integrated cyber risk management becomes vital. In this regard, several legal requirements demand adequate protection of information, such as, e.g., the Sarbanes-Oxley Act in the US or Directive 2006/43/EC ("EuroSOX") in Europe. The Sarbanes-Oxley Act (Section 404; introduced 2002) and the European Directive 2006/43/EC (implemented in

---

41 136 USD amounts to the mean value of all industrial classes, as established within Ponemon Institute's (2013) analysis. While the *healthcare* sector shows per capita costs of 233 USD, the *retail* sector shows a per capita cost of 78 USD (see Ponemon Institute, 2013, pp. 4-6).

42 See McAfee (2013, p. 5).

43 See Corporate Trust (2012, p. 8), Corporate Trust (2014, p. 8).

44 See World Economic Forum (2012, pp. 12, 27), World Economic Forum (2014, p. 17).

45 See Biener, Eling, and Wirfs (2015, pp. 138-139).

46 See Biener, Eling, and Wirfs (2015, p. 139).

47 The authors further conduct analysis on industry dependency (financial, non-financial), interrelation to losses in other firms (one firm, multiple firms affected) and company size (measured by number of employees) (see Biener, Eling, and Wirfs, 2015, pp. 139-141).

Germany via BilMoG in 2009, valid from 2010 on)[48], for instance, can be interpreted as requirements for information security, as they demand the implementation of an internal control structure, its correct documentation and the monitoring of the internal control system, thereby ensuring the integrity and correctness of processed financial data. Furthermore, some country-specific regulations in Germany include, for instance, the Act for Control and Transparency in the Corporate Sector (KonTraG) and the German Federal Data Protection Act.[49] In addition, some industries such as the German insurance sector are required by regulation (MaRisk VA 7.2.2.2) to have adequate IT systems that ensure integrity, availability and authenticity as well as confidentiality.[50]

ISO/IEC 27000 series

According to the ISO/IEC 27000 series, which consists of standards on information security, the ISO/IEC 27001 standard for "Information technology - Security techniques - Information security management systems - Requirements" provides guidance on the information security management system (ISMS). This ISMS is based on the plan-do-check-act (PDCA) cycle as a key principle[51], representing the continuous improvement and optimization of enterprise-wide information security.[52] Although we do not analyze the PDCA cycle in detail, we explain the individual steps and their idea of continuous improvement and optimization, which are necessary for an efficient cyber risk management process as threats in the digital world are fast-moving and quick to adapt. The individual PDCA cycle steps are i) *plan*, i.e., the planning of the implementation of an information security management system or the possible adjustments to an existing ISMS; ii) *do*, which focuses on the realization of the previously determined ISMS changes, i.e., the implementation and operation of the ISMS; iii) *check*, which describes the phase of monitoring and reviewing previously implemented changes and actions; iv) and *act*, which compromises the information from the check phase and consequently initiates quality and improvement actions.[53] Thus, the key idea of the PDCA cycle, which is generally a tool for quality management, should also be applied to cyber risk management, leading to a continuous execution of the risk management steps as presented in the following

---

[48] The SOX Act is applied to firms that offer stocks on the US stock markets, equity securities (not listed) or public offerings, as well as all subsidiary companies. The "EURO-SOX", however, refers to all larger capital companies (listed and not listed).

[49] See http://www.kompass-sicherheitsstandards.de/43738.aspx, access 11/28/2014, for further information on these regulations.

[50] See BaFin – MaRisk VA 7.2.2.2, https://www.bafin.de, access 11/28/2014.

[51] This refers to the ISO/IEC 27001:2005 standard; however, the ISO/IEC 27001:2013 standard does not limit the information security management system to the PDCA cycle but also allows other improvement processes, such as the Six Sigma DMAIC (define, measure, analyze, improve and control).

[52] See Brenner et al. (2011, pp. 21-24).

[53] See Brenner et al. (2011, pp. 21-24).

integrated cyber risk management process. Besides the ISO/IEC 27000 standards, the German Federal Office for Information Security, for instance, offers the "IT-Grundschutz", which also in general aims for the continuous improvement of information security; however, it provides a more detailed kind of information security guideline. Thus, the ISO/IEC 27000 focuses instead on a top-down approach and defines general steps of cyber risk management, whereas the "IT-Grundschutz" provides a detailed bottom-up approach, focusing on threats and risk control measures.[54] Still, the two security approaches are compatible, and thus the "IT-Grundschutz" can be certified according to the ISO/IEC 27001 certification standards. Further IT-relevant standards that also encompass information or IT security to some extent are the COBIT framework, the IT Infrastructure Library (ITIL) or the IDW PS 330 (also IDW RS FAIT 1) set out by the Institute of Public Auditors in Germany (IDW), for instance.[55]

An integrated cyber risk management framework

We next present the main components and success factors for a basic cyber risk management approach (see Figure 1; see.also Biener et al., 2015). We further primarily focus on the previously introduced ISO/IEC 27000 series of standards[56] as this is the most commonly used standard in terms of information security management systems. In addition, we extend these steps with findings from the literature and with risk or information security management insights. The approach should, however, be interpreted as a non-exhaustive extension of a general risk management approach with a focus on the management of cyber risks. As previously explained, the continuous evaluation, assessment and control of risks is necessary to provide an efficient cyber risk management. In this regard, the risk management steps 1 to 4 should thus be implemented as a continuous process. Furthermore, risk culture is promoted as a subsequent organizational element of a holistic cyber risk management approach, which needs to be continuously maintained and intensified within businesses and their relevant stakeholder groups.

---

[54] See http://www.security-insider.de/themenbereiche/sicherheits-management/standards/articles/287441/index2.html, access 12/01/2014.

[55] See http://www.kompass-sicherheitsstandards.de/43726.aspx, access 12/01/2014.

[56] We therefore particularly focus on the ISO/IEC 27001:2005 and the ISO/IEC 27005:2008, if the standards' version is not specifically outlined.

Figure 1: Basic operational cyber risk management process[57]

|| 1. Risk identification

1.1 Define and understand firm's business model, business objectives and assets; determine relevance of IT for business; agree on level of IT security

(ISO/IEC 27005 – Context Establishment; ISO/IEC 27005 – Risk Identification – Identification of Assets)

1.2 Identify all cyber risks by a top-down or bottom-up approach

(ISO/IEC 27005 – Risk Identification – Risk Identification of Vulnerabilities, Threats, Existing Controls)

|| 2. Risk assessment and valuation

2.1 Quantify risks (qualitatively or quantitatively) by determining probability of occurrence and estimated impact of cyber risk event (e.g., with a risk matrix)

(ISO/IEC 27005 – Risk Identification – Risk Estimation)

(ISO/IEC 27005 – Risk Evaluation)

2.2 Aggregate cyber risks in holistic and company-wide risk management by application of interdependencies (correlations) between risks, and determine relevant risks

(ISO/IEC 27005 – Risk Evaluation)

|| 3. Risk response

Decide adequate solutions for

3.1 Risk avoidance (e.g., avoid use of USB flash drives)

(ISO/IEC 27005 – Risk Treatment – Risk Avoidance)

3.2 Risk mitigation (e.g., implement firewalls)

(ISO/IEC 27005 – Risk Treatment – Risk Reduction)

3.3 Risk transfer (e.g., purchase cyber insurance)

(ISO/IEC 27005 – Risk Treatment – Risk Transfer)

3.4 Risk acceptance (self-insurance)

(ISO/IEC 27005 – Risk Treatment – Risk Retention)

(ISO/IEC 27005 – Information Security Risk Acceptance)

|| 4. Risk control

4.1 Monitor and proactively control risks and regularly check adequacy of risk response measures (e.g., logging of confidential data access)

(ISO/IEC 27005 – Risk Monitoring and Review)

4.2 Implement regular operational testing of risk exposures and possible vulnerabilities of risk response solutions

(ISO/IEC 27005 – Information Security Risk Monitoring and Review)

4.3 If risks exceed agreed risk level, report divergences to management

[57] For further recommendations and measures see, e.g., Biener et al. (2015, pp. 34-50), Gordon, Loeb, and Sohail (2003, pp. 83-84), Kersten, Reuter, and Schröder (2013, p. 48), Romeike and Hager (2009, pp. 377-387), Shackelford (2012, p. 16), Zurich (2014, pp. 22-27).

|| 5. Risk culture and risk governance

5.1 Focus on company-wide risk culture and create risk awareness among all employees and provide regular trainings and instructions on IT security for all employees

(ISO/IEC 27005 – Information Security Risk Communication)

5.2 Apply risk governance and define a business continuity management plan

(ISO/IEC 27005 – Information Security Risk Communication)

(ISO/IEC 27005 – Information Security Risk Monitoring and Review)

1. Risk identification

1.1 The identification of cyber risks is vital in order to manage them. To do so, firms need to provide information on their business model, in order to identify valuable firm *assets*, e.g., by relying on a standardized assessment format such as ISO/IEC 27005.[58] According to the ISO/IEC 27000 series, valuable assets that have major importance for business operability can be, e.g., *information (data)*, *software*, *physical assets (e.g., PC, router)*, or general *IT infrastructure such as data centers*. In addition, *employees*, *services* and other *intangible assets* might also be identified as valuable *assets*, and may be affected by cyber risk.[59] Further, companies need to identify the importance and dependency of the cyber environment for their individual core business. For example, companies focusing on e-commerce have greater cyber risk exposure than firms with business models that mainly operate offline.[60] Therefore, particularly companies exposed to threats of cyber risk should behave proactively, by continuously identifying, assessing, controlling and monitoring possible vulnerabilities from cyber risk exposures.[61] These findings are also confirmed by Hovay and D'Arcy (2003), who show that Internet-specific firms display a slight indication of negative abnormal returns after the occurrence of a denial-of-service[62] cyber attack. According to the ISO/IEC 27001 and 27005, a firm should therefore identify its general need for information security (i.e., cyber risk management) and comprehensively determine the requirements, as well as deciding about the level of information and IT security.[63]

[58] See further information on identification and valuation of assets within the ISO 27005 Annex B. See further, e.g., Siegel, Sagalow, and Serritella (2002, p. 33).

[59] See Brenner et al. (2011, p. 16), Kersten, Reuter, and Schröder (2013, pp. 24-25).

[60] See Luzwick (2001, pp. 16-17), Marsh (2014, p. 11).

[61] See, e.g., IBM (2012, p. 10), Shackelford (2012, pp. 4-5).

[62] Denial-of-service is a cyber attack aiming to influence the availability of, e.g., a network, database or website (see Brenner et al., 2011, p. 4).

[63] See ISO/IEC 27005 Annex A.

1.2 The next step is a comprehensive risk identification. The identification process should comprise the identification of cyber threats, general vulnerabilities, already existing risk controls, and consequences for assets if breaches of information security occur.[64] Based on the ISO/IEC 27005, risk exposition is solely existent when a certain threat can be identified and the firm is vulnerable to this particular threat.[65] In this regard, risk identification comprises a detailed approach, consisting of the identification of *threats* (threat to an information asset), the *vulnerabilities* (the individual weakness of the information security management system protecting the information asset) and the *consequences* (the expected amount of loss due to harm to the information asset). Furthermore, firms need to determine their already implemented *control objectives*. Such an analysis can be done by either a *top-down* or *bottom-up* approach, where a *top-down* approach is applied rather quickly, generally just considering the major cyber risks from a strategic perspective. The more complex and therefore slower *bottom-up* approach, in contrast, captures and analyzes all relevant enterprise processes.[66] Hence, for the comprehensive evaluation of a firm's cyber risk exposure, the *bottom-up* approach appears to be advisable, as with the *top-down* analysis some risks may not be identified correctly or correlations between individual risks may possibly be incorrectly estimated.[67] The risk identification process requires a substantial analysis ranging from physical security to general vulnerabilities of the IT systems.[68] A possible risk classification could involve arrangement into the following categories, as previously presented: *actions of people, failed internal processes, system and technical failure*, and *external events*.[69] Another approach, outlined by Posthumus and von Solms (2004), for the risks of business information includes these risk categories: *natural risks*, *technical risks* and *deliberate or accidental acts of humans.*[70]

To summarize, the risk identification step determines the firm's context for IT and information security, and its valuable assets, and outlines the relevant cyber risks (threats, vulnerabilities, consequences) in addition to already implemented controls. The identified *assets* are thus valuable for the firm and therefore need to be protected by a cyber risk management (i.e., information security management system).[71] Hence, the identified assets are at risk, if, e.g.,

---

[64] See ISO/IEC 27005 Annex B for examples of assets and business processes, Annex C for examples of threats, and Annex D for vulnerabilities and their assessment methods.

[65] See Kersten, Reuter, and Schröder (2013, p. 31).

[66] See Romeike and Hager (2009, p. 377).

[67] See Romeike and Hager (2009, p. 377).

[68] See Siegel, Sagalow, and Serritella (2002, p. 34).

[69] See Biener, Eling, and Wirfs (2015, p. 139).

[70] See Posthumus and von Solms (2004, p. 641).

[71] See Brenner et al. (2011, p. 16).

cyber attacks, *system blackouts*, *lack of staff*, *natural hazards*, *carelessness* or *operating errors* occur.[72]

From a practical perspective, risk identification is also necessary for insurance companies offering cyber risk coverage within their underwriting process, as they need to identify their customers' risks before offering adequate insurance solutions. Risk identification and assessment is thus often conducted via questionnaires to identify the essential cyber threats as a first step.[73] In the example of Zurich Cyber & Data Protection, the questionnaire includes questions regarding, for example, *general information* (e.g., requested coverage), *policyholders' profile* (e.g., annual revenue in Europe, USA/Canada and Other), *business activities* (e.g., the proportion of online purchases/bill payments/banking or trading, the personal information that is stored, or whether business and customer information, healthcare information, tax files, etc., are stored), o*rganization and governance* (e.g., whether security risk assessments are conducted), *network security* (e.g., whether firewall technology is used at all Internet points), *data management* (e.g., whether security configuration standards and procedures exist for new system components), *incident response* (e.g., whether system and security logs are placed on all systems that collect, process or store personal information), *business continuity planning* (e.g., whether a business continuity and disaster recovery plan exists), *incident history* (e.g., whether significant systems intrusions have been recorded in the past three years) and *Internet media* (e.g., whether policies or procedures are in place to screen Internet content for potential infringement). Such questionnaires not only comprise possible cyber threats as part of the risk identification, but also request information on already established risk response measures to facilitate adequate risk identification and assessment by the underwriter. However, in the case of more complex risks or requests for larger financial coverage, insurance companies identify the individual firm's risk by a technical underwriting (i.e., risk assessment by experts).[74]

2. Risk assessment and valuation

2.1 After the identification of cyber risks, the firm's individual risk exposure needs to be *assessed* and if possible *quantified*.[75] According to ISO/IEC 27001 and 27005, firms therefore need to assess the possible losses and impact probabilities of identified cyber risks. This involves the realistic estimation of consequences of cyber risks, their occurrence probabilities, and the adequate assessment of the general risk level (e.g., within a risk matrix). Finally, the

---

[72] See Kersten, Reuter, and Schröder (2013, pp. 27-28).

[73] See, e.g., Baer and Parkinson (2007, p. 53).

[74] See, e.g., Baer and Parkinson (2007, p. 53).

[75] See Romeike and Hager (2009, p. 377).

decision as to whether risks are acceptable or if risk response measures are required has to be made by the management.[76]

Further *risk valuation* approaches could be of a quantitative or qualitative nature. However, a final assessment of these risks in monetary units should be conducted to enable the valuation of cyber risks.[77] Smith (2004), for instance, presents an approach for the valuation of costs after an IT system has been harmed by a cyber attack. The author takes into account the valuation of tangible and intangible costs, as such an analysis might be beneficial when attempting to estimate impacts from system vulnerabilities. The valuation of tangible losses is thereby based on the calculation of system restoration and lost productivity, which consist of labor, material and overhead costs (e.g., costs for IT experts to recover the system). Furthermore, the valuation of the intangible costs can be achieved by, e.g., the calculation of expected losses due to the unavailability of the website. However, for this calculation, financial information (e.g., sales) and the website statistics are a necessity to adequately calculate lost profits.[78] In addition, the calculation of long-term profit losses, which account for the majority of losses from a cyber attack (e.g., customers not returning to a website anymore) must be estimated.[79]

Furthermore, capital market reactions also need to be taken into account when analyzing losses from security breaches, as cyber risks might affect the business's valuation on the stock markets. Cavusoglu, Mishra, and Raghunathan (2004a) show, based on an event study, that the impact of security breaches (defined by the authors as "malicious attempts to interfere with a company's business and its information") directly affects a firm's market value by an average market value decline of 2.1 % within two days after the attack announcement. Additionally, the market value of firms that build security technology showed an abnormal return of 1.36 %, also within two days after the breach announcement. The authors construct their firm valuation model based on the efficient market hypothesis and calculate the firm's value from the discounted value of expected future cash flows determined by all available information in the market until the time of valuation.[80] The model is subsequently evaluated for security breaches announced on the technology websites Lexis/Nexis, CNET and ZDNET between January 1996 and December 2001. In addition, Campbell et al. (2003) find that security breaches involving confidential data produce highly significant negative stock market reactions. Such approaches can be used for estimating expected losses, for instance.

---

[76] See Brenner (2011, p. 39).

[77] See Romeike and Hager (2009, p. 378).

[78] See Smith (2004, p. 51).

[79] See Smith (2004, pp. 52-53).

[80] See Cavusoglu, Mishra, and Raghunathan (2004a, pp. 72-73).

A classification of costs (and the degree of uncertainty in the estimation) from security breaches can further be found in Cavusoglu, Mishra, and Ragunathan (2004b). The authors hereby differentiate between short-term and long-term as well as tangible and intangible costs. The short-term costs mainly include losses from business operations and decreased productivity, costs for data recovery, investigation costs, destroyed IT property, notification and information costs, as well as media costs. On the other hand, the long-term costs (and damages) can influence the firm's cash flows, customer attractiveness, reputation, goodwill, loss of trust of customers and business partners, and legal liabilities.[81] In addition, costs for debt or equity capital might increase due to greater risk exposure.[82] Therefore, the damages, costs and losses from cyber crime should not only be associated with the tangible costs, as they occur when, e.g., a PC system is damaged and needs to be replaced. Additional costs can also arise from slower network access and therefore lower operability, a loss of productivity, the increased monitoring of systems or the recovery of infected PC systems and data.[83] As many firms operate business via the Internet and the IT infrastructure relies on a few individual technologies, risks in cyber space are often correlated.[84] In addition, for a single crime incident, the highest financial loss still arises from the theft of confidential information.[85]

Although it is not directly linked to risk assessment or valuation, the tracking of digital information inside the company is particularly necessary for the valuation of losses *after* a cyber risk incident has occurred. Only firms that can accurately determine their profits due to their individual lines of business and marketing tools (e.g., online sales), for instance, can adequately handle the loss estimation after a cyber incident has occurred, as copious information from company statistics (e.g., customer sales via the website, new customers on the website per day, probability of return of customers to the website) and the financial information (e.g., average sales per customer) is required for calculation.[86] Hence, as part of a holistic risk management strategy and in order to ease loss valuation from cyber risks, the comprehensive knowledge of the business operations needs to be established early and especially *before* any cyber incidents occur.[87]

2.2 In addition, cyber risks need to be aggregated and analyzed on an enterprise-wide basis which requires the consideration of correlations of cyber risks and other business risks.[88] As

---

81 See Öğüt, Raghunathan, and Menon (2011, p. 497), Smith (2004, pp. 50-51).
82 See Cavusoglu, Mishra, and Raghunathan (2004b, p. 72).
83 See Smith (2004, p. 46).
84 See Öğüt, Raghunathan, and Menon (2011, p. 497).
85 See Campbell et al. (2003, p. 436).
86 See Smith (2004, p. 51).
87 See Smith (2004, p. 55).
88 See Romeike and Hager (2009, p. 379).

presented in Böhme and Kataria (2006), these correlations might be assessed on a firm internal and external basis to better determine dependencies of these risks, and to form a basis for further risk response decisions. The authors analyze correlations of different classes of cyber risk by applying t-copulas for modeling extreme values, a) within the firm (intra-firm risk correlation) and b) externally (global risk correlation), where the global risk correlation directly affects cyber risk insurers' premium decisions, and the internal correlation affects the firm's decision whether to purchase cyber insurance or not. In addition, Wang and Kim (2009) show that network risks are allegedly higher for companies in neighboring countries compared to networks in more dispersed geographical locations. Hence, firms thinking about the optimum locations for their data centers might be advised to lower their security risks by avoiding neighboring countries (or generally countries with higher interdependence) as locations for their centers.

3. Risk response

Based on the results of the risk identification and assessment, adequate risk response measures must be applied, such as *risk avoidance*, *risk mitigation*, *risk transfer* or *risk acceptance*. In any case, despite the application of such risk response methods, risks will never be completely eliminated, and thus residual risks may still remain with the firm. Residual risks result from i) the risk acceptance, or ii) risk mitigation, which only reduces the probability or minimizes the loss amount from an actual cyber risk incident.[89]

3.1 *Risk avoidance* includes giving up potential chances to take such risks. A cyber risk avoidance strategy could involve either the complete avoidance of IT systems in general, which is not feasible for all modern types of business, or the avoidance of certain IT systems, for instance.[90] Certain subcategories of cyber risks can thus be avoided, e.g., by abandoning the use of USB flash drives or CDs on computer systems connected with the business network, hence avoiding risks of malware infection from external data sources.[91]

3.2 With regard to *risk mitigation* of cyber risks, IT and information security tools can be implemented, such as, e.g., firewalls or cryptographic techniques for data submission.[92] These preventive measures allow companies to reduce the probability of occurrence of specific types of cyber risks or diminish the severity of such cyber risk incidents (e.g., protection of the net-

[89] See Brenner et al. (2011, p. 40, 42), Romeike and Hager (2009, pp. 378-380).

[90] Such as, e.g., the avoidance of Microsoft Windows as an operating system. See Romeike and Hager (2009, p. 161).

[91] See, e.g., Gibson (2010, p. 17).

[92] See Francis (2013, p. 28).

work or the company website; mitigating chances of successful denial-of-service attacks).[93] The ISO/IEC 27001 lists some extensive control objectives and control measures that can be applied to mitigate risks, as illustrated in Table 2.[94]

Table 2: ISO/IEC 27001:2013 control objectives and controls

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

Still, such risk mitigating measures imply costs, and hence the trade-off of costs and reduced losses (either by probability of occurrence or its severity) needs to be individually analyzed. In addition, ISO/IEC 27005 specifies the following constraints that need to be determined for the implementation of risk reduction measures: time constraints, financial constraints, technical constraints, operational constraints, cultural constraints, ethical constraints, environmental constraints, legal constraints, ease of use, personnel constraints, and constraints of integrating new and existing controls.[95] To further assess the value of IT security investments, Cavusoglu, Mishra, and Raghunathan (2004a) implement a game theory-based model. Their model evaluates the IT security investments based on cost and quality parameters of various applicable technologies and determines the cost savings based on hacker attacks and firm specific parameters. Further findings by Wang, Chaudhury, and Rao (2008) show that firms can assess their financial risk exposure by the implementation of information security measures (e.g., implementation of firewall systems or increased backup frequency) based on a value-at-risk (VaR) approach using extreme value theory. With the underlying parameters for individ-

[93] See Gibson (2010, p. 96).

[94] Each of these categories consists of further controls and control objectives (see Brenner et al., 2011, pp. 63, 65-128). See ISO/IEC 27001 Annex A.

[95] See ISO/IEC 27005 Annex F.

ual incident probabilities and resulting costs, firms can calculate their own VaR before and after implementing IT security measures. Extreme value theory is thereby used to provide an adequate characterization of the tail behavior of the daily losses, which is afterwards used for the VaR estimation. A further study focusing on the optimal amount of investment into information security and thus cyber security is provided by Gordon and Loeb (2002). The authors present an economic model taking into account the vulnerability of information to a security breach and additionally examine the potential loss due to such a breach, distinguishing between two classes of vulnerability-to-expected-loss relations (linear and convex). They show that for a non-linear relation of vulnerability and expected loss firms should not solely concentrate their security investments on information that exposes the highest vulnerability, as such protections are rather expensive and difficult to maintain, but firms should instead favor security investments in information exposed to mid-range risks. According to Shackelford (2012), firms should also act proactively and primarily invest in cyber security, and secondarily rely on cyber insurance as a risk transfer instrument, if favored by the management.

3.3 Furthermore, when previous risk management solutions are not sufficient, *risk transfer* can be an additional risk management tool, including cyber risk insurance, for instance, or the transfer of risks to customers or suppliers.[96] Although insurance is classified as a risk transfer tool, many traditional third-party liability insurances do not always cover losses from cyber risks or cyber crime. Thus, specialized cyber risk insurance products may become vital. These cyber insurance solutions often cover liability claims from, e.g., property loss and theft, losses or damage of data, income losses due to downtimes of networks and computer failures. Haas and Hofmann (2014), for instance, provide a brief overview of current cyber insurance policies in the German market.[97] Furthermore, Choudhry (2014, p. 1) states that currently 12 insurance companies offer products in the German insurance market, such as ACE, AIG, Allianz or AXA, for instance. In contract, in the US market more than 30 insurance companies provide cyber insurance products, while the UK market has 15 insurance companies offering cyber policies.

In the literature, pricing (see, e.g., Herath and Herath, 2011) and the adequate utilization of cyber insurance (see, e.g., Böhme and Kataria, 2006) have been discussed in particular. Mukhopadhyay et al. (2013) analyze the general question of whether IT systems should be insured or not. They focus on cyber risk insurance and calculate the premium charged for insuring cyber risks using the collective risk modeling theory. As their main result, they advise the utilization of cyber risk insurance based on financial trade-offs and benefits. To study the

---

[96] See, e.g., Behrends (2014, p. 16), Kersten, Reuter, and Schröder (2013, p. 59), Zurich (2014, p. 27).

[97] See Bandyopadhyay, Mookerjee, and Rao (2009, p. 68). See also Haas and Hofmann (2014) for a more detailed overview of cyber risk insurance coverage.

question of adequate pricing of cyber insurance, Herath and Herath (2011) implement a cyber insurance model and derive cyber insurance premiums for three types of insurance policy models by using the Clayton and Gumbel copulas to determine the loss distribution based on an empirical distribution of the number of infected computers and the timing of the trigger event. Böhme and Kataria (2006) further suggest that cyber insurance should be used for risk classes with high internal correlation (failure of multiple systems on firm's own network) and low global correlation (across independent firms in insurer's portfolio), because the opposite situation, with low internal correlation, would provide the firm with self-insurance effects on its own network, while high global correlation impairs the insurer's risk-pooling, and hence increases insurance premiums for the cyber insurance product. Nevertheless, even with the purchase of cyber risk insurance, the insured firm still has to keep up risk identification, assessment and valuation as well as risk control, as cyber insurance itself cannot act as a preventive measure or a risk mitigation tool.[98] In addition, Biener et al. (2015, p. 65)[99] outline that information asymmetries can lead to adverse selection effects, whereby firms that have suffered a cyber attack are more willing to purchase cyber insurance. This could be avoided by screening (e.g. audits) or signaling (e.g. via questionnaire) measures. Additionally, moral hazard, i.e. the change of behavior after purchasing cyber insurance, can be reduced by the implementation of deductibles, for instance.[100]

3.4 Finally, self-insurance, and hence *risk acceptance*, can be chosen as a risk response option, depending on the individual agreed level of cyber risks that the firm is willing to take. Risk acceptance can be considered an option if the assessed risks are not identified as sufficiently relevant to initiate risk mitigation or risk transfer measures; or if these measures are too costly (expected losses lower than costs for risk management tools). However, risks that are accepted on an involuntary basis need to be explicitly specified. According to ISO/IEC 27001, the management needs to be informed about any resulting risks and has to explicitly accept these.[101]

4. Risk control

4.1/4.2/4.3 After the identification, assessment and valuation of cyber risks, as well as the initiation of risk response strategy, the proactive *risk control* is the subsequent step in a holistic risk management. ISO/IEC 27005 demands an ongoing review of risk factors as well as the risk management in general (e.g., risk acceptance criteria, risk assessment approach, etc.).

---

98 See Siegel, Sagalow, and Serritella (2002, p. 33).

99 Based on Baer and Parkinson (2007), Gordon, Loeb and Sohail (2003), Majuca, Yurcik and Kesan (2006), Shackelford (2012).

100 See Biener et al. (2015, p. 65).

101 See Brenner (2011, p. 42), Kersten, Reuter, and Schröder (2013, p. 60).

Companies should regularly monitor their risks and control the initiated risk response measures, and adjust or improve these if necessary (e.g., 24/7 real-time monitoring of access to confidential data). In this context, regular IT audits need to be performed to achieve adherence to IT security measures. In addition, any divergences should be *reported* to the management or other responsible executives.[102]

5. Risk culture and risk governance

5.1 In addition to the regular risk management steps, *risk culture* and an established *risk governance* are required to complete a holistic cyber risk management. *Risk culture* is particularly important as a majority of cyber incidents occur due to actions of people, malpractices and user faults.[103] Therefore, besides monitoring the identified risks, proactive trainings of all employees[104] and *regular testing* of established IT security measures, it is necessary to provide a well operating risk management system.[105] Moreover, different employees have different access authorizations. To establish an operational risk culture, senior managers, Chief Information Officers, system and information owners, business and functional managers, and IT security personnel in particular need to fulfill their individual roles and responsibilities in a holistic cyber risk management.[106] Roles and organizational structures are outlined in the COBIT framework.[107]

5.2 The connection of *risk management*, *risk governance* and *cyber risks* can be seen as a value-creating combination.[108] For instance, in the concrete business case of a cyber incident, companies should be following a *business continuity management* (BCM) plan, promoted by a holistic risk governance objective. Detailed concepts, plans and measures for a case of cyber incident occurrence are a valuable tool for recovering business operations after a security breach.[109] A BCM generally comprises actions that are required to ensure the operability of core business processes.[110] The BCM might consist of a *continuity of operations* plan, a *disaster recovery* plan, a *vulnerability and incident response* plan and an *IT contingency* plan. Each measure covers a different phase of a cyber attack recovery and hence is required to be an

---

[102] See Brenner et al. (2011, pp. 44-46, 51-52), Romeike and Hager (2009, p. 387).

[103] See, e.g., Biener, Eling, and Wirfs (2015, p. 139).

[104] Training is necessary for all employees, as cyber risks do not only occur by immediate interruption of hardware or software systems monitored by internal IT departments but also by, e.g., *social engineering*, the social manipulation of employees to get user passwords and thereby access company systems.

[105] See Francis (2013, p. 28).

[106] See Stoneburner, Goguen, and Feringa (2002, p. 6).

[107] See COBIT (2012, pp. 76-77).

[108] See Biener et al. (2015, p. 34), Spörrer (2014, pp. 53-54).

[109] See Romeike and Hager (2009, pp. 396-397).

[110] See Romeike and Hager (2009, pp. 396-397).

integrative part of a holistic BCM. As an example, the *continuity of operations* consists of the main minimal arrangements or requirements that are necessary to maintain core business operations.[111] The *disaster recovery* plan as an integrative part of a BCM is a relevant element for the recovery and rehabilitation of business processes, for instance covering courses of action for the recovery of lost data or replacement of non-usable hardware or IT infrastructure.[112] In addition, the *vulnerability and incident response* can be seen as part of risk prevention and is also essential in the phase of damage control, containing for instance information on the defense against certain risk events (e.g., denial-of-service attacks). Finally, the *IT contingency* plan involves measures for the recovery of IT systems and should therefore be directly linked with the BCM plan.[113] The ISO/IEC 27005 also advises the development of risk communication, not only for regular operations but also for emergency situations, as outlined above.

Implications

In summary, based on the existing frameworks and the findings and discussions in the literature, a holistic management of cyber risks appears to be vital. With the increasing importance of information and information technology for business operations, the implementation of an enterprise-wide cyber risk management process and the adaption of adequate response objectives is a necessity. Adequate IT security measures as well as coverage by cyber insurance policies as a particular risk management tool can help to lower cyber risk exposures. Particularly, *Internet-only* firms and service platforms (e.g., information and communication platforms such as Twitter.com, or shopping platforms such as Amazon.com) should hedge their risk positions, as in the actual case of website downtimes, revenues will drop and customers will still be able to acquire the desired goods from other firms. Possible intangible long-term costs from such cyber incidents will therefore directly influence all lines of business and hence, in the worst case, strongly reduce market value.[114] Furthermore, cyber risk management should be interpreted as a process, being subject to continuous monitoring, reviewing and improvement.[115] Finally, the management should be aware that risk awareness among all stakeholders (employees, suppliers, etc.) creates a sound environment for good cyber risk management.

[111] See Romeike and Hager (2009, p. 397).
[112] See Romeike and Hager (2009, p. 398).
[113] See Romeike and Hager (2009, p. 399).
[114] See Cavusoglu, Mishra, and Raghunathan (2004b, pp. 75-76), Smith (2004, p. 51).
[115] See Biener et al. (2015, p. 36).

4. CHALLENGES ASSOCIATED WITH CYBER RISK MANAGEMENT

Although risk management frameworks such as the ISO/IEC 27000 series or other guiding frameworks exist, a successful cyber risk management still represents a challenge for businesses. Such challenges partly arise from the continuous change (the continuous change of traditional business models to Internet and digitally dependent business models) and knowledge deficits (problems with the correct asset valuation/loss estimation, data insufficiencies or lack of awareness among stakeholders).

The *change of traditional business models* to modern, more complex and interconnected Internet-based business models affects the vulnerability of data privacy and will increasingly boost demand for cyber risk management. For instance, with the market entry of Google Inc.[116] into the automobile insurance sector (by comparing tariffs), accessibility and transparency in the market might improve, as comparability among auto insurance products is easier accessibly by potential insurance customers. However, with customers using this service, private customer and contract data will be stored online, e.g., at Google Inc. The continuing digitalization of traditional business models will consequently force usage of online applications, increasing the amount of personal data online and hence expanding the potential for cyber risks.[117]

Furthermore, the current knowledge on cyber risks and risk management plays a crucial role. From a business perspective, the correct *asset valuation* in terms of a cyber risk management process is a key challenge for companies assessing cyber risks in general. Firms need to adequately assess their tangible and intangible assets to determine *possible losses and threats*. This is particularly relevant for the determination of the precise loss amount in a case of cyber incident occurrence, but also for the implementation of adequate risk response measures, as previously outlined.[118] In this regard, firms have to understand that many IT systems (hardware and software) are mainly mass products, and thus a particularly high *correlation of risks* is possible, leading to potential accumulation risks.[119] In addition, the fast changing technological evolution demands for a dynamic cyber risk management process, which quickly

---

[116] For more information see Google: https://www.google.co.uk/compare/carinsurance/form, access 08/03/2013.

[117] See ACE (2013, p. 7), AWK Group (2013, p. 1).

[118] In the US, for example, a federal crime under the Computer Fraud and Abuse Act (CFAA) must have exceeded 5,000 USD to be investigated; however, this requirement was changed. Still, the attacked firms need to provide information on their suffered loss or damages (see Smith, 2004, pp. 47, 56). See also *18 US Code §1300 – Fraud and related activity in connection with computers* and *Identity Theft Enforcement and Restitution Act, Pub. Law 110-326, 122 Stat. 3560* of 2008. See further Baer and Parkinson (2007, p. 54), Smith (2004, p. 47).

[119] See Baer and Parkinson (2007, pp. 53-54), Böhme (2005, p. 13).

adapts to a changed cyber environment and thus cyber risk exposures.[120] Furthermore, the general problem of *insufficient data* for the proper calibration of cyber risks management (e.g., in terms of impacts from cyber threats) is strengthened by the fact that cyber incidents are often not *reported*, as firms fear negative effects on their shareholder value or reputational losses.[121] This reduces the total knowledge base on cyber risks, and although data from operational risk databases seem to be available that also include losses from cyber risk incidents, the quantity and quality of these data appear to be insufficient to cover the breadth of cyber risk incidents.[122] The future reporting of cyber incidents, however, will be strengthened with the implementation of new regulatory requirements by the European Commission (European General Data Protection Regulation), as mentioned previously – although the information may not be publicly available.[123] Finally, an essential challenge for effective cyber risk management will be presented by people, as general awareness of cyber risks, i.e., its threats and consequences, seems lacking among a large share of IT users.

5. SUMMARY

In this paper, we outline the main components and challenges of an integrated cyber risk management process. As cyber risks are amongst the most underestimated business risks in 2013, and against a background of increasing demand for cyber risk management, we primarily focus on the management of cyber risks and the associated challenges of cyber risk management based on a structured review of the academic literature and ISO/IEC 27000 standards.

We lay out the main steps within a risk management framework and present an operational approach for a risk management process based on the ISO/IEC 27000 series. Risk identification, risks assessment and valuation, risk response and risk control objectives, as well as risk governance and risk culture, are explicitly discussed. In this context, we emphasize that cyber risk should also be controlled, supervised and emphasized by the management. In the event of a cyber attack, business operability and continuity should be ensured at all times by the implementation of, for instance, a business continuity management plan. Furthermore, cyber risk management should be implemented as a continuous process. However, firms still face many challenges with the implementation of cyber risk management that need to be considered

---

[120] See Biener et al. (2015, p. 46).

[121] See Cavusoglu, Mishra, and Raghunathan (2004b, p. 87), Dowdy (2012, p. 131), Gordon, Loeb, and Sohail (2003, p. 82), Herath and Herath (2011, p. 9).

[122] See e.g., Biener, Eling, and Wirfs (2015, p. 139).

[123] See http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf, access 03/04/2014.

thoroughly, such as the change of traditional business models, the correct asset valuation or the loss determination.

In addition, we show that besides the implementation of an adequate cyber risk management process, firms need to determine whether to purchase risk transfer tools such as cyber insurance or not. To do so, adequate cyber insurance products are required to offer firms the possibility of a holistic risk management. In this regard, insurers are in demand to conduct adequate risk transfer solutions to protect companies from resulting costs of IT security breaches. However, the creation of adequate risk solutions requires a broader knowledge and a sufficient database on cyber risks in general, as outlined previously. Thus, further research is particularly necessary in the area of empirical data on cyber insurance to promote further knowledge and empirical evidence, enabling insurers to offer efficient risk transfer tools such as cyber insurance. To conclude, although a successful cyber risk management comprising effectively operating internal risk management processes including emergency plans (i.e., business continuity management plans) can be implemented, well-designed risk transfer tools like cyber insurance still require further research to provide adequate coverage for the case of an actual cyber risk event.

APPENDIX A

Table A.1: Literature review on cyber risk management and cyber insurance

a) Academic literature

Topics	*Author(s)*	*Summary/Findings*
Correlation of cyber risk-classes/claims/interdependencies	Böhme and Kataria (2006)	This paper identifies cyber risk-classes that, when failing, influence (firm) internal correlation, and then models the effects on the general cyber insurance market. According to the authors, the internal correlation of failures influences the company's demand for cyber insurance, whereas the external correlation impacts the insurance premium. In conclusion, cyber insurance tends to be most suitable for risk classes with high internal and low global correlation, as low global correlation leads to lower premiums because risk pooling for the cyber insurer is possible, and the high internal correlation complicates self-insurance in the firm's network.
	Böhme (2005)	The author presents a brief literature review on cyber risk and a simplified insurance model for cyber risks, in which the correlation of cyber risks is implemented and costs for insurance are illustrated. As a major finding, the paper outlines the fact that traditional approaches (risk pooling) for insurance companies do not fit into the insurance of cyber risks, as these underlie different (higher) correlation of claims. These circumstances slow the maturity process of the cyber insurance market in general.
	Wang and Kim (2009)	Findings show that overall network risks tend to be higher for companies operating in neighboring countries than in more dispersed geographical locations. In addition, the authors provide implications for government policies, cyber insurers and businesses.
Loss valuation for cyber attack	Smith (2004)	Smith provides a basic approach for the valuation of tangible and intangible assets that have been harmed after a cyber crime attack, such as increased wage costs, lost productivity, losses from unavailability of network (website) and losses from lost data. As outlined in the paper, it is of major importance to legal entities and insurance companies to correctly valuate the losses and provide press reports, insurance companies, and the investigators with the correct loss figures from data and corporate information that has been collected before the cyber attack.
Risk management, adverse selection and moral hazard	Gordon, Loeb, and Sohail (2003)	The publication "A Framework for Using Insurance For Cyber Risk Management" provides general information on the pricing, adverse selection and moral hazard issues of cyber insurance. In addition, the authors implement a four-step cyber risk insurance decision plan by adapting a risk management framework to the needs of cyber insurance.
Cyber crime and shareholder value	Hovay and D'Arcy (2003)	The authors analyzed the financial effects (measured by the stock market reaction) of denial-of-service attacks on corporate websites. In general their results show no effects on the firms' stocks; however, "Internet-specific" firms showed a slight indication of negative abnormal returns in comparison to "non-Internet-specific" firms. So, the authors conclude that "non-Internet-specific" companies seem to overreact and invest capital into preventive measures, although cyber attacks might just have a low impact on the firms' stock price and shareholder value.
Capital market reactions to security breach announcements	Cavusoglu, Mishra, and Raghunathan (2004b)	The main findings in this paper show that, according to the results of an event study analysis, the impacts of security breaches (defined by the authors as "malicious attempts to interfere with a company's business and its information") directly impact a firm's market value (and the market value of firms that build security technology). On average, attacked firms showed a loss of 2.1 % of market value in the two days after the attack announcement, whereas the security technology firms showed abnormal returns of 1.36 % in the same two-day period. Further findings show that a) security breach costs are higher for Internet-only firms, and b) that the breach costs increased during the analyzed period. In addition, the authors' findings show that c) security breaches are more expensive for smaller firms than larger firms and d) the costs are not significantly different across different types

		of security breaches.
	Campbell et al. (2003)	Campbell et al. find that publicly announced (January 1995 to December 2000) information security breaches illustrate highly significant negative stock market reactions for security breaches of confidential data; however, breaches not involving confidential data show no significant reaction on the firms' stock.
Value-at-risk approach to IT security investments	Wang, Chaudhury, and Rao (2008)	The authors provide a VaR approach based on extreme value analysis to measures daily losses, and finally calculate the VaR in the context of information security risks. Furthermore, they apply their approach to a scenario at a financial institute to assess proper security solutions based on the firm's individual risk appetite.
Optimum amount of security investments	Gordon and Loeb (2002)	According to the authors' findings, based on the assumption of two different classes of security breach functions (class i: expected loss increases linearly with rising vulnerability, class ii: expected loss increases as a convex function with increasing vulnerability), the optimal amount of security investments never exceeds 37 % of the expected loss.
Pricing of cyber insurance	Herath and Herath (2011)	The authors introduce a cyber insurance model implementing copula methodology (Gumbel, Clayton copula) for adequate pricing of insurance policies based on three risk variables: a) occurrence of the event, b) the time when the insurance is paid and c) the amount paid. The premiums for first-party losses (e.g., due to virus) are thereby estimated by the application of ICSA survey data on computer incidences and further calculated for three insurance policy models: a) no deductible, b) with deductible and c) deductible, coinsurance and limit.
Implementation of cyber insurance in general	Mukhopadhyay et al. (2013)	In this paper, the authors build a decision model for whether and to what extent cyber insurance products are implemented. To do so, a copula-aided Bayesian belief network (Gaussian copula) for the assessment of cyber risks was built and further used for the modeling to compute expected losses, based on the likelihood of breach and impact of damages. By applying these findings to the concepts of risk modeling, the authors compute the proper cyber insurance premiums (utility-based preferential pricing), ensuring insurance companies do not default. To summarize, this papers advises, according to the main findings, the acquisition of cyber insurance products.
	Luzwick (2001)	The author states that cyber insurance is an appropriate measure if most of the firm's revenues are from e-commerce, as a cyber policy then assures a) higher earnings due to reduced intellectual property disclosure and fraud, b) lower overhead costs due to reduced improper behavior and c) smooth earnings in case of damage or fraud.
	Shackelford (2012)	Shackelford states that firms first should act proactively, improving security of IT systems and, second, should assess their insurance coverage and analyze their cyber risk exposure. Third, managers should decide whether to increase cyber insurance, which will depend on increasing investor awareness of cyber threats.
Cyber insurance market and market growth	Bandyopadhyay, Mookerjee, and Rao (2009)	This paper analyses the characteristics of the cyber insurance market, particularly pointing out the slow market growth and problems in terms of information asymmetry between the insurer and the insured. The authors advise a shift from information asymmetry to information symmetry, thus enabling the insurer to lower policy premiums (and therefore increase market growth). As a secondary substantial issue, the authors see a structural problem within the cyber insurance market, as secondary losses (such as indirect losses from consumer confidence, goodwill or reputation) need to be included in cyber insurance contracts to promote cyber insurance market growth.
Development of cyber insurance, adverse selection, and moral hazard	Majuca, Yurcik, and Kesan (2006)	This paper depicts the risk management process and the business perspectives of cyber insurance, analyzing the business idea of cyber insurers as well as policyholders. Additionally the authors consider the development of cyber insurance in the US market and examine recent (2006) cyber insurance products, followed by a detailed analysis of adverse selection and moral hazard issues in cyber insurance markets. In conclusion, a) cyber insurance provides economic incentives for insurers but also for policyholders and b) social welfare is increased as

		screening of policyholders enables insurers to differentiate between low-risk and high-risk policyholders, avoiding losses from the adverse selection.
Overview and insurability of cyber risk	Biener, Eling, and Wirfs (2015)	The paper provides a general overview on cyber insurance and focuses on the insurability of cyber risks based on the criteria of Berliner (1982). Additionally, they study empirical data from SAS OpRisk Global Data, and the loss data for certain cyber risk factors (actions of people, systems and technical failure, failed internal processes, external events) and further characteristics (region of domicile, industry, relation to losses in other firms, company size by number of employees).
Cyber risks as an incentive for overall network/Internet security	Bolot and Lelarge (2009)	Bolot and Lelarge question whether the insurance of cyber claims, which according to the authors will likely be correlated, and hence less attractive to insurers, makes sense. The authors' findings show that cyber insurance will increase overall Internet security, by promoting self-protection among all users of the network/Internet, and will thus provide general benefits.
	Shetty et al. (2010)	The paper shows that, against, e.g., Bolot and Lelarge (2009), a competitive cyber insurance market affects network security and safety in a negative way. With the availability of a competitive cyber insurance market, user incentives to improve IT security decrease (moral hazard problem/information asymmetries). Furthermore, the authors' results outline a negative outlook for cyber insurance market development and the general improvement of network security.

b) Practical literature and industry studies

Topics	*Author(s)*	*Summary*
Cyber-physical systems	acatech (2011)	Industry study on cyber-physical systems, its potential, challenges (in Germany) and recommendations for action.
	BITKOM (2010)	Study on embedded systems (synonym for CPS) shows definitions, figures, trends and examples of use of such systems.
Cyber risk in general	Harvard Business Review (2013)	The authors conduct a survey among 152 risk management representatives, presenting information on, e.g., the major threats, invested security standards, or purchase of insurance coverage as assessed by the interviewees.
	Towers Watson (2013)	The *Risk and Finance Manager Survey* says that financial service companies in particular are more likely to buy cyber policies (56 %) in comparison to non-financial firms (33 %), mainly due to higher risk exposure of personal customer data. This survey further questions, e.g., "reasons for not having a network security/privacy policy".
	Marsh (2013)	In the Marsh (2013) *Cyber Risk Survey*, 85 risk managers of European companies have been assessed on their views of cyber risks, e.g., their own recent cyber incidents, cyber insurance policies, and general assessment of losses and major expected threats from cyber risks.
	Zurich (2014)	Zurich outlines recommendations for governments and organizations with systemic responsibilities (system-wide risk) and for individual organizations (local risk), based on an aggregation of cyber risk into seven categories (internal IT enterprise, counterparties and partners, outsourced and contract, supply chain, disruptive technologies, upstream infrastructure, and external shocks).
Reputation and cyber risk	IBM (2012)	IBM (2012) provides a global survey of 472 senior executives, particularly focusing on the interdependencies between reputation and reputational losses due to cyber incidents.
Cyber war and industrial espionage	Corporate Trust (2012)	This study among 6,924 participating German surveyed companies analyses cyber threats and industrial espionage, providing findings, that, e.g., German medium-sized businesses are major victim of cyber espionage, leading to a loss to the German economy of 4.2 billion Euros per year.
	McAfee (2013)	McAfee (2013) tries to determine economic impacts from cyber crime and cyber espionage, by examining, e.g., components of malicious cyber activity and by using analogies to other kinds of crime and loss to find a maximum and minimum for the estimation of costs of malicious cyber incidents.

REFERENCES

acatech (2011): Cyber-Physical Systems. Driving Force for Innovation in Mobility, Health, Energy, and Production, acatech Position Paper, December 2011.

ACE (2013): Cyber-Risiken. Herausforderungen und Lösungen. FACEOFACE, Edition 2/2013, http://www.adfinity.de/servace/daten/FACEOFACE2_2013.pdf, access 04/02/2014.

Alali, F. A., and Yeh, C. (2012): Cloud Computing: Overview and Risk Analysis, *Journal of Information Systems*, Vol. 26(2): 13-33.

AWK Group (2013): Cyber-Security – aktuelle Trends und Schutzmaßnahmen. Eine Fachpublikation der AWK GROUP, June 2013, http://www.awk.ch/de/component/jdownloads/finish/102-informationssicherheit/517-cyber-security-aktuelle-trends-und-schutzmassnahmen, access 04/02/2014.

Baer, W. S., and Parkinson, A. (2007): Cyberinsurance in IT Security Management, *IEEE Security & Privacy*, Vol. 5(3): 50-56.

Bandyopadhyay, V. S., Mookerjee, R. C., and Rao, R. C. (2009): Why IT Managers Don't Go For Cyber-Insurance Products, *Communications of the ACM*, Vol. 52(11): 68-73.

Behrends, J. (2013): Cyber-Versicherungen haben eine große Zukunft, *Versicherungswirtschaft*, Nr. 2: 24-25.

Behrends, J. (2014): Die Cyber-Versicherung: Unerlässlicher Teil eines effektiven Risikomanagements, *I.VW Management-Information*, St. Galler Trendmonitor für Risiko- und Finanzmärkte, 01/2014: 13-16.

Berliner, B. (1982): Limits of Insurability of Risks. Prentice Hall, Englewood Cliffs, NJ.

Biener, C., Eling, M., and Wirfs, J. H. (2015): Insurability of Cyber Risk: An Empirical Analysis, *Geneva Papers on Risk and Insurance*, Vol. 40: 131-158.

Biener, C., Eling, M., Matt, A., and Wirfs, J. H. (2015): Cyber Risk: Risikomanagement und Versicherbarkeit, I-VW HSG Schriftenreihe, Band 54.

BITKOM (2010): Eingebettete Systeme – Ein strategisches Wachstumsfeld für Deutschland, BITKOM, 2010.

Bodin, L. D., Gordon, L. A., and Loeb, M. P. (2008): Information Security and Risk Management, *Communications of the ACM*, Vol. 51(4): 64-68.

Böhme, R. (2005): Cyber-Insurance Revisited, *Fourth Workshop on the Economics of Information Security (WEIS)*, Kennedy School of Government, Cambridge, MA.

Böhme, R., and Kataria, G. (2006): Models and Measures for Correlation in Cyber-Insurance, *Proc. of Workshop on the Economics of Information Security (WEIS)*, University of Cambridge, UK, June 26-28, 2006.

Bolot, J., and Lelarge, M. (2009): Cyber Insurance as an Incentive for Internet Security, *Seventh Workshop on the Economics of Information Security (WEIS)*, Hanover, NH.

Brenner, M., Gentschen Felde, N., Hommel, W., Metzger, S., Reiser, H., and Schaaf, T. (2011): Praxisbuch ISO/IEC 27001, Hanser Verlag, München.

Bundeskriminalamt (2012): Cybercrime. Bundeslagebild 2012, http://www.bka.de, access 04/12/2014.

Cabinet Office (2011): The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World, https://www.gov.uk, access 07/01/2014.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. (2003): The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, *Journal of Computer Security*, Vol. 11(3): 431-448.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004a): A Model for Evaluating IT Security Investments, *Communications of the ACM*, Vol. 47(7): 87-92.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004b): The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, *International Journal of Electronic Commerce*, Vol. 9(1): 69-104.

Cebula, J. J., and Young, L. R. (2010): A Taxonomy of Operational Cyber Security Risks, Software Engineering Institute, Carnegie Mellon University.

Choudhry, U. (2014): Der Cyber-Versicherungsmarkt in Deutschland, Eine Einführung, Springer Gabler Verlag, Wiesbaden.

COBIT (2012): COBIT 5. A Business Framework for the Governance and Management of Enterprise IT, http://www.isaca.org, access 07/12/2014.

Corporate Trust (2012): Studie: Industriespionage 2012, https://corporate-trust.de/, access 11/12/2014.

Corporate Trust (2014): Studie: Industriespionage 2014, https://corporate-trust.de/, access 11/12/2014.

Dinger, J., and Hartenstein, H. (2008): Netzwerk- und IT-Sicherheitsmanagement, Universitätsverlag Karlsruhe.

Dowdy, J. (2012): The Cybersecurity Threat to U.S. Growth and Prosperity, in: Securing Cyberspace: A New Domain for National Security (eds. Burns, N., and Price, J.), Aspen Strategy Group. http://www.aspeninstitute.org/, access 02/02/2014.

European Commission (2012): General Data Protection Regulation. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF, access 07/10/2013.

Federal Ministry of the Interior (BMI) (2011): Cyber-Sicherheitsstrategie für Deutschland, http://www.bmi.bund.de, access 07/03/2014.

Federal Ministry of the Interior (2014): IT-Sicherheitsgesetz, http://www.bmi.bund.de, access 09/03/2014.

Federal Office for Information Security (BSI) (2012): Register aktueller Cyber-Gefährdungen und -Angriffsformen. BSI-CS 026, Bonn, https://www.bsi.bund.de/, access 04/07/2014.

Federal Office for Information Security (2013): IT-Grundschutz-Kataloge. 13. Ergänzungslieferung-2013, https://www.bsi.bund.de, access 07/12/2014.

Fernandez, J. D., and Fernandez, A. E. (2005): SCADA Systems: Vulnerabilities and Remediation, *Journal of Computing Sciences in Colleges*, Vol. 20(4): 160-168.

Francis, T. (2013): Managing Cyber Risk: The Trifecta, *American Agent & Broker*, 85(8): 28.

Gatzert, N., Schmit, J., and Kolb, A. (2013): Assessing the Risks of Insuring Reputation Risk, *Journal of Risk and Insurance*, forthcoming.

Gibson, D. (2010): Managing Risk in Information Systems, Jones & Bartlett Learning, Sudbury, MA.

Gordon, L. A., and Loeb, M. P. (2002): The Economics of Information Security Investment, *ACM Transactions on Information and System Security*, Vol. 5(4): 438-457.

Gordon, L. A., Loeb, M. P., and Sohail, T. (2003): A Framework for Using Insurance for Cyber-Risk Management, *Communications of the ACM*, Vol. 46(3): 81-85.

Haas, A., and Hofmann, A. (2014): Risiken aus der Nutzung von Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit, *Zeitschrift für die gesamte Versicherungswissenschaft*, Vol. 103(4): 377-407.

Harvard Business Review (2013): Meeting the Cyber Risk Challenge, *Report by Harvard Business Review Analytical Services*, Harvard Business School. www.hbr.org, access 07/12/2013.

Herath, H. S. B., and Herath, T. C. (2011): Copula-based Actuarial Model for Pricing Cyber-Insurance Policies, *Insurance Markets and Companies: Analyses and Actuarial Computations*, Vol. 2(1): 7-20.

Hovay, A., and D'Arcy, J. (2003): The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms, *Risk Management and Insurance Review*, Vol. 6(2): 97-121.

Hult, F., and Sivanesan, G. (2013): Introducing Cyber, *Journal of Business Continuity & Emergency Planning*, 7(2): 97-102.

IBM (2012): Reputational Risk and IT, Findings from the 2012 IBM Global Reputational Risk and IT Study, www.ibm.com/, access 11/21/2014.

Kersten, H., Reuter, J., and Schröder, K.-W. (2013): IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Springer Vieweg Verlag, 4th Edition, Wiesbaden.

Lenz, S. (2009): Vulnerabilität Kritischer Infrastrukturen. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Luzwick, P. (2001): If Most of Your Revenue Is From E-Commerce, Then Cyber-Insurance Makes Sense, *Computer Fraud & Security*, Issue 3: 16-17.

Majuca, R. P., Yurcik, W., and Kesan, J. P. (2006): The Evolution of Cyberinsurance, *ACM Computing Research Repository* (CoRR).

Marsh (2013): Cyber Risk Survey, https://www.allianz-fuer-cybersicherheit.de, access 11/12/2014.

Marsh (2014): Cyber-Risiken. Marktentwicklung & Risikomanagement, Frankfurt, February 12, 2014, http://www.lloyds.com, access 07/05/2014.

McAfee (2013): The Economic Impact of Cybercrime and Cyber Espionage. Center for Strategic and International Studies.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., and Sadhukhan, S. K. (2013): Cyber-Risk Decision Models: To Insure IT or Not? *Decision Support Systems*, forthcoming.

Munich Re (2012): Cyberrisiken. Herausforderungen, Strategien und Lösungen für Versicherer, *Knowledge Series. Technology, Engineering and Risks.*

National Institute of Standards and Technology (NIST) (2013): Glossary of Key Information Security Terms, http://www.nist.gov, access 07/05/2014.

Njegomir, V., and Marović, B. (2012): Contemporary Trends in the Global Insurance Industry, *Procedia - Social and Behavioral Sciences*, Vol. 44: 134-142.

Öğüt, H., Raghunathan, S., and Menon, N. (2011): Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection, *Risk Analysis*, Vol. 31(3): 497-512.

Ponemon Institute (2013): 2013 Cost of Data Breach Study: Global Analysis, http://www.symantec.com, access 11/04/2013.

Posthumus, S., von Solms, R. (2004): A Framework for the Governance of Information Security, *Computers & Security*, Vol. 23: 638-646.

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001): Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, *Control Systems, IEEE*, Vol. 21(6): 11-25.

Romeike, F., and Hager, P. (2009): Erfolgsfaktor Risiko-Management 2.0, Gabler Verlag, 2nd Edition, Wiesbaden.

Shackelford, S. J. (2012): Should Your Firm Invest in Cyber Risk Insurance? *Business Horizons*, forthcoming.

Shetty, N., Schwartz, G., Felegyhazi, M., and Walrand, J. (2010): Competitive Cyber-Insurance and Internet Security, in: Economics of Information Security and Privacy (eds. Moore, T., Pym, D., and Ioannidis, C.), New York, NY: 229-247.

Siegel, C. A., Sagalow, T. R., and Serritella, P. (2002): Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security, *Information Systems Security - Security Management Practices*, September/October 2002.

Sinanaj, G., and Muntermann, J. (2013): Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis, in: *Proceedings of the 26th International Bled eConference, Bled, Slovenia, June 9-13, 2013*: 78-89.

Slay, J. and Miller, M. (2008): Lessons Learned From the Maroochy Water Breach, in: IFIP International Federation for Information Processing, Vol. 253, Critical Infrastructure Protection (eds. E. Goetz and S. Shenoi), Springer, Boston: 73-82.

Smith, G. S. (2004): Recognizing and Preparing Loss Estimates from Cyber-Attacks, *Information Systems Security*, Vol. 12(6): 46-58.

Spörrer, S. (2014): Business Continuity Management: ISO 22301 und weitere Normen im Rahmen der Informationstechnologie, Kölner Wissenschaftsverlag.

Stoneburner, G., Goguen, A., and Feringa, A. (2002): Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology. Special Publication 800 (30).

Towers Watson (2013): 2013 Risk and Finance Manager Survey, www.towerswatson.com/, access 11/23/2014.

Tuttle, B., and Vandervelde, S. D. (2007): An Empirical Examination of CobiT as an Internal Control Framework for Information Technology, *International Journal of Accounting Information Systems*, Vol. 8: 240-263.

Von Solms, R., and van Niekerk, J. (2013): From Information Security to Cyber Security, *Computers & Security*, Vol. 38: 97-102.

Wang, J., Chaudhury, A., and Rao, H. R. (2008): A Value-At-Risk Approach to Information Security Investments, *Information Systems Research*, Vol. 19(1): 106-120.

Wang, Q.-H., and Kim, S.-H. (2009): Cyber Attacks: Cross-Country Interdependence and Enforcement, Working Paper. National University of Singapore.

World Economic Forum (2012): Global Risks, http://www.weforum.org/, access 11/21/2014.

World Economic Forum (2014): Global Risks, http://www.weforum.org/, access 11/21/2014.

Zurich (2014): Risk Nexus, Beyond Data Breaches: Global Interconnections of Cyber Risk, www.zurich.com, access 11/21/2014.