ZVersWiss (2015) 104:615–634
DOI 10.1007/s12297-015-0316-8

ABHANDLUNG

Components and challenges of integrated cyber risk management

Thomas Kosub

Published online: 1 September 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 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.

Zusammenfassung Cyber Risiken sind durch die zunehmende Anzahl und Höhe der verursachten Schäden zu einer relevanten Bedrohung für Unternehmen geworden. Aus diesem Grund ist ein umfassendes Cyber Risikomanagement für Unternehmen notwendig, um die kontinuierliche Funktionsfähigkeit der unternehmerischen Tätigkeiten unter Berücksichtigung dieses Risikos zu gewährleisten. Dieses Paper fokussiert daher auf die zentralen Bestandteile eines Cyber Risikomanagements auf Basis der akademischen Literatur und der relevanten Sicherheitsstandards (ISO/IEC 27000). Das Paper beschreibt schrittweise den Cyber Risikomanagementprozess und stellt alle wichtigen Schritte eines umfassenden Cyber Risikomanagements dar. Darüber hinaus werden bestehende Herausforderungen bei der Absicherung von Cyber Risiken diskutiert.

T. Kosub (✉)
Department of Insurance Economics and Risk Management, Friedrich-Alexander University Erlangen-Nürnberg (FAU),
Lange Gasse 20, 90403 Nürnberg, Germany
e-mail: thomas.kosub@fau.de

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] 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.[3] In addition, Biener et al. (2015b, 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 set 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.[4] 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.[5] In addition, many countries (more than 50) have published strategic proposals on cyber security and cyber risks as well.[6] 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.[7] 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 1 million Euros or 2 %[8] of the worldwide annual

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

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

[3] http://www.roberthalf.de/id/PR−04055/cyber-security-unterschaetzt, access 01/27/2015.

[4] Dowdy (2012, p. 129).

[5] German Federal Ministry of the Interior (2014, p. 1).

[6] Von Solms and van Niekerk (2013, p. 97).

[7] German Federal Data Protection Act, Haas and Hofmann (2014).

[8] 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 million

turnover of the company responsible for the violation.[9] In addition, any privacy data violations will have to be reported, if feasible, to the supervisory authority within 24 h of detection.[10] Regulatory restrictions will certainly support 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.[11] The increasing severity and frequency of cyber incidents 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 et al. 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 et al. 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 et al. (2004b) state that costs among the different types of security breaches do not differ and find that market value drops by 2.1 % over 2 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 et al. (2015a) provide an empirical analysis of the insurability of cyber risks and Biener et al. (2015b) additionally analyze cyber risk management. This paper aims to contribute to the 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. (2015b), for instance, this paper primarily focuses on the cyber risk management process and links various 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 and the cyber terminology. In Sect. 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 Sect. 4, and Sect. 5 concludes.

Euros, whichever is the larger value (http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf, access 03/04/2014).

[9] European Commission (2012, pp. 92–93).

[10] 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 (§ 42a German Federal Data Protection Act; Behrends, 2013, p. 25).

[11] Behrends (2013, p. 25).

2 Definition and cyber terminology

One definition of the term *cyber* (an abbreviation for *cyber space*) encompasses all digital networks required for storage, modification and communication of information.[12] 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".[13]

Returning to the actual definition of *cyber risks*, one can treat them in a narrow or broader sense.[14] For instance, Öğüt et al. (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 et al. (2015a) (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.[15]

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. 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. Such *cyber attacks* can further be categorized into *espionage*, e.g., illegitimate information retrieval or *sabotage* such as intentional damage to IT systems.[16]

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.[17] This is particularly the case with c*yber-physical systems*, i.e., electronic components monitoring and controlling physical entities such as, e.g., embedded systems in trains or airplanes, but also control systems for, e.g., water pumps. 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 3 months.[18] The vulnerability of such Supervisory Control and Data Acquisition (SCADA) systems has

[12] Biener et al. (2015a, p. 132), Cabinet Office (2011, p. 11).

[13] NIST (2013, p. 58).

[14] Biener et al. (2015a, p. 132), Hult and Sivanesan (2013, p. 97).

[15] Biener et al. (2015a, p. 133), Cebula and Young (2010, p. 2).

[16] German Federal Ministry of the Interior (2014), German Federal Office for Information Security (2012).

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

[18] Slay and Miller (2008, pp. 73–75).

often been discussed, but in practice, however, SCADA systems are still often in use for controlling infrastructure facilities.[19] 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.[20] 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.[21]

With regard of *cyber security*, Hult and Sivanesan (2013), for instance, determine a mix of protection of IT systems (IT security) and information security.[22] 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.[23] In this regard, the ISO/IEC 27001 defines abstract protection goals and security requirements for information 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*.[24]

[19] Fernandez and Fernandez (2005, pp. 162–164), Rinaldi et al. (2001).

[20] E.g., Hult and Sivanesan (2013, p. 99), Lenz (2009, pp. 17–18).

[21] Lenz (2009, pp. 24–25).

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

[23] Von Solms and van Niekerk (2013, pp. 100–101).

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

3 Cyber risk management

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 (Sect. 404) and the European Directive 2006/43/EC[25], 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.[26] 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.[27]

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[28], representing the continuous improvement and optimization of enterprise-wide information security. 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.[29] 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 integrated cyber risk management process.

[25] 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).

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

[27] BaFin—MaRisk VA 7.2.2.2, https://www.bafin.de, access 11/28/2014.

[28] 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).

[29] Brenner et al. (2011, pp. 21–24).

Table 1 Basic operational cyber risk management process. (For further recommendations and measures see, e.g., Biener et al. (2015b, pp. 34–50), Gordon et al. (2003, pp. 83–84), Kersten et al. (2013, p. 48), Romeike and Hager (2009, pp. 377–387), Shackelford (2012, p. 16), Zurich (2014, pp. 22–27))

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
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)

We next present the main components and success factors for a basic cyber risk management approach (see Table 1; see also Biener et al. 2015b). We primarily focus on the previously introduced ISO/IEC 27000 series of standards[30] 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. As previously explained, the continuous evaluation, assessment and control of risks is necessary to provide an efficient cyber

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

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.

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.[31] 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.[32] 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.[33] 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.[34] 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[35] 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 decide about the level of information and IT security.[36]

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.[37] 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.[38] In this regard, risk identification comprises a detailed

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

[32] Brenner et al. (2011, p. 16), Kersten et al. (2013, pp. 24–25).

[33] Luzwick (2001, pp. 16–17), Marsh (2014, p. 11).

[34] E.g., Shackelford (2012, pp. 4–5).

[35] 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).

[36] ISO/IEC 27005 Annex A.

[37] 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.

[38] Kersten et al. (2013, p. 31).

approach, consisting of the identification of *threats* (to an information asset), the *vulnerabilities* (individual weakness of information security management system protecting the information asset) and the *consequences* (expected amount of loss due to harmed information asset). Furthermore, firms need to determine their already implemented *control objectives* (implemented risk control measures). Such an analysis can be done either by 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. 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 estimated incorrectly.[39] The risk identification process requires a substantial analysis ranging from physical security to general vulnerabilities of the IT systems.[40] 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*.[41] 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*.[42]

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 valuable for the firm and therefore need to be protected by a cyber risk management (i.e., information security management system).[43] Hence, the identified assets are at risk, if, e.g., *cyber attacks, system blackouts, lack of staff, natural hazards, carelessness* or *operating errors* occur.[44]

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. In the example of Zurich Cyber & Data Protection, the questionnaire includes questions regarding, for instance, *business activities* (e.g., the proportion of online purchases/bill payments/banking or trading) or *network security* (e.g., whether firewall technology is used at all Internet points). 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

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

[40] Siegel et al. (2002, p. 34).

[41] Biener et al. (2015a, p. 139).

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

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

[44] Kersten et al. (2013, pp. 27–28).

risks or requests for larger financial coverage, insurance companies identify the individual firm's risk by a technical underwriting.[45]

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*.[46] 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 decision as to whether risks are acceptable or if risk response measures are required has to be made by the management.[47] 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.[48] 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). 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.[49] 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) must be estimated.[50]

A classification of costs (and the degree of uncertainty in the estimation) from security breaches can further be found in Cavusoglu et al. (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.[51] In addition, costs for debt or equity capital might increase due to greater risk exposure.[52] Therefore, the damages, costs and losses from cyber crime should not only be associated with

[45] E.g., Baer and Parkinson (2007, p. 53).

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

[47] Brenner (2011, p. 39).

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

[49] Smith (2004, p. 51).

[50] Smith (2004, pp. 52–53).

[51] Öğüt et al. (2011, p. 497), Smith (2004, pp. 50–51).

[52] Cavusoglu et al. (2014b, p. 72).

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.[53] 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.[54]

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 et al. (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 2 days after the attack announcement. Additionally, the market value of firms that build security technology showed an abnormal return of 1.36 %, also within 2 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.[55] 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.

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., sales), for instance, can adequately handle the loss estimation after a cyber incident has occurred, as copious information from company statistics (e.g., sales or new customers on the website) and the financial information (e.g., average sales per customer) is required for calculation.[56] 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.[57]

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.[58] As 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

[53] Smith (2004, p. 46).

[54] Öğüt et al. (2011, p. 497).

[55] Cavusoglu et al. (2014a, pp. 72–73).

[56] Smith (2004, p. 51).

[57] Smith (2004, p. 55).

[58] Romeike and Hager (2009, p. 379).

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.[59]

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.[60] Certain subcategories of cyber risks can however 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.[61]

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.[62] 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 network or the company website; mitigating chances of successful denial-of-service attacks).[63] The ISO/IEC 27001 lists some extensive control objectives and control measures that can be applied to mitigate risks, such as *access control, cryptography* or *physical and environmental security*, for instance.[64]

Still, such risk mitigating measures imply costs, and hence the trade-off of costs and reduced losses (e.g. reduced probability of occurrence or severity) needs to be individually analyzed. In addition, ISO/IEC 27005 specifies the following

[59] Brenner et al. (2011, pp. 40, 42), Romeike and Hager (2009, pp. 378–380).

[60] Romeike and Hager (2009, p. 161).

[61] E.g., Gibson (2010, p. 17).

[62] Francis (2013, p. 28).

[63] Gibson (2010, p. 96).

[64] 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.

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.[65] To further assess the value of IT security investments, Cavusoglu et al. (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 et al. (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 individual 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.[66] 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. 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 contrast, the US market consists of more than 30 insurance companies provid-

[65] ISO/IEC 27005 Annex F.

[66] E.g., Behrends (2014, p. 16), Kersten et al. (2013, p. 59), Zurich (2014, p. 27).

ing 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 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, i.e. 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.[67] Regarding the purchase of cyber insurance, Biener et al. (2015b, p. 65)[68] 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.

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.[69]

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 measures, *risk control* is the subsequent step in a holistic risk management. Hereby, the corresponding ISO/IEC 27005 demands an ongoing review of risk factors as well as the risk

[67] Siegel et al. (2002, p. 33).

[68] Based on Baer and Parkinson (2007), Gordon et al. (2003), Shackelford (2012).

[69] Brenner (2011, p. 42), Kersten et al. (2013, p. 60).

management in general (e.g., risk acceptance criteria, risk assessment approach, etc.). Companies should thus 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.[70]

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.[71] Therefore, besides monitoring the identified risks, proactive trainings of all employees[72] and *regular testing* of established IT security measures, it is necessary to provide a well operating risk management system.[73] 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.[74] Roles and organizational structures are outlined in the COBIT framework, for instance.[75]

5.2 The connection of *risk management, risk governance* and *cyber risks* can be seen as a value-creating combination.[76] For instance, in the actual 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.[77] A BCM generally comprises actions that are required to ensure the operability of core business processes. 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 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. 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

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

[71] E.g., Biener et al. (2015a, p. 139).

[72] 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.

[73] Francis (2013, p. 28).

[74] Stoneburner et al. (2002, p. 6).

[75] COBIT (2012, pp. 76–77).

[76] Biener et al. (2015b, p. 34).

[77] Romeike and Hager (2009, pp. 396–399).

the recovery of lost data or replacement of non-usable hardware or IT infrastructure. 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 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. In this case, 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 or resulting losses. Particularly, *Internet-only* firms and service platforms (e.g., information and communication platforms such as Twitter.com, or e-commerce 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.[78] Furthermore, cyber risk management should be interpreted as a process, being subject to continuous monitoring, reviewing and improvement.[79] Finally, the management should be aware that risk awareness among all stakeholders (employees, suppliers, etc.) creates a sound environment for good cyber risk management.

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. Challenges partly arise from 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 (e.g., e-commerce) affects the vulnerability of data privacy and will certainly increase the relevance of cyber risk management,

[78] Cavusoglu et al. (2004b, pp. 75–76), Smith (2004, p. 51).

[79] Biener et al. (2015b, p. 36).

as the continuing digitalization will consequently increase the amount of digital personal data and hence expand the potential for cyber risks.

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. 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.[80] In addition, the fast changing technological evolution demands for a dynamic cyber risk management process, which quickly adapts to a changed cyber environment and its cyber risk exposures.[81]

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.[82] This reduces the total knowledge base on cyber risks, and although data from operational risk databases seem to be available, the quantity and quality of these data appear to be insufficient to cover the breadth of cyber risk incidents.[83] The future reporting and awareness of cyber incidents, however, will be strengthened with the implementation of new regulatory requirements by the European Commission (2012) (European General Data Protection Regulation), for instance. Finally, an essential challenge for effective cyber risk management consists from risk culture and risk knowledge, as a large amount of IT users lacks the general awareness of cyber risks, i.e., its threats and consequences.

5 Summary

In this paper, we outline the main components and challenges of an integrated cyber risk management. 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

[80] Baer and Parkinson (2007, pp. 53–54), Böhme (2005, p. 13).

[81] Biener et al. (2015b, p. 46).

[82] Cavusoglu et al. (2014b, p. 87), Dowdy (2012, p. 131), Gordon et al. (2003, p. 82), Herath and Herath (2011, p. 9).

[83] E.g., Biener et al. (2015a, p. 139).

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, the cyber risk management itself should be implemented as a continuous process. Finally, firms still face many challenges with the implementation of cyber risk management that need to be considered thoroughly, such as the change of traditional business models, the correct asset valuation and the loss determination, or lacking awareness for cyber risks in general.

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. In this regard, insurers are in demand to conduct adequate risk transfer solutions to protect companies from resulting costs of cyber risk incidents. However, the product design 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 and beneficial risk transfer tools.

References

Baer, W.S., Parkinson, A.: Cyber insurance in IT security management. IEEE. Secur. Priv. **5**(3), 50–56 (2007)

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

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

Biener, C., Eling, M., Wirfs, J.H.: Insurability of cyber risk: An empirical analysis. Geneva. Pap. Risk. Ins. **40**, 131–158 (2015a)

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

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

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

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

Cabinet Office: The UK cyber security strategy. Protecting and promoting the UK in a digital world. https://www.gov.uk (2011). Accessed 01 July 2014

Campbell, K., Gordon, L.A., Loeb, M.P., Zhou, L.: The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. J. Comput. Secur. **11**(3), 431–448 (2003)

Cavusoglu, H., Mishra, B., Raghunathan, S.: A model for evaluating IT security investments. Commun. ACM. **47**(7), 87–92 (2004a)

Cavusoglu, H., Mishra, B., Raghunathan, S.: The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. Int. J. Electron. Comm. **9**(1), 69–104 (2004b)

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

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

COBIT: COBIT 5. A business framework for the governance and management of enterprise IT. http://www.isaca.org (2012). Accessed 12 July 2014

Dinger, J., Hartenstein, H.: Netzwerk- und IT-Sicherheitsmanagement. Universitätsverlag Karlsruhe, Karlsruhe (2008)
Dowdy, J.: The Cyber security 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/ (2012). Accessed 02 Feb 2014
European Commission: General data protection regulation. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF (2012). Accessed 10 July 2013
Fernandez, J.D., Fernandez, A.E.: SCADA systems: Vulnerabilities and remediation. Journal. Comput. Sci. Coll. **20**(4), 160–168 (2005)
Francis, T.: Managing cyber risk: The Trifecta. Am. Agent. Brok. **85**(8), 28 (2013)
German Federal Ministry of the Interior (BMI): http://www.bmi.bund.de (2014). Accessed 03 Sept 2014
German Federal Office for Information Security (BSI): https://www.bsi.bund.de/ (2012). Accessed 07 April 2014
Gibson, D.: Managing Risk in Information Systems. Jones & Bartlett Learning, Sudbury (2010)
Gordon, L.A., Loeb, M.P.: The economics of information security investment. ACM Trans. Inf. Syst. Secur. **5**(4), 438–457 (2002)
Gordon, L.A., Loeb, M.P., Sohail, T.: A framework for using insurance for cyber-risk management. Commun. ACM. **46**(3), 81–85 (2003)
Haas, A., Hofmann, A.: Risiken aus der Nutzung von Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit. Zeitschrift für die gesamte Versicherungswissenschaft. **103**(4), 377–407 (2014)
Herath, H.S.B., Herath, T.C.: Copula-based actuarial model for pricing cyber-insurance policies. Insur. Mark. Co.: Anal. Actuar. Comput. **2**(1), 7–20 (2011)
Hovay, A., D'Arcy, J.: The impact of denial-of-service attack announcements on the market value of firms. Risk. Manage.Insur. Rev. **6**(2), 97–121 (2003)
Hult, F., Sivanesan, G.: Introducing cyber. J. Bus. Contin. Emer. Plan. **7**(2), 97–102 (2013)
Kersten, H., Reuter, J., Schröder, K.-W.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, 4th edn. Springer Vieweg Verlag, Wiesbaden (2013)
Lenz, S.: Vulnerabilität Kritischer Infrastrukturen. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2009)
Luzwick, P.: If most of your revenue is from e-commerce, then cyber-insurance makes sense. Comput. Fraud. Secur. **2001**(3), 16–17 (2001)
Marsh: Cyber-Risiken. Marktentwicklung & Risikomanagement, Frankfurt. http://www.lloyds.com (2014). Accessed 05 July 2014
Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sadhukhan, S.K.: Cyber-risk decision models: To insure IT or not? Decis. Support. Syst. (2013) (forthcoming)
Munich Re: (2012): Cyberrisiken. Herausforderungen, Strategien und Lösungen für Versicherer, Knowledge Series. Technology, Engineering and Risks
National Institute of Standards and Technology (NIST): Glossary of key information security terms. http://www.nist.gov (2013). Accessed 05 July 2014
Öğüt, H., Raghunathan, S., Menon, N.: Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. Risk. Anal. **31**(3), 497–512 (2011)
Posthumus, S., von Solms, R.: A Framework for the governance of information security. Comput. Secur.. **23**, 638–646 (2004)
Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K.: Identifying, understanding, and analyzing critical infrastructure interdependencies. Control. Syst. IEEE. **21**(6), 11–25 (2001)
Romeike, F., Hager, P.: Erfolgsfaktor Risiko-Management 2.0, 2nd edn. Gabler Verlag, Wiesbaden (2009)
Shackelford, S.J.: Should your firm invest in cyber risk insurance? Bus. Horiz. (2012) (forthcoming)
Siegel, C.A., Sagalow, T.R., Serritella, P.: Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. Information Systems Security - Security Management Practices (2002)
Sinanaj, G., Muntermann, J.: Assessing Corporate Reputational Damage of Data Breaches: An Empirical Analysis, in: Proceedings of the 26th International Bled eConference, pp. 78–89. Bled, Slovenia, June 9–13 2013
Slay, J., Miller, M.: Lessons learned from the maroochy water breach. In: Goetz, E., Shenoi, S. (eds.) IFIP International Federation for Information Processing, vol. 253, Critical Infrastructure Protection, pp. 73–82. Springer, Boston (2008)
Smith, G.S.: Recognizing and preparing loss estimates from cyber-attacks. Inf. Syst. Secur. **12**(6), 46–58 (2004)

Stoneburner, G., Goguen, A., Feringa, A.: Risk management guide for Information Technology systems, National Institute of Standards and Technology. Special Publication 800(30) (2002)
Von Solms, R., van Niekerk, J.: From information security to cyber security. Comput. Secur. **38**, 97–102 (2013)
Wang, J., Chaudhury, A., Rao, H.R.: A value-at-risk approach to information security investments. Inf. Syst. Res. **19**(1), 106–120 (2008)
Wang, Q.-H., Kim, S.-H.: Cyber Attacks: Cross-Country Interdependence and Enforcement, Working Paper. National University of Singapore, 2009
Zurich: (2014): Risk Nexus, Beyond Data Breaches: Global Interconnections of Cyber Risk. www.zurich.com. Accessed 21 Nov 2014