J Manag Gov (2017) 21:793–814
DOI 10.1007/s10997-016-9358-0

Information security governance: pending legal responsibilities of non-executive boards

Laura Georg[1]

Published online: 8 September 2016

Abstract The study shows that a structural conflict of interest in non-executive boards exists due to missing corporate governance structures and a lack of awareness for legal issues with regard to information security risks. Non-executive boards receive information on strategic security threats as a part of their oversight function to fulfill investor interest in transparency. At the same time, they act as representatives of company stakeholders and have an interest to counteract to information security risks based on the stakeholder's risk disposition. If not properly structured by corporate governance rules, these different interests may lead to regulatory aberrations on non-executive board level. The study analyses a Deutsche Telekom AG case where non-executive board members, employees, and journalists fell victim to a spying scandal subject to the German telecommunications secrecy law in 2005–2006. The analysis demonstrates how the handling of information security on non-executive board level bears governance risks as well as legal risks that are insufficiently addressed in corporate governance research. The paper contributes to avoid a reproduction of events in the future, by suggesting the principle of a segregation of duties on non-executive boards as well as providing an overview of relevant legislative requirements that clarify tasks of non-executive board members with regard to information security. The study therefore helps protecting corporations and their stakeholders from similar consequences of missing corporate security governance.

Keywords Information security governance · Operational risk management · Non-executive board research · Information security legal obligations · Conflict of interest

✉ Laura Georg
Laura.Georg@ntnu.no

[1] Norwegian University of Science and Technology NTNU, P. O. Box 191, 2802 Gjøvik, Norway

1 Introduction

> Boards that choose to ignore, or minimize, the importance of cyber security oversight responsibility, do so at their own peril. SEC Commissioner Luis A. Aguilar, June 10, 2014.

1.1 Information security as a strategic risk

As a discipline in research and business, information security has undergone an impressive development in the past decades. It started as technical topic (McCarthy 1995; Martin 1973) focused on developing security technology to improve defense mechanisms against attacks, such as identity management, intrusion detection systems and malware detectors. It also became a research subject in procedural complexity (Siponen 2001; Rainer et al. 2007) introducing procedural, economic and managerial aspects of information security in the profession. This made it increasingly accessible to managers and non-IT professionals to grasp the risk landscape and include information security in the organization's decision-making process and business strategy (Georg 2007). This accessibility made information security become a regular topic in executive board meetings—together with the threat of losses in a digital economy based on the confidentiality, integrity and availability of its core assets. As a result information security has attracted multi-faced managerial interest and became their second biggest concern in 2015, according to 103 US CEOs interviewed in a PWC study (PricewaterhouseCoopers 2015). The importance is measured in its financial impact in terms of losses following an information security event. Yet in 2003, researchers showed a correlation between information security incidents and companies' stock market performance (Garg et al. 2003). Management, employees, clients, but also investors and owners are concerned about millions of lost credit card data, including personal information disclosed to unauthorized individuals, as in the large media scandal of the Target Group in 2014 (Wall Street Journal 28/05/2014). Equally, they are concerned about years of news coverage following the spying scandal at Deutsche Telekom from 2008 to 2012 (Spiegel 2008/22, Wiwo 10/10/2012). Another study from July 2014 estimated losses in the countries with the highest confidence in their loss ratings with 0.64 % in US, 0.64 % in Norway, 1.6 % in Germany and 0.63 % in China of GDP (McAfee 2014). In financial terms, the loss in Germany alone was thus estimated at over USD 62 billion.

But it is not only the fear of becoming a victim of an information security attack, which draw board attention towards security. The increasing investments and costs related to security let companies think about alternative ways to manage it. Most possibilities to optimize reactive security management have been extensively discussed, researched and tested, where post-breach analysis is the basis for new preventive and detective security mechanisms. While investments into these reactive mechanisms reach every year all-time highs, organizations, industries, and states alike look at different solutions to stop the ever-increasing number of attacks and their financial consequences. Increasing attention therefore goes to proactive

cyber defense mechanisms at industry level in order to actively manage security risks (Christiansen and Westervelt 2015). This however bears new challenges for company boards as well as the regulator.

1.2 Legal requirements to non-executive boards in information security

Compared with the attention and scale of investments to prevent and detect information security attacks at the executive board level the expertise and attention at non-executive boards is comparably low although the owners of the key assets, the shareholders, that need protection, are represented in the non-executive boards. One reason to focus on information security is that it deals with particularly sensitive legal issues that could present significant risks from lacking legal prosecution. Following a large-scale data security incident, the board members at Target Group were among the first to be sued for breach of fiduciary duty. The Institutional Shareholder Services Inc., which advises shareholders how to vote on corporate ballots, called on Target Group shareholders to oust seven of the company's ten directors. They commented the cases with "these committees should have been aware of, and more closely monitoring, the possibility of theft of sensitive information." (Wall Street Journal 28/05/2014) 6 months later a US survey of 75 board members found 59 % of them saying their board is more involved in cyber security today than it was 12 months ago. However, 29 % say they are not briefed on the topic at all and 30 % only once a year (BDO 2014).

1.3 History of information security scandals with strategic impact

In the years 2000–2010, several cases in Germany showed a lax treatment of security sensitive data at major companies including Deutsche Bank AG (Wall Street Journal 2009), Deutsche Post AG (Wirtschaftswoche 21/1/2009), Lufthansa AG (Spiegel 2008/24), and Deutsche Bahn AG (Handelsblatt 2009). This study demonstrates areas, where non-executive boards lack guidance on how to govern information security effectively. It therefore draws conclusions from a case study of Deutsche Telekom between 2005 and 2011 and a comprehensive qualitative analysis of legal frameworks impacting non-executive board governance decisions in a single institutional setting in Germany. As a result the study emphasizes limited or non-existent overview over legal obligations, rights, and jurisdictional consequences as part of existing and further research.

1.4 The information security governance gap in corporate governance research

Little research has been conducted on the governance of information security risk on a non-executive board level. Also, on its strategic controlling and arising conflict of interest between supervision of the security department, risk reporting and legislation, we miss profound analysis. Finally, we lack detailed accounts to better address information security risk in corporate governance. The objective of this study is to start filling in these three blanks.

My starting hypothesis is as following: There is a structural conflict of interest at the non-executive board level between the reporting of security risks and the risk-based supervision of risk mitigation in the area of information security. This may also lead to legal aberrations. At the end, a better knowledge of legislation will lead to a better judgment of information security and hence to manage operational risks that conflict on non-executive board level against improving strategic control in corporate governance.

The paper will first return to current research in operational risk management (Part 1) and then explain the deployed research methodology (Part 2). An empirical analysis of the case study at Deutsche Telekom (Part 3), followed by an overview of related legal requirements in security on non-executive board level (Part 4), leads to the discussion of empirical data in the context of legal responsibilities of non-executive board's role and its implications on governance research (Part 5). In the final section, developments in security potentially impacting future security governance are described (Part 6) leading to potential future areas of research (Part 7).

2 Operational risk management in corporate governance research

Information security as part of operational risk management is not yet seen as a separate research domain in corporate governance research (Shleifer and Vishny 1997; Bailey 2013) and few specific research projects investigate best practices in corporate governance at non-executive boards. One of the standards that comment on the role of board in risk management is the Enterprise Risk Management (ERM)—Integrated Framework from the Committee of Sponsoring Organizations of the Treadway Commission defining ERM as "A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and management risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." (COSO 2014, 2) The framework thus includes both identification and management of risks in the non-executive board function. Hence, the non-executive board reflects stakeholders' risk appetite, thus, entrepreneurial aspects as well as the control function, creating transparency on operational risks to investors. Both functions again must follow legislation to create transparency on risks as well as not taking unbearable risks.

Yatim (2010) shows in a regression analysis that the establishment of a risk management committee in addition to the audit committee is favorable. He analyzed Malaysian listed firms and found strong support for an association between the establishment of a risk management committee and board structures (Yatim 2010). His research indicates risk management committees to improve awareness for internal control and internal control systems. Yatim suggests a separation of the control function from a committee specialized in business risks. He bases his research on Power's findings that show a shift of firm's corporate governance focus from legal and regulatory compliance to broader-based business risks (Power 2000). As introduced by Turnbull (1999), this task is often taken over by the audit

committee. Zaman (2001) found that expectations towards audit committees to perform more than high-level reviews are unreasonable due to their lack of expertise, missing time, and new legislative forms being imposed on them (Zaman 2001). While Yatim focuses his research on a governance improvement through specialization argument, standards see, in particular for information security, the application of segregation of duties necessary while assigning responsibilities. The separation of duty is applied in several standards, such as ISO 27001:2013 (International Organization of Standardization 2013) to ensure the separation of executive and judicative:

> Control Information security roles and responsibilities, A.6.1.1: All information security responsibilities shall be defined and allocated
>
> Control Segregation of duties, A.6.1.2: Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. (ISO 27001:2013, Annex A)

In order to elaborate further why a separation of duties is useful from a governance perspective. Crombie (2011) lined out theoretical conceptions that opposed corporate logic to investor logic. He reflects the motivation and incentives of non-executive board members and their influence on organizational behavior (Crombie 2011). Whilst strict corporate logic asserts directors and executives as knowledgeable professionals that can be trusted by stakeholders to act in their best interest, investor logic asserts that independent directors should be appointed to control executives (Zajac and Westphal 2004). Investor interest, as corporate objective, is share- and not stakeholder value maximization (Crombie 2011). Thus, what would an application of corporate versus investor logic as described by Crombie mean for security governance? From the perspective of investor logic, maximizing the company value affects the management of corporate security. The investor decision to either invest into mitigation of a risk versus a simple acceptance of this risk depends on multiple factors. Beside the factor of market development, these can be individual risk dispositions or overall company performance. The investor logic can therefore be quite varied, if it comes to security and might not overlap with general best practices used in corporate security standards.

Further, a conflict of interest may arise when private corporations are concerned primarily with loss prevention rather than law enforcement. In cases of acts being both harmful to the corporation and illegal, law enforcement agencies are not oriented towards recouping the losses of the company (Johnsten and Shearing 2003), therefore corporation tend to try overcoming security issues themself. Lippert et al. (2013) conclude that corporations often employ security personnel because they permit greater control of and a superior capacity to investigate acts deemed harmful but which are not necessarily illegal. The use of corporate security allows the corporation to prohibit conduct it deems harmful to its profit accumulation, but which may not be deemed illegal (Lippert et al. 2013). But this entrepreneurial incentive on non-executive level has so far not been investigated in current research in operational risk management.

The lack of corporate governance research received particular attention in the aftermaths of the financial crisis (Hilb 2011). Ahrens' call to adjust the research frontier in corporate governance resulted from his conclusion that current corporate governance research has failed to address the real risk—which became apparent in the financial crisis (Ahrens et al. 2011). While corporate governance research is encouraged to move more towards the area of value creation (Huse et al. 2011), operational risk management and in particular information security governance are focusing mainly on the entrepreneurial versus control aspect in research but require just as much attention to avoid further gaps in risk management.

3 Research method: case study based on in-depth content analysis

The research provided to fill this gap is based on a qualitative case study of the involvement of the Non-Executive board of Deutsche Telekom AG during the spy-case beginning at 2005 and ending with the discharge of the non-executive board chairman's duties at Deutsche Telekom in 2011. The basis for the empirical analysis is Deutsche Telekom's annual reports 2000–2015 as well as articles in newspapers and press releases from the years 2005–2011. Additionally, publicly available documentation of the law cases at the Landgericht in Bonn has been used as well as documentation from attorneys of the victims and from the defense. References to original sources were used where possible. The subsequent sequestration of material in the course of the state prosecution's investigation, and understandable 'low-key' handling at Deutsche Telekom, made a widely usage of secondary sources necessary (Table 1).

These problems add up to "the problem of collecting empirical data on the computer (in)security phenomena" that "has been examined by a number of disciplines and professions in various countries" (Kowalski 1994, 97). Despite a large amount of data being gathered on attacks, estimates of losses, and infected

Table 1 Secondary sources

Issuer	Title	Author/type	Date (Accessed)
Deutsche Telekom	*Annual Reports 2000–2015*	Annual Report, https://www.telekom.com/investor-relations/publications/Financial-results/204382	2001–2016, Accessed 2 May 2016
Deutsche Telekom	*Data Privacy & Data Security 2009*	Report	2010
Deutsche Telekom	*Streit zwischen Konzern und ehemaligen Organmitgliedern gütlich beigelegt*	Press release	February 1, 2011
Deutsche Telekom	*Data Privacy and Data Security 2014*	Report	February 2015

Table 1 continued

Issuer	Title	Author/type	Date (Accessed)
Deutsche Telekom	*Special Data Privacy and Data Security Measures since 2008*	https://www.telekom.com/corporate-respnsibility/data-protection/	25 August 2015
Der Spiegel	*Projekt 'Clipper'*	Beat Balzli, Jürgen Dahlkamp, Frank Dohmen, Klaus-Peter Kerbusk	22/2008
Der Spiegel	*Did Deutsche Telekom Spy on Journalists and Board Members?*	http://www.spiegel.de/international/business/telecommunications-scandal-did-deutsche-telekom-spy-on-journalists-and-board-members-a-555363-2.html	From the issue 22/2008, Accessed 27 July 2015
Der Spiegel	*Big Brother: Der unheimliche Staatskonzern*	Lead Article Paper Issue	23/2008
Der Spiegel	*Die Dunkle Seite der Macht*	Alexander Neubacher	24/2008
Der Spiegel	*Verdächtiger Fund*	Georg Bönisch, Frank Dohmen, Klaus-Peter Kerbusk, Barbara Schmid	25/2008
Der Spiegel	*Mitten im Feuer*	Interview René Obermann	27, 2008
Der Spiegel	*Die Männer von KS3*	Frank Dohmen, Klaus-Peter Kerbusk	47/2008
Der Spiegel	*Gipfel der Unverfrorenheit*	Jürgen Dahlkamp, Frank Dohmen	51/2009
Frankfurter Allgemeine Zeitung	*Deutsche Bahn überprüfte heimlich 173.000 Mitarbeiter*	http://www.faz.net/aktuell/wirtschaft/unternehmen/datenschutz-deutsche-bahn-ueberpruefte-heimlich-173-000-mitarbeiter-1753575.html	January 28, 2009, Accessed 27 July 2015
Handelsblatt	*Die Deutsche Bahn und die Spione*	Sönke Iwersen, http://www.handelsblatt.com/unternehmen/industrie/spitzelaffaere-die-deutsche-bahn-und-die-spione-seite-2/3169708-2.html	May 5, 2009, Accessed 28 July 2015
Handelsblatt	*Spitzelprozess wirft Fragen zur Rolle Zumwinkels auf*	Sandra Louven	October 6, 2010
Handelsblatt	*Daimler schafft Vorstandsposten für "Integrität und Recht"*	http://www.handelsblatt.com/unternehmen/industrie/kandidat-gesucht-daimler-schafft-vorstandsposten-fuer-integritaet-und-recht/3549528.html	September 28, 2010, Accessed 18 July 2015
Le Monde	*Scandale d'espionnage chez Deutsche Telekom*	Marie de Vergès	May 26, 2008
Le Monde	*Affaire d'espionnage: Deutsche Telekom verse 1,7 million d'euros*	http://www.lemonde.fr/technologies/article/2010/11/16/affaire-d-espionnage-deutsche-telekom-verse-1-7-million-d-euros_1440604_651865.html	November 16, 2010, Accessed 18 July 2015

Table 1 continued

Issuer	Title	Author/type	Date (Accessed)
New York Times	*Phone Giant in Germany Stirs a Furor*	Mark Landler	May 27, 2008
n-tv.de	*Bahn-Vorstand komplett: Abschied von der Ära Mehdorn*	Dpa	May 28, 2009
Rechtsportal.de	*Sentence Dresp Nr. 2013/10453*	http://www.rechtsportal.de/Rechtsprechung/Rechtsprechung/2010/LG-Bonn/Der-Hauptangeklagte-in-der-Spitzelaffaere-bei-der-Deutschen-Telekom-wird-zu-dreieinhalb-Jahren-Haft-verurteilt-In-der-technisch-ordnungsgemaess-und-unter-Bezahlung-des-geschuldeten-Entgelts-hergestellten-Telekommunikationsverbindung-liegt-keine-rechtswidrige-Inanspruchnahme-von-Telekommunikationsnetzen-Der-Abteilungsleiter-der-Telekom-Konzernsicherheit-verstiess-durch-das-Ausspionieren-von-Telefondaten-von-Gewerkschaftern-Journalisten-und-Aufsichtsratsmitgliedern-gegen-das-Fernmeldegeheimnis/%28h%29/1ba962837d798d431d74a52e5495b81c/%28off%29/1	November 30, 2010 Accessed 18 August 2015
SpiegelOnline	*Obermann zum Rapport*	Video: http://www.spiegel.de/video/telekom-affaere-obermann-zum-rapport-video-31142.html	June 2, 2008
SpiegelOnline	*Probe Shows Deutsche Bank Spied on Board Members and Shareholder*	Christoph Pauly, Wolfgang Reuter	June 7, 2009
SpiegelOnline	*Einigung mit der Telekom: Ricke und Zumwinkel zahlen für die Spitzelaffäre*	http://www.spiegel.de/wirtschaft/unternehmen/einigung-mit-der-telekom-ricke-und-zumwinkel-zahlen-fuer-die-spitzelaffaere-a-743001.html	February 1, 2011, Accessed 18 July 2015
Stern	*Bahn bespitzelte eigene Mitarbeiter*	Johannes Rörig, Marcus Gatzke, Florian Güssgen	03/2009
Süddeutsche.de	*Die Späher aus der Schlüterstrasse*	Hans Leyendecker, Caspar Dohmen, Ulrich Schäfer	May 10, 2010
Süddeutsche Zeitung	*Staatsanwalt prüft Ermittlung gegen Telekom Betriebsrat*	Reference Financial.de	June 2, 2008

Table 1 continued

Issuer	Title	Author/type	Date (Accessed)
Wall Street Journal	*Bank Spy Scandal Widens*	David Crawford, Matthew Karnitschnig	August 3, 2009
Wall Street Journal	*ISS's View on Target Directors Is a Signal on Cybersecurity*	Paul Ziobro, Joann S. Lublin	May 28, 2014
Wirtschaftswoche	*Schnüffeln mit Wissen der Chefs*	Wilfried Eckl-Dorna	June 4, 2008
Wirtschaftswoche	*Kein Skandal, aber Vertrauensverlust: Bespitzelung bei der Bahn*	Christian Schlesinger	January 21, 2009
Wirtschaftswoche	*Dossier belasted Zumwinkel in der Telekom-Spitzel-Affäre*	Jürgen Berke, Hans-Peter Canibol	February 13, 2009
Wirtschaftswoche	*Weshalb Ermittler Zumwinkel und Ricke im Visier haben*	Wilfried Eckl-Dorna	March 13, 2009
Wirtschaftswoche	*Aufklärer mit gebremstem Ehrgeiz*	Sandra Louven, Hans-Peter Siebenhaar	February 11, 2010
WiWo	*Verfahren gegen Ricke und Zumwinkel eingestellt*	APN	January 14, 2011
WiWo	*BGH bestätigt Urteil gegen Sicherheitschef*	APN	October 10, 2012

computers, the overall database on the measurement of strategic risks and numerical security decision-making processes, is left without empirical evidence. Therefore, the research methodology to deliver most accurate and conclusive results for qualitative empirical assessment is in-depth content analysis of media sources. The public sphere as primary space, in which problems with their solutions are discussed, and responsibilities as well as competences are contested (Neidhardt 1994), the modern public sphere is largely represented and influenced by the media. These media as structured social space follows specific logics and characteristics (Hilgartner and Bosk 1988). These may include an agenda-setting and gate-keeping function, and assigns news value or issue attention cycles. It is "a site on which various social groups, institutions, and ideologies struggle over the definition and construction of social reality" (Gurevitch and Levy 1985, 19). Media may also partake in the construction of social realities by presenting these realities as legitimate or illegitimate (Lok 2010).

Following the methodology of in-depth content analysis, applicable legal frameworks in the single institutional setting of Deutsche Telekom have been chosen and evaluated in the context of the case and hence limited to Europe and the US.

4 Empirical research: Deutsche Telekom spy case 2005–2011

4.1 Extraction of events related to the case

Deutsche Telekom is one of Europe's largest telecommunications companies with over 200,000 employees worldwide (Forbes 2015). In 2008, the company experienced a high profile scandal with extensive national and international news coverage after its disclosure in 2008 (Spiegel 2008/22, Wirtschaftswoche 2008, Handelsblatt 2008, Manager Magazin 2008, New York Times 2008, Le Monde 2008). The role of the Chairman of the Non-Executive Board from 2003 to 2008 was discussed widely until the official ending of negotiations between him and Deutsche Telekom AG and after his discharge from the non-executive board in 2011 (Deutsche Telekom 2011).

Foundations of the scandal were laid in 2005 and 2006, when a corporate security unit 'KS3' analyzed data available in house on phone connections of members of the non-executive board, other Deutsche Telekom employees, and journalists (Spiegel, 2008/27). After multiple disclosures of strategically important information in newspapers, journalists were suspected to disclose confidential information handed over by an internal source. Finally, board representatives of Deutsche Telekom had been targets of the internal investigation (Wirtschaftswoche 04/05/2008). In 2009, one of the non-executive board members that became victim in the spy case was accused to have leaked strategically critical information to external sources. The prosecution examined a potential investigation for a criminal offense for treason of company secrets (Süddeutsche Zeitung 2008). In February 2010, Deutsche Telekom disclosed a total number of 84 spying actions including 22 persons whose bank accounts had been monitored (Wirtschaftswoche 11/02/2010). This event marks a first violation of security in the here-analyzed case as well as a potential conflict of legal requirements that need to be taken into account by board members.

4.2 Legal aspects of the case

In the course of the scandal, the state prosecution had further collected enough material to justify investigations against the chairman of the non-executive board, not for disclosing information but for supporting the hunt of the mole through illegal means, confiscating material from his office as well as his private home. Concrete accusations throughout the scandal included

– Knowledge and/or delegation of task to identify the fraudulent source (Spiegel 2008/22), in a meeting with the KS 3 security officer (compensation claim

launched by a law firm engaged on behalf of Deutsche Telekom) (Spiegel 2009/51); following an internal report of the law firm Oppenhoff & Partner published in February 2009, the suspicion was raised that the chairman of the non-executive board had given orders himself to investigate the data leakage based on phone connection data (Wirtschaftswoche 13/03/2009);
- Payments from a common account of the CEO and the Non-Executive Chairman to an external company engaged to conduct investigations on behalf of Deutsche Telekom (Spiegel 2008/22; Spiegel 2008/47);
- Change of the 'Geschäftsverteilungsplan'– the organizational chart in December 2005 with the head of KS3 receiving direct orders from the Chairman of the Non-Executive Committee (Spiegel 2008/47; Wirtschaftswoche 13/02/2009).

Due to lack of evidence, the former Chairman of the non-executive board was not accused in front of a court of law or charged. The investigation started with a complaint of an offense by Deutsche Telekom in May 2008 suggesting the Chairman to have possibly ordered, controlled or at least not suspended spying activities (Spiegel 2009/51). The scandal around his role ended with the final report of the prosecution and the Annual Shareholder Meeting in May 2011. Until then, Deutsche Telekom refused to discharge him from his duties on its yearly shareholder meetings in 2009 and 2010 until all charges were dropped in January 2011.

In April 2009, attorneys on behalf of Deutsche Telekom claimed one million Euro of compensation from the former chairman and hence settled a lump sum (Deutsche Telekom 01/02/2011) of EUR 250,000 (SpiegelOnline 2011) with an additional sum being covered by a management insurance. Deutsche Telekom justified its claim for indemnification by saying that the affair only became possible due to mistakes in management (Wiwo, 14/1/2011). This quoted statement demonstrates that the chairman encountered significant challenges in governing the security risk appropriately ensuring a legal handling of the mitigation of the risk.

From Deutsche Telekom, the former head of KS3 was charged among other delicts of breaking the Fernmeldegeheimnis—the secrecy of telecommunications—in seven cases (Rechtsportal 30/11/2010). According to Deutsche Telekom's corporate council at the time and later head of the new Board of Management department Privacy, Legal Affairs and Compliance, he was only admonished internally following the advice of the Chairman of the Non-Executive board (Handelsblatt 06/10/2010).

4.3 Deutsche Telekom non-executive board composition and relevant governance findings from annual reports

Due to the size of the corporation, Deutsche Telekom's non-executive board counts 20 members out of which half are internal and half external members. Due to the company's listing in the US, the Audit Committee holds the responsibility for the under S-OX required internal control system. Thus, the committee should also be the recipient for all risk reports, including strategically significant security risks. In the annual reports before the scandal became public, security was not explicitly

mentioned in the tasks of either of the five existent committees (Deutsche Telekom Annual Report 2000–2007). This changed in 2008, when an additional meeting of the audit committee was established to specifically discuss data security issues. In the following years, this extraordinary fifth annual meeting continued in addition to the ordinary four meetings. In this additional meeting, data security has always been mentioned on the agenda for that meeting (Deutsche Telekom Annual Report 2008–2015).

The analysis further showed that although an additional chair for data security, legal affairs and compliance was created on executive board level, no personal changes were mentioned in relation to responsibilities and expertise on non-executive board level. Until 2015, only one external board member with an IT-industry background joint the non-executive board but did not become a member of the, for information security responsible, audit committee. In 2011, an additional committee for Technology and Innovation was established, however no tasks or responsibilities specific to information security are mentioned (Deutsche Telekom Annual Report 2011).

Other milestones that followed were the certification of Deutsche Telekom headquarters and large parts of its service units according to the ISO 27001 standard (ISO/IEC 27001 2013)—an internationally accepted information security standard requiring the formalization of an Information Security Management System (ISMS). As mentioned in Part 2, an ISMS requires the segregation of duties. The analysis of the annual reports 2006–2015 however shows that the responsibilities of the non-executive board for security have not been changed, neither in the aftermath of the scandal nor through the introduction of the ISMS. Nevertheless, responsibilities for security have been made more apparent with an extraordinary meeting of the audit committee discussing security related issues.

4.4 Aftermaths of the scandal

Deutsche Telekom took a number of relevant governance initiatives in the aftermath of these events (Deutsche Telekom 2015):

- October 2008: Formation of a Board of Management department for Privacy, Legal Affairs and Compliance, the first DAX 30 corporation to do so.
- March 2009: A 10-point program of immediate measures among which an "increased protection of Supervisory Board members—*Supervisory Board members will be better protected from unauthorized internal investigations through a new "consultation procedure." This means that beyond the regularly occurring compliance audits, the Board of Management must consult the responsible Supervisory Board committee before initiating internal investigations" (Deutsche Telekom 2010).*
- Realignment of Group Security and the "double checking" of control structures, with two separate members of the Board of Management responsible for the operative side of security and the supervision/internal guidelines for information security.

- Spring 2009: Publication of the first yearly Data Privacy Report as first corporation in the DAX 30 Group with the objective to facilitate open, transparent communication on data incidents and data privacy measures.
- February 2009: Formation of a Data Privacy Advisory Board with data privacy experts from politics, academia, industry and independent organizations. These as outlined in the annual report from 2009, however only report to the executive board (Deutsche Telekom Annual Report 2009).
- Mid-2010: Introduction of a standard security and data privacy procedure with standardized documents for the German Group companies.
- To recover from the reputational damage, Deutsche Telekom launched multiple programs, e.g., 1.7 million Euro transferred to multiple data privacy organizations in 2010 (Le Monde 16/11/2010).

4.5 Comparison to other cases relating to security governance on non-executive boards

In the years 2000–2010 similar cases in Germany but also the US showed an at least overly lax treatment of security sensitive data (Wirtschaftswoche 4/6/2008; Wall Street Journal 03/08/2009, Spiegel 25/2008), including at companies such as Deutsche Bank AG (Spiegel 7/6/2009), Deutsche Post AG (Wirtschaftswoche 21/1/2009), Lufthansa AG, Deutsche Bahn AG (Wirtschaftswoche 21/1/2009; Handelsblatt 05/05/2009), was uncovered shortly after the Deutsche Telecom scandal. Lufthansa acknowledged to have used data from flight bookings to seek information on an internal informant (Spiegel, 24/2008), which was recognized by the later appointed CEO and defended as an action within legal boundaries (Spiegel 2008/24). Despite several violations of the federal privacy law being found by the German government's commissioner, no criminal charges were raised against Deutsche Bahn (Stern 2009). After an official report by the German Parliament, the Chairman of the Executive Board resigned. In particular Deutsche Bahn, followed the restructuring of governance at Deutsche Telekom by creating an own Board of Management for Privacy, Legal Affairs, Compliance, and Corporate Security., Other DAX 30 companies, such as Daimler AG for example, followed suit (n-tv 28/5/2009; Handelsblatt online 28/9/2010).

While at Deutsche Bank the prosecution could also not charge executive or non-executive board members, the bank faced "a major conflict of interest in the form of supervisory board chairman Clemens Borsig, who shares responsibility for at least some of the snooping operations" (Wall Street Journal 3/8/2009). In his previous role as Chief Financial Officer he was in charge of the corporate security department that had been involved in the spying scandal (SpiegelOnline 7/6/2009). A press release by the non-executive board referencing to a non-public internal report defended the absence of knowledge "The questionable methods used were not authorized by members of the Supervisory Board or the Management Board. We regret what took place. Internal measures have been initiated to prevent similar incidents in the future" (Wall Street Journal 3/8/2009).

5 Legal frameworks on information security responsibilities for non-executive boards in a single institutional setting

The case of Deutsche Telekom is specific as it remained within one legislative system and although the company is involved in a multitude of markets. In addition, Deutsche Telekom as a former state monopoly has been particularly regulated. Its services fall under the "Fernmeldegeheimnis"—secrecy of telecommunications (Telekommunikationsgesetz 2004). For example, Lufthansa, which used flight data of its customers to conduct a similar internal security investigation, could not be accused in a court of law in the same way. And at Deutsche Bahn AG no charges could formally brought to court (FAZ 28/1/2009) despite the fact that a report of the German parliament that claimed several violations of the law. As an exhaustive study of all applicable laws in information security would go beyond the scope of this study. For different institutional settings already provided (e.g., Schwarz et al. 2014), a comprehensive overview of the given institutional setting is presented to discuss non-executive board responsibilities and emphasize the necessity of their reassessment according to that setting.

From a legal perspective critical issues encompass the protection of critical infrastructures, compliance to data privacy and the integrity of financial data.[1] Legal responsibilities of non-executive boards include identifying applicable laws, which, if broken, would present a strategic risk to the company, as well as those laws that require direct or indirect action by the non-executive board or laws that enshrine an implicit meaning in addition to its explicit address.

Despite its strong reputation and high importance to large parts of the German population due to historical reasons, the German Privacy Law only foresees penalties up to EUR 300,000 or, if proven, to be used for profit, equal to the obtained monetary advantage of the fraudster. If unjust enrichment can be proven, an additional forfeit of up to 2 years in prison can be imposed (Bundesdatenschutzgesetz § 43/44). The risk of violating the law for a company of the size of Deutsche Telekom AG can hence be considered to be rather reputational than financial.

From a legal perspective the scandals around providing incorrect financial data to shareholders e.g., Enron in 2001 (Petrick and Scherer 2003) can be considered more important for non-executive boards. The US answer was the subsequent development and introduction of the Sarbanes–Oxley-Act (2002) for companies listed in the US (which was the case at Deutsche Telekom at the time). It required a statement of "responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting." (Sarbanes–Oxley Act 2002). In 2006, the 8th EU Company Law Directive (European Union 2006) passed European institutions to be adapted in the following years by all EU countries. The requirements for establishing internal control systems to implement risk management controls for early warning on

[1] Health and Safety regulations are not included, since security research acknowledges a clear difference.

substantial risk were translated e.g., in Germany into the Aktiengesetz (2008). A violation of these duties may lead to a delisting and hence presents a major risk if the integrity of data is not ensured. The law requires correct data and also transparency of risks for shareholders.

The law further requires non-executive boards to control whether the executive board has taken all necessary measures to counteract substantial risks and hence non-executive boards can also ask to improve these. The non-executive board is held liable if it supervises poorly whether the executive board performs adequate risk management (Aktiengesetz §§116, 93). Here the non-executive board transforms into a risk management role that ensures all necessary measures have been executed. From an auditor perspective this often goes hand in hand with identifying necessary measures to improve the internal control system, however in the context of this paper an emphasis shall be given that the two tasks given by law to the non-executive board encompass different intentions. One is to create transparency through an internal control system and the second is to ensure that security risks are managed efficiently.

6 Discussion

In the center of the present research is the structural conflict of interest concentrating on non-executive board level regarding investor legal requests for transparency on information security risk and investors' individual risk disposition regarding the management of information security risks (Fig. 1).

In a first step, it is important to analyze the context of the case study in terms of legal responsibilities of the non-executive board. The board needed to be informed about the strategic risk arising from confidential data leaking to the press, causing competitive damage to the company, which in itself is subject to legal prosecution. One of the most important ways of implementing strategic control by the non-executive board is to know criticalities. In its supervisory function the board, or more concrete in this case the audit committee, needed to be informed of those risks which are considered strategic for the business following the definition of the e.g., Aktiengesetz. In the case of Deutsche Telekom, the information security reporting

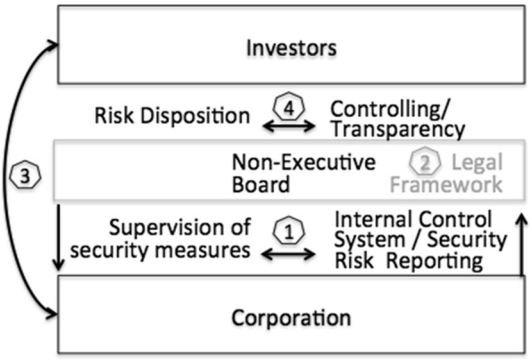

Fig. 1 Security governance issues in non-executive boards

was incomplete. The source for the data leakage was unknown, and the board and in particular the audit committee that was assigned with supervising the security management, was not properly informed on the activities of the security unit. This incomplete reporting information could also be observed in the other mentioned scandals in the years 2000–2010. Coming back to Lippert et al's theory that information security companies tend to prohibit conduct they deem harmful to their profit accumulation but may not be deemed illegal (Lippert et al. 2013). Here shareholder representatives have an interest to optimize profits and have at the same time an interest to prevent the company from any damage. Analyzing the case of Deutsche Telekom, the chairman of the non-executive board was acting to mitigate strategic risk caused through information leakage. In this specific situation as this leakage being suspected to take place within the non-executive board, he took charge to become not only the recipient of information in this regard but also to facilitate finding a solution. His assumed unawareness of countermeasures demonstrates lack of control or knowledge of the measures taken, despite being involved in concrete activities. During investigations of the prosecution his attorneys defended him by denying that he had any know-how of actions taken to resolve the security leakage risk. In terms of liability to ensure the efficiency of actions taken, this is an important statement, which demonstrates the conflict of 'command and control' in this case. As chairman of the non-executive board, he should have been aware of the activities involved in mitigating the risk of strategic data leakage. Deutsche Telekom taking the path of full transparency on security and privacy actions as aftermaths of the case by establishing two separated reporting lines up to executive board level, worked on governance structures of security information provision. The events that led to one of Deutsche Telekom's employees being convicted because of a violation of the telecommunications secrecy law should not have been possible to go unnoticed to the management and further the non-executive board. Lack of transparency in actions of the security unit was a failure in risk reporting.

In a second step, we go deeper into the analysis of perceived legal boundaries. None of the actors on non-executive board level had been accused to have acted out of personal interest, neither to disclose data nor to apply unlawful means to find the leak. On the contrary, all action was performed by the board members putting rather their own reputation and credibility at risk. Even if no legal obligation would have been violated the awareness on non-executive board level for potential scandals based on an investigation on an information security leak must have been perceived by its members to have been low. It must have been unawareness of a corporate unit potentially surpassing the law and hence damaging the company financially and in its reputation. The media scandal following the unlawful actions created new social reality and pressure that made the former non-executive board chairmen of Deutsche Telekom pay compensation to Deutsche Telekom despite him being already cleared at that time from all accusations in front of the law. Lok's theory used as research methodology is hence validated of media creating social reality may it be legal or illegal (Lok 2010).

In a third step, the case also shows the successful application of Zajac and Westphal's theory that security interests may differ from and conflict with investor logic and corporate logic (Zajac and Westphal 2004). In the case of Deutsche Telekom the non-executive board included union representatives as well as shareholder representatives. Interestingly enough, during the scandal both parties were accused to have violated the law—one party by disclosing strategic information to potentially protect corporate interests, the other taking unlawful measures to avoid that, protecting investor interests. Both parties were not charged, however the situation of data leakage on the one side and the illegal usage of telecommunication data, demonstrate that the security risk governance was not properly conducted at the time causing damage in form of loss of reputation, unplanned investments etc. to the company. The shown differences in motivation contribute to Zajac and Westphal's theory by extending the theory to information security management. Conflicts of interests in the role of non-executive board members would be either corporate, thus acting as strategic advisor on information security to the executive board or investor related, thus monitoring risk management of the executive board.

In a fourth step, shareholders owning the company have direct interest in executing but also managing the mitigation of that risk as required by law and standards. Good corporate governance, such as strong control over data security as well as steering of security measures must be ensured up to non-executive board level. Whereas in executive boards, as was the case at Deutsche Telekom, the split of the two responsibilities, control and execution, were introduced through a new board of management, this split has so far not been introduced neither in governance frameworks for non-executive board nor is it part of corporate governance research.

In the combination of having either not the correct information on the security measures deployed or tolerating these, both aspects show a potential jurisdictional and societal conflict. This conflict generates corporate governance issue that could have been actively avoided with the awareness of legal responsibilities. In view of the former Vice-Chairman of the Non-Executive Board who first fell victim of the spy case and later became a prosecutor in the law suit, he declared through his attorneys that missing data security is encouragement to abuse economic power (Däubler-Gmelin 2011). The contribution of this paper to corporate governance research is the enlargement of scope to information security being a topic that non-executive boards need to decide on governance structures and create awareness amongst their non-executive board members regarding legal obligations. Yatim suggested further research on the independence of risk management committees and their interaction with the audit committee and strategy development (Yatim 2010). My research shows that a clear separation of duties among members and/or committees is necessary to be enforced also on non-executive board level to avoid a structural conflict of interest. Such a separation is necessary in view of the increasing number of legal requirements in security but also to protect shareholders as well as the company from an accumulation of competences that, given the raising criticality of information security, bears a risk that can be avoided through better governance.

7 Future developments of information security with implications on board governance

To cope with the importance of the topic, the tightening regulatory rules in information security management, as well as the developments in handling information security risks have to be considered.

Looking at current developments in the regulatory field in Europe and the US, legal obligations are in the course of being implemented to integrate best practice security as well as set up reporting structures asking for sharing information on security incidents. But certain specifications are still left open to be discussed in industry. The development in Asia, the Monetary Authority of Singapore (MAS) requires, as part of its Regulatory and Supervisory Framework (Monetary Authority of Singapore 2013b), the management of Technology Risks to provide a notification. "The Notice on Technology Risk Management ('the Notice') requires financial institutions to notify MAS as soon as possible, but not later than 1 h, upon the discovery of a Relevant Incident" (Monetary Authority of Singapore 2014). Also the authority provides clear guidelines on the role of the Non-Executive Board. "The Board and senior management should be actively involved in the formulation and review of the institution's stress testing programs. The stress testing programs should be forward-looking and commensurate with the institution's risk profile. It should adopt suitably severe assumptions and seek to address feedback effects and system-wide interaction between risks. The results of the stress testing program should be integrated into its decision-making, risk management processes (including contingency arrangements) and the assessment of its capital and liquidity levels." (Monetary Authority of Singapore 2013a) Regulatory requirements in the US and Europe move in a similar direction as the ones MAS provides in Asia. Board functions should therefore gain sufficient in- and oversight in corporation's security incident processes to avoid sanctions. For the future, attention shall also be drawn to two new EU directives harmonizing legislation in Europe in the area of information security and privacy. Both will add to creating assurance and boundaries for organizations to deploy information security measures lawfully but also increase their competences in protecting their assets. In Germany the so called IT-Security Law—Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme—was enforced on July 17, 2015 and requires companies that are part of critical infrastructures to report security incidents and establish a security baseline (Bundestag 2015). Overarching for Europe, the EU-directive on Network and Information Security (NIS) has been adopted by the European Parliament in 2014. It is currently discussed in the European Council (European Commission 2013) focusing on standards in particular for critical infrastructures. Furthermore, the EU Directive for Data Protection is currently under revision and has been adopted by the European Parliament in 2012 including an increased level of data protection requirements strengthening in particular European customer rights (European Council 2012). These two European laws, if passed, will increase trans- territorial legal responsibilities within companies and hence their required transparency on security incidents beyond enterprise boundaries. They generally increase the

legislative requirements for companies in security and thus for non-executive boards the task to supervise their enforcement as well as being informed on relevant risks.

A second important concern is the placement of responsibility within the non-executive boards given new developments in the security sector that show increasing potential for legal conflicts. Industry and also governments move increasingly into the arena of proactive cyber defense mechanisms. These defense mechanisms are built upon classic war theory, such as those of Sun Tzu, The Art of War (Tzu 1994). They comprise classical methods of gathering counterintelligence, preparation of disabling attack vectors and execution. Examples of such activities can be a proactive monitoring of IT security (Deutsche Telekom 2014) or—quite different in terms of consequences—a largely coordinated Counter Attack against central host computers of botnets that hijack and infiltrate devices in their network of organizations, performed e.g., by the Dutch Police in 2010 taking a total of 143 servers offline that managed 30 million hijacked computers (MELANI 2011). Disabling such central computers frees up these hijacked resources and destroys the attackers infrastructure to launch new attacks. Obviously, using such mechanisms is a highly sensitive topic when it comes to who is allowed what, due to what evidence and up to what extent. As general principles on government level, the principles of necessity as well as proportionality have been deployed (Hathaway et al. 2012). However, a possible scenario mentioned negatively in an interview for this study is that a hijacked computer might shut down, after its host was destroyed, in a proactive counter attack. But what if this computer is a lung ventilator in a hospital—in such a case who bears the consequences of actions?

Prosecution of attackers has been a major issue so far, in particular if these are hiding in the internet's no man's land, making it almost impossible to locate them in one specific country. Today, states but also industry networks, particularly encouraged by public authorities, if part of critical infrastructures, discuss the options to actively defend their networks. The discussion of applicable laws in cyber warfare, cyber attacks and cybercrime leaves authors of an article on the Law of Cyber-Attack with the statement that "Cyber-attacks on vital infrastructure are already becoming widespread. […] And yet, while the threat of cyber-attacks has rapidly grown, the response has not kept pace. The article has shown that both the U.S. government and the international community at large have thus far largely failed to update the legal framework for responding to cyber-attacks." (Hathaway et al. 2012) This leaves states, industries, and companies with a range of options to change strategy and potentially affectivity by turning towards active defense mechanism. Nevertheless, a number of laws have been brought forward to regulate the appropriateness of responses. While these are mostly trying to regulate cyber space from a government perspective, insecurity exists of who may be lawfully allowed to carry out a cyber attack in industry. For example the US Department of Defense strategy emphasizes partnering with private sector to encourage innovation, incremental improvements, and workforce development (DoD Strategy Department of Defense 2011). The appropriateness of actions and the jurisdictional basis for launching a counterattack on industry are not yet sufficiently defined and bear legal insecurity towards future prosecution and legal responsibilities.

8 Further research problems in information security governance

The first problem is testing governance solutions that avoid the here described conflict of interest in security on non-executive board level. Calls for finding new solutions try to analyze the current unsatisfying situation of a lack of best practices on role management in the board. Commissioner Luis A. Aguilar, from the United States Securities and Exchange Commission, stated that the establishment of risk committees and educating board members in the area of cyber security "is good business practice, it is not necessarily a panacea to comprehensive cyber security oversight." (Aguilar 2014) The effectiveness of such measures in role management and board responsibility is important to be analyzed.

A second problem relates to non-executive boards and their capability to perform tasks that the regulator has given them. Following Zaman's argumentation on lack of awareness and expertise in audit committee's for detailed understanding of operational risks, this is another field of potential legal conflict in the realm of non-executive boards that would need further investigation (Zaman 2001). The board size, analyzed as general determining factor (di Pietra et al. 2008), could be critical in this particular context. The degree of understanding for information security related strategic risks has so far not been sufficiently investigated through research. In non-executive boards this expertise can be externally provided. However, ultimate accountability will remain with the non-executive board function and should therefore be sufficiently enough represented through expertise in the area in non-executive boards.

Deutsche Telekom's Data Privacy Report from 2014 emphasizes that many businesses still think of "IT security as an expense, not as an investment, […] despite the soaring financial damage caused by cybercrime and online espionage. Many only acknowledge the risks when it's too late—shutting the stable door after the horse has bolted." (Deutsche Telekom 2014) This error should be avoided in corporate governance research.

References

Aguilar, L. A. (2014). Board of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Cyber Risks and the Boardroom Conference, New York Stock Exchange. http://www.sec.gov/News/Speech/Detail/Speech/1370542057946. Accessed 15 July 2015.

Ahrens, T., Filatotchev, I., & Thomsen, S. (2011). The research frontier in corporate governance. *Journal of Management and Governance,*. doi:10.1007/s10997-009-9115-8.

Aktiengesetz (AktG). 1965, revised last 2015, BGBI. I S. 1089.

Bailey, P. (2013). Boardroom strategic decision-making style: Understanding the antecedents. *Corporate Governance: An International Review, 21*(2), 131–146.

BDO. (2014). 2014 BDO Board Survey. https://www.bdo.com/getattachment/84604876-6221-4873-bfea-ca984ff65702/attachment.aspx.

Bundesdatenschutzgesetz (BDSG). (1990, revised 2009), BGBI. I, 2254.

Bundestag. (2015). Gesetz zur Erhöhung der Sicherheit informationstechnischer System (IT-Sicherheits-gesetz), Bundesanzeiger.

Christiansen, C. A., & Westervelt, R. (2015). Security in the 3rd platform: Marching toward proactive defense. IDC Research, 6.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2014). *Enterprise risk management—Integrated framework*. New York: AICPA.

Crombie, N. (2011). A discourse analysis of corporate governance texts. University of Canterbury, http://www.academia.edu/7207626/2011_-_Crombie_-_A_Discourse_Analysis_of_Corporate_Governance_Texts. Accessed 13 Aug 2015.

Däubler-Gmelin, H., Merzhäuser, M., Rothbauer, H., Baum, G., Reiter, J., & Methner, O. (2011). Bericht der Anwälte. 51.

Department of Defense. (2011). DoD Strategy. Supra note 14, at 10–11.

Di Pietra, R., Grambovas, C. A., Raonic, I., & Riccaboni, A. (2008). The effects of board size and 'busy' directors on the market value of Italian companies. *Journal of Management and Governance, 12*(1), 73–91.

European Commission. (2013). *Proposal for Directive to secure a high common level of network and information security across the Union*. COM 48.

European Council. (2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

European Union. (2006). *8th Company Law Directive*, Directive 2006/43/EC.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management and Computer Security, 2*(11), 74–83.

Georg, L. (2007). The function of corporate security within large organization: The interrelationship between Information security and business strategy. https://archive-ouverte.unige.ch/files/downloads/461/unige_461_thesis.pdf. Accessed 25 Sept 2015.

Gurevitch, M., & Levy, M. R. (Eds.). (1985). *Mass communication review yearbook*. Beverly Hills: Sage.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., et al. (2012). The law of cyber-attack. *California Law Review, 100*(4), 817–886.

Hilb, M. (2011). Redesigning corporate governance: Lessons learnt from the global financial crisis. *Journal of Management and Governance, 15*(4), 533–538.

Hilgartner, S., & Bosk, C. L. (1988). The rise and fall of social problems: A public arena model. *American Journal of Sociology, 94*(7), 53–78.

Huse, M., Hoskisson, R., Zattoni, A., & Viganò, R. (2011). New perspectives on board research: Changing the research agenda. *Journal of Management and Governance, 15*(1), 5–28.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements*, Geneva.

Johnsten, L., & Shearing, C. (2003). *Governing security: Explorations in policing and justice* (pp. 281–297). New York: Routhledge.

Kowalski, S. (1994). *Do computer security models model computer crime*. Stockholm: Royal Institute of Technology.

Lippert, R. K., Walby, K., & Steckle, R. (2013). Multiplicities of corporate security: Identifying emerging types, trends and issues. *Security Journal, 26*, 206–221.

Lok, J. (2010). Institutional logics as identity projects. *Academy of Management Journal, 53*(6), 1305–1335.

Martin, J. (1973). *Security, accuracy, and privacy in computer systems.* New Jersey: Englewood Cliffs: Prentice-Hall.

McAfee. (2014). *Net Losses: Estimating the Global Cost of Cybercrime*. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf. Accessed on 17 May 2015.

McCarthy, J. (1995). *Memorandum to P. M. Morse Proposing Time Sharing,* Stanford University. http://www-formal.stanford.edu/jmc/history/timesharing-memo/timesharing-memo.html. Accessed on 29 Sept 2015.

Melde- und Analysestelle Informationssicherung (MELANI). (2011). *Informationssicherung: Lage in der Schweiz und international.* Halbjahresbericht 2010/II, 45.

Monetary Authority of Singapore. (2013a). *Guidelines on Risk Management Practices—Board and Senior Management*. http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Board%20and%20Senior%20Mgmt_1%20Apr%25MAS.

Monetary Authority of Singapore. (2013b). *Technology Risk Management Guidelines*. http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%25Tsu:.

Monetary Authority of Singapore, *Instructions on Incident Notification and Reporting to MAS*. http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Technology-Risk.aspx . Accessed on 12 June 2015.

Neidhardt, F. (1994). Öffentlichkeit, öffentliche Meinung, soziale Bewegungen. *Kölner Zeitschrift für Soziologie und Sozial-Psychologie, 34*, 7–41.

Petrick, J. A., & Scherer, R. F. (2003). The Enron scandal and the neglect of management integrity capacity. *American Journal of Business, 18*(1), 37–50.

PriceWaterhouseCoopers. (2015). *Leading in extraordinary times, The 2015 US CEO Survey, in CEOs' words*. 1–30.

Rainer, R. K., Marshall, T. E., Knapp, K. J., & Montgomery, G. H. (2007). Do information security professionals and business managers view information security issues differently? *Information Systems Security, 16*, 100–108.

Sarbanes-Oxley-Act (SOX). (2002). *Public Law No. 107–204*. Washington, DC: GPO.

Schwarz, D., Ferrillo, P., & Gotshal, W. (2014). Cyber Security and Cyber Governance: Federal Regulation and Oversight—Today and Tomorrow. *Harvard Law School Forum on Corporate Governance and Financial Regulation*, September 10.

Shleifer, A., & Vishny, R. W. (1997). A survey of corporate governance. *The Journal of Finance, 52*(2), 737–783.

Siponen, M. T. (2001). An analysis of the recent IS security development approaches: Descriptive and prescriptive implications. In G. Dhillon (Eds.), Information security management: Global challenges in the New Millennium (pp. 101–123). Idea Group Publication, Hershey

Telekommunikationsgesetz (TKG). (2004). BGBI. I S. 1190.

Tzu, S. (1994). *The art of war*. Barnes & Noble.

Turnbull Report. (1999). *Internal control: Guidance for directors on the combines code,* Institute of Chartered Accountants in England and Wales.

Yatim, P. (2010). Board structures and the establishment of a risk management committee by Malaysian listed firms. *Journal of Management and Governance, 14*(1), 17–36.

Zajac, E. J., & Westphal, J. D. (2004). The social construction of market value: Institutionalization and learning perspectives on stock market reactions. *American Sociological Review, 69*(3), 433–457.

Zaman, M. (2001). Turnbull, generating undue expectations of the corporate governance role of audit committees. *Managerial Auditing Journal, 16*(1), 5–9.

Laura Georg is Associate Professor and Head of the Norwegian Information Security Laboratory with over 50 affiliated staff. The institute is part of the Norwegian University of Science and Technology NTNU. Laura's research contributes to the Information Security Management Research Group focusing on economic and socio-technical aspects of Information Security. She holds three Master of Science degrees from Germany and France. She received her Ph.D. with high distinction from the University of Geneva. During her PhD she visited the London School of Economics' Information Systems Department as Research Student in 2006. From 2007 to 2015 she worked in management consulting advising corporations operating in Switzerland and internationally, on information security strategy and governance issues.