Corporate management boards' information security orientation: an analysis of cybersecurity incidents in DAX 30 companies

L Georg-Schaffner, Enrico Prinz

GEORG SCHAFFNER, Laura et PRINZ, Enrico, 2021. Corporate management boards' information security orientation: an analysis of cybersecurity incidents in DAX 30 companies. Journal of Management and Governance. 19 juin 2021. DOI 10.1007/s10997-021-09588-4.

Corporate Management Boards' Information Security Orientation: An Analysis of Cybersecurity Incidents in DAX 30 Companies

Our study analyzes the impact of cybersecurity incidents (CSIs) at executive level in German blue-chip companies between 2005 and 2018. Using Upper Echelons Theory, we examine the effect of CSIs on both the composition of management boards as well as their members' profiles and related responsibilities, performing a qualitative in-depth analysis of the positive cases found. Our results show that while CSIs are a common problem for large German groups, only a few of them address IT-related incidents directly through governance. Firms that reacted strongly went against the general trend, and either added a new functional unit to the management board or strengthened functions related to the issue. Our findings indicate that German blue-chip companies have not yet devised a common strategy to deal with CSIs. Firms that reshape their management boards instead tend to take a more compliance-oriented approach.

Keywords: Security Management, Cybersecurity Incidents, Management Boards, Germany

If war is too important to leave to the generals, the deployment of information technology is far too important, in 1988, to be left to information technologists (John F. Rockart, 1988, p. 60)

1. Introduction

Cybersecurity incidents (hereafter CSIs) pose a considerable threat to economies and appear to concern all businesses. According to a report by McAfee (2020), in a survey of 1,500 organizations from seven countries (G7 member states excluding Italy but including Australia) only 4% claimed to have experienced no CSIs in 2019. When financial and non-financial damage is taken into account, cybercrime-related costs almost doubled between 2018 and 2020 to exceed $1 trillion (McAfee, 2020). Other sources suggest that the total is expected to reach $6 trillion in 2021, representing the "greatest transfer of economic wealth in history [... which] will be more profitable than the global trade of all major illegal drugs combined" (Cybersecurity Ventures, 2018). On a technical level, however, firms frequently lack effective CSI detection and defense mechanisms, with the result that only every second attack (53%) is detected by internal IT systems (Kutscher, 2017) and only after an average of 99 days (Kasperski, 2016). As a result CSIs continue to cause serious problems illustrated by the steady increase in both the number of sensitive data records and the severity of IT breaches (Risk Based Security, 2021). While the risk to critical IT infrastructure from CSIs is global, the economic impact varies from country to country. According to a McAfee report (2014), referred to in a review of the European Union Agency for Cybersecurity (ENISA, 2016), cybercrime costs when measured as the ratio of a country's GDP, are higher in the U.S. (0.64%) and China (0.63%) than in the EU (0.41%), with some members considerably exceeding the EU and the global average, including Germany (1.6%).

Whereas small and medium-sized enterprises often struggle to create an IT security baseline, larger firms and multinationals are expected to have both the financial resources and the governance structures to respond and adapt to the challenges of CSIs. Although full IT security appears to be unachievable even in large companies, we might assume that firms learn from past incidents, especially when obliged to publicly disclose the significant effects recorded to their stakeholders. However, there is little in the academic literature on the outcomes of post-CSI learning processes. Kvochko and Pant (2015) point to the fact that, due to a lack of data on CSI experiences, related learning outcomes appear to be ignored by the stock market. Likewise, Masli et al. (2016, p. 687) argue that while "scholarly and practice literature both stress the importance of senior executive engagement with IT management, the recommendations for doing so remain, at best, limited and general". The fact that most of the companies surveyed by McAfee (2020) in their latest report do not have plans or solutions to respond to CSIs appears to confirm this observation.

While several scholars have examined the engagement of executives in the management of IT-related activities over the last three decades (e.g., Jarvenpaa and Ives 1991; Purvis et al. 2001; Sharma and Yetton 2003; Kearns and Sabherwal 2007; Liang et al. 2007) little attention has been paid to the

governance aspects concerning executives in firms that experienced CSIs. Masli et al. (2016) sought to fill this gap by analyzing the likelihood of CEO/CFO turnover in U.S. firms that report IT material weaknesses. According to these authors, senior executive turnover appears to be determined by the type of IT deficiency, with CEO turnover affected by issues related to global IT management responsibilities, and CFO departures by problems related to internal IT control. Studying the S-OX 404 reports of U.S. firms, Haislip et al. (2016) also found higher levels of CEO/CFO turnover in cases of IT-related material weaknesses, as well as a shift towards greater IT expertise to redress negative CSI effects. Li et al. (2019) confirmed that internal control material weaknesses are associated with both higher CEO and CFO turnover, but only observed remediation measures once the CEO had left the company. Likewise, Banker and Feng (2019) confirmed higher CSI-related turnover of CEOs and CIOs in U.S. firms, with the exception of CFOs who do not appear to be held accountable for such incidents. Several authors who focused on individual expertise with respect to IT infrastructures, further emphasize the positive impact of CEO IT expertise (Haislip et al., 2017; Haislip and Richardson, 2018), board IT expertise (Vincent et al., 2019) and the active engagement of board committees in IT risk management (Higgs et al., 2016; Smith et al., 2019) with respect to the likelihood of CSIs occurring and the related costs.

While these recent studies analyzed multiple governance issues dealing with CSIs, they mainly focused on U.S. firms. To our knowledge, no analysis of European samples exists to date. This is particularly surprising as European economies appear to be affected by CSIs at least as much as other regions. In fact, when considering certain aspects such as cybercrime costs expressed as a percentage of a nation's GDP some European countries, namely the Netherlands, Norway and Germany, figure in the upper section of international comparisons (ENISA, 2016). An analysis of their economies with respect to CSIs, therefore, appears justified. With regard to these three countries, an in-depth analysis of CSIs in German companies seems particularly interesting. First, Germany is the leading European economy and the world's fourth-largest industrial nation in terms of GDP (Worldbank, 2019). Given the size of Germany's economy and its strong ties to other economies in Europe, the extent of CSIs and their cost is expected to be considerable. Estimating the country's annual cybercrime cost to exceed $64 billion, McAfee (2020) even considered Germany to be the "most developed criminal underground in the EU". Second, German firms (unless listed on a U.S. stock exchange) do not underlay the obligation for fulfilling S-OX, notably SEC requirements, as both national and European legislation had less formalized requirements regarding IT risk reporting, at least until 2019.[1] Consequently, we may expect different governance outcomes as a result of CSIs. Finally, Germany's two-tier governance system noticeably differs from the Anglo-Saxon system in that listed companies are run by a management board (*Vorstand*) in charge of operational affairs, which is separate from the supervisory board (*Aufsichtsrat*) responsible for monitoring the management team and offering advice on the firm's long-term strategic orientation (German Stock Corporation Act, §§76-117). While one-tier board systems permit internal executives to sit on or even to head (in the case of CEO duality) the board of directors, this configuration is prohibited in Germany. Hence, internal executives do not have a direct impact on the efficiency of the monitoring instance but are in charge of the day-to-day implementation of the supervisory board's strategic decisions. This last point is particularly interesting as U.S. studies on the effects of governance on CSIs usually focus their analysis on the board of directors and senior executives (CEO, CFO, CIO, etc.), but rarely consider the composition, profiles and related responsibilities of the whole management team. An analysis of the latter, however, when run under a two-tier board structure, extends the focus beyond key (senior) executives. This enlarged perspective may contribute to a better understanding of the effects of IT-related incidents on aspects of governance, notably whether a change in the scope of responsibilities or the appointment of new top executives following a CSI will lead to a more efficient management team with respect to IT risk management.

The aim of our study is to analyze the effects of IT-related incidents disclosed by firms at their executive level. Following Upper Echelons Theory (Hambrick and Mason, 1984), an organization's

[1] In 2019, the European Securities and Monetary Authority (ESMA) published new guidelines on risk reporting that obligate publicly listed European companies to report material risks, including cyber risk. That said, these requirements remain less comprehensive than those requested in the Security and Exchange Commission's Statement and Guidance on Public Company Cybersecurity Disclosures (2011 and 2018).

outcome is said to be determined by the characteristics of the decision-makers among other things. Consequently, top management team variables, such as composition, profiles, and responsibilities are expected to determine a firm's performance, the latter being seen as the outcome of the decision-makers' individual cognitive biases, values and personality traits. We assume that this can also apply to how top management teams deal with cybersecurity issues. Accordingly, our research question addresses how far CSIs impact on the composition of management boards as well as the profiles and responsibilities of their members. Deploying Upper Echelons Theory, we focused on the characteristics of the management boards of firms that have experienced significant CSIs. Our analysis is based on a sample of 43 German companies listed on the country's Dax 30 blue-chip index between 2005 and 2018, which we examined for CSIs that were experienced and disclosed. Due to the absence of CSI databases in Germany, we ran an in-depth content analysis of the CSIs identified by gathering information from websites, corporate documentation and other communication sources. In addition, we collected data on the companies' top management teams from which we quantitatively analyzed the characteristics through variables related to the management board itself and the demography and education of the members. We further qualitatively analyzed any changes in the management boards' composition and the scope of the managers' responsibilities regarding cybersecurity in the years following a CSI. That said, the professional experience of IT executives, as examined in U.S. firms by Lim et al. (2013) or Haislip et al. (2016, 2018), could not be included in our study as data on these aspects was incomplete or unavailable.

The remainder of our paper is organized as follows. Part 2 looks at the underlying theoretical assumptions that explain the factors determining any changes in the composition of top management teams, with a focus on the cybersecurity-related literature. Part 3 describes our data and presents the methodology adopted. Part 4 presents the main results of our analysis, while part 5 interprets the findings in the light of the literature and offers a critical discussion. Part 6 presents the conclusion, and part 7 addresses the limitations of our analysis and suggests avenues for further research.

2. Upper Echelons Theory, Top Management Teams and Cybersecurity Incidents

2.1 Upper Echelons Theory and top management team composition

Upper Echelons Theory (Hambrick and Mason, 1984) states that an organization's performance is partially determined by the characteristics of its decision-makers. Consequently, the composition of top management teams is assumed to play a decisive role in a firm's strategic policies and outcomes. Given the assumption of bounded rationality (March and Simon, 1958; Cyert and March, 1963) according to which informationally complex and uncertain situations are not objectively "knowable" but are merely interpretable (Hambrick and Snow, 1977; Mischel, 1977), the theory's basic premise is that "organizational outcomes [...] are viewed as reflections of the values and cognitive biases of powerful actors in the organization" (Hambrick and Mason, 1984, p. 193). In other words, it is the top manager's individual cognitive biases, values and personality traits that shape their perceptions and interpretations of situations and thus determine their behavior and strategic choices. Given how hard it is to collect psychometric data on managers, Hambrick and Mason (1984, p. 198) suggest using observable background characteristics, such as age, professional background, education, socioeconomic roots and group characteristics, as proxies to explain (at least partially) organizational outcomes. In our analysis, we focused on observable variables of the categories of age, formal education, career experiences other than functional track and group characteristics.

Initially developed in the 1980s and widely disseminated in recent decades, Upper Echelons Theory includes several conceptual and methodological weaknesses (Hambrick, 2007; Abatecola and Cristofaro, 2018; Neely et al., 2020). Both top managers' cognition processes and their interactions are thus often seen as a black box, although some progress has been made with respect to methodological techniques. Likewise, we can criticize the lack of evidence regarding the sense of causality between managerial background characteristics and strategic outcomes, as well as the still unclear role of contingencies and moderating conditions such as culture and diversity. The widespread use of

(aggregated) proxy variables causes further incongruities between theoretical constructs and empirical measures. Issues of endogeneity are also worth examining, since managerial decision-making observed may mirror the board of directors' expectations rather than the characteristics of individual executives. Finally, and more fundamentally, the issue of the role of the company's performance that managers can themselves effectively determine continues to generate ongoing academic debate.

Following Upper Echelons Theory, background characteristics of top executives are seen as a proxy for their socio-cognitive diversity, skills and socio-professional ties (Finkelstein and Hambrick, 1996) whose combination is assumed to shape a firm's strategic direction and performance (Michel and Hambrick, 1992; Carpenter and Fredrickson, 2001; Dezsö and Ross, 2012). Scholars apply this theory in multiple ways by mainly focusing on senior executive characteristics like education, experience and personality traits (for an overview see Wang et al., 2016). Studying the banking industry in the U.S., Bantel and Jackson (1989) demonstrated more than three decades ago that the educational level of top management teams is a key factor in a firm's capacity to innovate. In line with these findings, Wiersema and Bantel (1992) observed a positive link between the educational level of top management teams and their propensity for strategic change. Likewise, Wally and Baum (1994) found a positive link between top executives' cognitive skills and their decision-making speed. Over time, scholars have shifted their focus from specific background characteristics to a more general analysis of the composition of top management teams, as well as the diversity of the background characteristics of their members (for reviews see Certo et al., 2006; Abatecola et al., 2013). Auden et al. (2006) observed that age homogeneity among top executives stimulates firm performance as does the heterogeneity of a top management team's functional background, the latter also determining a positive performance effect of team tenure. Naranjo-Gil et al. (2008) confirmed these findings, showing that top executives' heterogeneity, when measured by a team's diversity relative to tenure, functional and educational background, moderates the impact of strategic change on operational performance. In addition, executives' personality traits and expertise are also considered to determine strategic outcomes (Bertrand and Schoar, 2003; Bédard et al., 2004; Ge et al., 2011; Winkler et al., 2020). Consequently Qu (2020) shows that characteristics, such as managers' personality (Hurtz and Donovan, 2000), self-perception (Judge et al., 1998), ethical beliefs (Koh and Boo, 2001) and childhood experience (Blustein et al., 1991) determine not only observable aspects, but also a firm's likelihood of financial misstatements.

2.2 Top management teams and cybersecurity incidents

While several scholars have examined executives' engagement in the management of IT-related activities over the last three decades (e.g., Jarvenpaa and Ives 1991; Purvis et al. 2001; Sharma and Yetton 2003; Kearns and Sabherwal 2007; Liang et al. 2007), little attention has been paid to specific governance aspects of the executives in companies that have experienced CSIs. The presumed impact of top management teams' background characteristics on organizational outcomes, however, also applies to CSIs. Accordingly, IT expertise of top executives, as well as their educational and functional background in this area are considered to have an impact on firm performance. On the one hand, when top managers have a higher level of IT expertise (Haislip et al., 2017; Vincent et al., 2019) and there is a comprehensive anchorage of IT issues in a firm's decision-making bodies (Higgs et al., 2016; Smith et al., 2019), it seems that there is a reduction in the likelihood of such incidents. On the other hand, CSIs may lead to noticeable changes in the composition of top management teams, such as more senior executive turnover (Masli et al., 2016; Li et al., 2019) or a readjustment in the makeup of boards and committees. Changes may include inviting IT experts with proven experience in a related industry to intervene, or appointing new board members with valuable educational and professional skills in IT-related areas, the aim being to avoid CSIs from reoccurring and to reduce the likelihood of new IT incidents.

Surprisingly, studies on the relations between IT-related incidents and specific governance aspects of management boards are limited to U.S. samples. Masli et al. (2016) analyzed the likelihood of CEO/CFO turnover in U.S. firms that reported an IT material weaknesses. According to these authors, senior executive turnover appears to be determined by the type of IT deficiency, with CEO turnover affected by issues with overall IT management responsibilities, and CFO departures affected

by problems related to internal IT control. Studying the S-OX 404 reports of U.S. groups, Haislip et al. (2016) also found higher levels of CEO/CFO turnover in cases of IT-related material weaknesses and observed further changes toward more IT expertise to remediate negative effects of IT-related incidents. While Li et al. (2019) confirmed that internal control material weaknesses were associated with higher CEO and higher CFO turnover, the authors only noted remediation measures when the CEO actually left the firm. Likewise, Banker and Feng (2019) confirmed higher CSI-related turnover for CEOs and CIOs in U.S. firms, with the exception of CFOs, who do not seem to be held accountable for such IT incidents. Analyzing the impact of operational IT failures on board-level governance of U.S. publicly listed firms, Benaroch and Chernobai (2017) also showed that IT incidents lead to adjustments to the board, including higher CIO turnover as well as more effort to increase the board's level of IT experience. However, these changes tend to be limited to internal executive directors.

By analyzing the relationship between top executives' IT knowledge and organizational output, Haislip et al. (2017) suggested that higher levels of IT expertise by CEOs lead to greater transparency, while greater CFO IT expertise reduces the number of problems reported, suggesting that it results in fewer CSIs. Likewise, Haislip and Richardson (2018) investigated a large sample of U.S. firms and found that CEOs with greater IT expertise appear to encourage more efficient IT practices. As a result, internal information reporting systems tend to improve through better forecasting accuracy and faster reporting cycles. Aside from senior executives, other scholars have studied the role of boards of directors regarding IT risk management. Their findings also suggest a positive yet less sharp impact of IT expertise, while highlighting the importance of committees both before and after CSIs. For example, Vincent et al. (2019) found a positive impact of IT expertise on management boards in terms of IT risk management practices, but suggested that a lack of IT expertise is less important than the board's involvement in IT risk monitoring since the former can be compensated for by bringing in external specialists. Furthermore, IT risk management practices appear more mature when monitoring is ensured at board level rather than by an executive committee. This confirms the findings of Higgs et al. (2016) who observed that firms with more mature technology committees are less likely to experience IT security breaches. In line with these findings, Smith et al. (2019) suggested that the presence of board-level risk committees as well as more active audit committees can help to mitigate higher audit fees related to data security breaches. More generally, firms hit by CSIs exhibit fewer innovative activities (He et al., 2020) and a greater propensity to manipulate earnings at the cost of future profitability (Xu et al., 2019) following a breach, leading to negative overall effects on shareholders' wealth (Gatzlaff and McCullough, 2010). To sum up these results, the current academic literature shows a link between the management of CSIs and executive board composition, tenure, responsibilities and expertise.

The low number of studies on the impact of CSIs on the composition of top management teams is quite surprising as the literature points to several links between IT-related incidents and firm performance. These include decisions about the voluntary disclosure of CSIs; diverse market reactions with respect to the nature of these incidents; as well as reactions to transparency requirements. Concerning the first point, managers seem to fear the effects of negative news on reputation and, therefore, tend to "sugarcoat" the anticipated negative consequences (Fang et al., 2014). Nevertheless, a study of U.S. firms (Gordon et al., 2010) found a positive link between the voluntary disclosure of incidents related to information security and firm value suggesting that managers should recognize the positive signaling effects of voluntary disclosures to market participants. In addition, both the nature and the severity of CSIs seemingly determine positive or (to be avoided) negative market reactions. Studies have found that breaches affect companies with customer data more substantially as these firms receive more public attention and are often associated with data protection laws such as GDPR (European Parliament and European Council, 2016). In line with this point, several studies have detected negative Stock Appreciation Rights (SARs) in firms experiencing failures regarding confidential customer information (Campbell et at., 2003; Aytes et al., 2006; Maholtra and Malholtra, 2011) and other privacy breaches (Acquisiti et al., 2006; Nicholas-Donald et al., 2012), with payment card fraud causing the highest losses (Johnson et al., 2017). Firms are also afraid of not respecting basic information security management principles as technically 'easy' breaches tend to have a stronger impact on stock prices than highly sophisticated attacks. Accordingly, Leung and Bose (2008) and later Bose and Leung (2014) noted that phishing, an example of an attack that can mostly be avoided through

internal awareness, leads to negative Cumulative Abnormal Returns (CARs). In general, this form of breach appears to have a more serious impact on technology companies than on non-technology firms (Pirounias et al., 2014). A link between reputation and stock market price was also found when good reputation is viewed as an investment against the impact of IT security breaches. Companies with greater pre-event corporate social responsibility thereby seem to exhibit less negative CARs (Akey et al., 2018) and are less likely to incur a breach (Lending et al., 2018). Finally, regulatory and financial market authorities increasingly require transparency from companies affected by IT security incidents, thereby determining managerial decision-making. Such requirements are, on the one hand, due to the need to protect critical national infrastructures (European Council, 2016) and on the other to protect investors from distorted information on the firm's health (Securities and Exchange Commission, 2018). Thus, simply accepting the consequences of a security breach (e.g., by compensating the customers after such an IT-related incident (Goode et al., 2017)) appears to be insufficient.

Since companies have an interest in managing CSIs to improve their performance, one way to do this is to strengthen their corporate governance through adjustments to the top management team. Prior research has suggested that individual members of executive teams can have a significant impact on improving firm management with respect to IT risks. However, no study to date has addressed changes that take the entire board into account or the specific situation in Europe. To fill this gap, we analyze the impact of CSIs at executive level, at the same time extending research to outside the U.S. (Masli et al., 2017; Vincent et al., 2019). Accordingly, we seek to answer the research question "How far CSIs impact on the composition of management boards as well as the profiles and responsibilities of their members?"

3. Data and Methodology

We base our study on German listed firms for the reasons already highlighted before (size of the economy and CSI-related costs, less formalized disclosure requirements, governance system with a two-tier board structure, lack of research exploring the link between CSIs and German top executive teams). We conduct our study on German blue-chip companies listed on the Dax 30 stock market index. Traded on the Frankfurt Stock Exchange, the index comprises the country's 30 largest industrial and financial listed firms. Index membership is reviewed twice a year and depends on companies' order book volume and their market capitalization.

To start, we identified all the firms listed in the Dax 30 index at any one time in the period 2005-2018. This gave us a total sample of 43 companies. We then identified any major publicly disclosed CSIs during the 14-year period for each firm. The biggest challenge here was to get precise information as, to our knowledge, no official database on relevant CSIs experienced by listed German firms exists to date. While the country has a Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*), the latter does not publish or distribute any data on IT-related incidents in German companies or their repercussions. This corresponds 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, p. 97). Despite extensive data being gathered on the technical consequences of IT-related incidents, the question of their impact on strategic decision-making and organizational outcomes lacks clear empirical evidence. Aiming to deliver the most accurate and conclusive results for a qualitative empirical assessment we, therefore, opted for a research method in the form of an in-depth content analysis of media sources.

The media represent and influence the public sphere in modern economies as a primary space in which problems and solutions are discussed, and responsibilities and competencies are contested (Neidhardt, 1994). Considered as a structured social space, the media follow a specific rationale and have specific characteristics (Hilgartner and Bosk, 1988) that include agenda-setting and gatekeeping functions as well as assigning news value and imposing attention cycles. In other words, the media are "a site on which various social groups, institutions, and ideologies struggle over the definition and construction of social reality" (Gurevitch and Levy, 1985, p. 19), actively taking part in the construction

of social realities by presenting them as legitimate or not (Lok, 2010). Consequently, the media affect the reputation of both firms and their managers, with the magnitude of the effect depending on the nature of the news. Studying German companies, Raithel and Schwaiger (2015) found reputational perceptions driven by non-financial aspects to have a bigger impact on shareholder wealth than those affected by financial factors. Stern and James (2016) noted that disclosing positive information on a firm's research and development activities as well as their performance also sends positive signals to the managerial labor market about the quality of a firm's executives and thus has a positive impact on voluntary executive turnover. Similar reputation reactions may also exist with respect to top executives' IT-related risk management and adequate handlings of experienced CSIs.

3.1 Identification of IT-related incidents

Given these considerations and the lack of an official database on CSIs in Germany, we decided to conduct an in-depth manual analysis of all IT incidents experienced by our sample firms that gained public attention by being disclosed during the observation period, either by the companies themselves or through third parties. Information on CSIs was gathered from corporate websites, official corporate documentation and online communication sources. To compile the relevant data, we employed the most frequently used search engines, Google and Bing. The links followed an n+2 logic, where n is the last tab showing relevant information on a potential CSI. Our keyword selection included the firm name as well as one of the items "security", "incident", "cybersecurity" or "attack", either in English or in German. Following the logic of a systematic review (Cook et al., 1997; Cooper, 1998; Denyer and Tranfield, 2008), the data were verified through cross-checks with other sources, including corrections or corporate (re)statements. For each of the CSOs detected, we noted the date of both the IT incident and its disclosure. In addition, we checked the firms' annual reports to identify whether any management board-related post-CSI governance measures (composition changes, restructuration of functional units or changes in responsibilities) were taken or if the topic of IT security was explicitly addressed. Positive findings were further analyzed and then presented as mini cases following our quantitative analysis. Contrary to U.S. studies on CSIs, missing or non-verifiable data on the IT-related incidents' financial outcomes of our German sample firms did not allow us to quantify their business impact (such as changes in market value or CARs), thereby limiting our analysis to directly observable and documented effects following the disclosure of CSIs (legal prosecution, loss of customers etc...).

3.2 Measurements of governance data

Governance composition information about the sample firms' management boards was gathered from the companies' annual reports over the 14-year observation period (2005-2018). The data comprised both individual information about the board members as well as the aggregated characteristics of the management board as an entity. Inspired by Hambrick and Mason (1984), we divided the management board members' background characteristics into four areas: personal, demographic, educational and professional information. Our data was completed by general management board characteristics comprising for each considered fiscal year the variables board size, proportion of female executives, level of turnover, presence of members with foreign citizenship, age, tenure and educational background. Table 1 details the measurement and operationalization of our governance data.

Table 1. Measurement and operationalization of governance data

Category	Variable	Measurement / Operationalization	
Characteristics of mangement board members	Personal information		
	Name	First name and surname	
	Demographic information		
	Age	Number of years at the end of the fiscal year or at the moment of departure	
	Gender	Female or male	
	Citizenship	Type of single or multiple nationalities	
	Educational information		
	Professional Education	Type of professional qualification	-
	Higher Education	Type of higher education degree	categorized for both into IT, business and economics, law, social
	Doctorate	Type of Ph.D. degree	sciences, languages, natural sciences, engineering, miscellaneous
	Professional information		
	Board position	Distinction between CEO, Vice-CEO, CFO and ordinary management board member	
	Functional responsibilities	Area of duties (when specified)	
	Geographical responsibilities	Geographical area of responsibilities (when specified)	
Characteristics of management boards	Board size	Sum of full-year members and day-based pro rata presence of joining or leaving members	
	Female members	Sum of full-year female members and day-based pro rata presence of joining or leaving female members dividided by board size	
	Foreign members	Sum of full-year members with foreign citizenship and day-based pro rata presence of joining or leaving members with foreign citizenship dividided by board size	
	Turnover level	Sum of day-based pro rata presence of joining or leaving members divided by board size	
	Age	Average age of full-year and joining members at the end of the fiscal year	
	Tenure	Sum of years of service of full-year, joining and leaving members (based on day of first appointment / of ast service) divided by board size	

4. Results and Analysis

Our multisource research shows that 16 of the 43 current or former Dax 30 companies experienced a significant CSI (19 IT incidents were identified in total) at least once during the 14-year period (2005-2018), representing 37.2% of all the sample firms. As Table 2 shows, five IT incidents took place prior to 2015, while almost three-quarters of all CSIs occurred after 2015. This may be interpreted in two ways: either the technological progress in IT combined with the subsequently more intensive use of data caused a parallel increase in the frequency of CSIs, or the growing rise in IT-related incidents is the result of increased public disclosure due to stronger interest and sensitivity of stakeholders together with a faster dissemination of related information.

Table 2. CSIs in Dax 30 companies occurring between 2005 and 2018

Company	Year	IT security incident
Adidas	2018	Loss of personal customer data
BASF	2018	Technology leak caused by employees
Bayer	2018	Malware attack of IT network
Deutsche Lufthansa	2018	Security vulnerability of booking platform
Infineon Technologies	2018	Security vulnerability of chipsets
Volkswagen	2018	Data breach
Beiersdorf	2017	Malware attack of IT network
Deutsche Post DHL	2017	Malware attack of IT network
E.ON	2017	IT failure of customer accounts
FMC	2017	Loss of patient data
Merck	2017	Malware attack of IT network
Deutsche Telekom	2016	Attack of customer routers
ThyssenKrupp	2016	Malware attack and theft of intellectual property
Volkswagen	2016	Security vulnerability of IT system of cars
BMW	2015	Security vulnerability of IT system of cars
Adidas	2011	Attack of website
Siemens	2010	Malware attack of control system of plants
Deutsche Telekom	2008	Supervsion of supervisory board members & executives
RWE	2008	Malware attack of IT network

Source: our own data; observation period = 2005-2018

After identifying all the companies affected by CSIs during our observation period, we conducted a comprehensive analysis of the characteristics of the management boards of all the firms concerned. Our analysis was conducted from three perspectives:

- a cross-company perspective that focused on the key characteristics of the management boards and their evolution during the observation period,
- a cross-company perspective that analyzed the profiles of all the board members and their evolution during the entire observation period, and,
- a firm-specific perspective that explored the characteristics of both the management board and its individual members for each firm responding to a CSI, while searching in particular for key changes following the IT security incident experienced.

4.1 Evolution of management board characteristics

Analysis of the characteristics of the management boards during the 14-year observation period shows some interesting findings (Table 3). Board size, measured by the relative indicator of the sum of full-year mandates completed by intermediate management board entrances and exits on a daily-basis, appears to be relatively stable over time as variation concerns around six members on average. Given the tougher legal requirements regarding the representation of women on the supervisory boards of German listed firms (minimum quota of 30% of all new members since 2016), the proportion of female representatives on management boards also increased over the course of the observation period, although it remained at a relatively low level. That said, in 2018, five out of 16 companies (BASF, E.ON, Infineon Technologies, RWE and ThyssenKrupp) still had no women among their top managers. As a result of ongoing internationalization, the percentage of non-German top managers increased to an average of 31% of all full-year mandates, representing a rise of around 50% compared to 2005. Firms with the highest average level of foreigners among their top executives were FMC (75%), Adidas (55%) and Deutsche Post (44%). Those with the lowest levels over time were E.ON (7%), BASF (12%) and Infineon Technologies (12%). While at first appearing somewhat counterintuitive, management board turnover also turned out to be quite stable over time, with annual entries and exits representing 16% of the members on average. Looking at the entire period, turnover was highest at Beiersdorf (22%), followed by Bayer (20%) and E.ON (20%), whereas it seems to have been quite low at Adidas (7%), BASF (8%) and FMC (12%). As a result of ongoing internationalization, the percentage of non-German top managers increased to an average of 31% of all full-year mandates, representing a rise of around 50% compared to 2005. Firms with the highest level of foreigners among their top executives were FMC (75%), Adidas (55%) and Deutsche Post (44%). Those with the lowest levels over time were E.ON (7%), BASF (12%) and Infineon Technologies (12%). Likewise, the average age of board members was stable over time, fluctuating at around 54 years old, with the youngest top managers during the period in question working at Infineon Technologies (51.5 years) and the oldest at Volkswagen (57.7 years). Finally, our analysis also showed relative stability of average tenure at around six years. The firms with the longest average tenure were Adidas (11.25 years) and BASF (7.57 years), while those with the shortest average stay were RWE (4.9 years) and Beiersdorf (4.52 years).

Table 3. Evolution of management board characteristics of sample firms between 2005 and 2018

Company / Year	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Size														
Mean	*6,21*	*6,11*	*5,90*	*5,72*	*5,66*	*5,91*	*6,14*	*5,97*	*5,81*	*5,79*	*6,05*	*6,13*	*6,19*	*6,41*
Median	*5,76*	*5,97*	*5,37*	*5,21*	*5,45*	*5,63*	*6*	*6*	*5,54*	*5,50*	*6,16*	*6,30*	*6,44*	*7*
Minimum	*3*	*3*	*3*	*3*	*3,59*	*3,09*	*3,75*	*3*	*3*	*3*	*3,25*	*3,83*	*2,33*	*2*
Maximum	*11,84*	*10,33*	*8,75*	*8,19*	*8,25*	*9*	*10*	*9,87*	*9*	*8,58*	*8,81*	*9*	*9*	*8,36*
Proportion of women														
Mean	*0*	*0*	*0*	*0,01*	*0,01*	*0,02*	*0,03*	*0,06*	*0,07*	*0,07*	*0,09*	*0,10*	*0,10*	*0,09*
Median	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0,12*	*0,12*	*0,12*
Minimum	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Maximum	*0*	*0*	*0*	*0,11*	*0,15*	*0,22*	*0,20*	*0,24*	*0,33*	*0,40*	*0,40*	*0,36*	*0,25*	*0,20*
Proportion of foreigners														
Mean	*0,21*	*0,22*	*0,22*	*0,22*	*0,23*	*0,25*	*0,25*	*0,25*	*0,24*	*0,28*	*0,29*	*0,27*	*0,29*	*0,31*
Median	*0,13*	*0,21*	*0,20*	*0,18*	*0,24*	*0,24*	*0,23*	*0,18*	*0,20*	*0,25*	*0,25*	*0,25*	*0,25*	*0,27*
Minimum	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Maximum	*0,86*	*0,86*	*0,86*	*0,86*	*0,85*	*0,86*	*0,86*	*0,86*	*0,63*	*0,60*	*0,60*	*0,66*	*0,72*	*0,76*
Turnover level														
Mean	*0,16*	*0,18*	*0,17*	*0,11*	*0,10*	*0,22*	*0,13*	*0,16*	*0,17*	*0,14*	*0,14*	*0,19*	*0,19*	*0,16*
Median	*0,11*	*0,20*	*0,07*	*0,03*	*0,08*	*0,24*	*0*	*0,13*	*0,15*	*0,14*	*0,07*	*0,17*	*0,18*	*0,07*
Minimum	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Maximum	*0,63*	*0,35*	*0,63*	*0,37*	*0,27*	*0,62*	*0,66*	*0,49*	*0,51*	*0,35*	*0,66*	*0,59*	*0,49*	*0,53*
Age														
Mean	*54,28*	*53,85*	*53,87*	*53,73*	*54,14*	*54,05*	*53,58*	*54,03*	*53,56*	*53,61*	*54,19*	*54,75*	*54,42*	*54,70*
Median	*54,91*	*54,35*	*54,67*	*54,03*	*53,85*	*53,88*	*53,73*	*54,04*	*54,25*	*53,55*	*54,11*	*54,54*	*54,31*	*54,93*
Minimum	*49,16*	*48,62*	*49,28*	*49,97*	*50,93*	*50,43*	*48,61*	*48,38*	*49,05*	*50,05*	*51,03*	*52,05*	*49,69*	*51,56*
Maximum	*58,59*	*57,31*	*57,04*	*58,04*	*59,04*	*57,23*	*58,02*	*59,02*	*58,90*	*59,89*	*60,47*	*60,35*	*60,30*	*57,78*
Tenure														
Mean	*6,19*	*5,88*	*5,40*	*5,67*	*6,02*	*6,35*	*5,96*	*6,41*	*5,98*	*5,94*	*5,85*	*6,02*	*5,72*	*5,75*
Median	*6,01*	*5,44*	*5,38*	*5,21*	*5,56*	*6,41*	*5,27*	*5,91*	*5,23*	*5,58*	*5,29*	*5,83*	*5,73*	*5,80*
Minimum	*3,97*	*4,12*	*0,90*	*2,29*	*2,53*	*3,49*	*3,21*	*3,57*	*2,55*	*2,67*	*2,81*	*3,03*	*3,27*	*2,90*
Maximum	*11,14*	*8,89*	*9,89*	*10,89*	*11,89*	*12,89*	*13,89*	*14,89*	*15,02*	*13,77*	*11,33*	*11,97*	*8,59*	*8,26*

Source: annual reports; observation period = 2005-2018, sample = 16 firms

4.2 Evolution of management board member profiles

In a second step, we studied the individual profiles of management board members in the sample firms, which also showed interesting results (Table 4). The data revealed a very high level of top managers holding a higher tertiary education degree. The average was 88% in 2005, increasing 13 years later to over 96%. Consequently, in 2018, only three groups (Deutsche Lufthansa (20%), Bayer (18%) and Merck (13%)) had management board members without higher education degrees. A more detailed examination of educational background revealed the predominance of business administration or economics degrees. The average number of management board members with this type of degree in fact grew over time (from 43% to 51%), exceeding 75% in five companies in the last year (Adidas, Beiersdorf, Deutsche Post, Deutsche Telekom and Siemens), while the firm with the lowest share of top executives with such a profile reported a percentage of 17% in 2018 (Merck). Alongside these aspects, the proportion of management board members with a law degree decreased significantly during the period investigated, passing from 13% on average in 2005 to just 6% in 2018. In 2005, the highest proportion of law graduates among German top managers in our sample firms was 67% (Deutsche Lufthansa), whereas 13 years later, the level was a mere 22% (E.ON).

Table 4. Evolution of management board member profiles from sample firms between 2005 and 2018

Education / Year	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
HE degree (all areas)														
Mean	*0,88*	*0,87*	*0,83*	*0,90*	*0,92*	*0,94*	*0,97*	*0,97*	*0,91*	*0,97*	*0,96*	*0,96*	*0,96*	*0,96*
Median	*0,91*	*0,86*	*0,89*	*0,98*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*
Minimum	*0,63*	*0,56*	*0,04*	*0,67*	*0,75*	*0,75*	*0,81*	*0,83*	*0,04*	*0,67*	*0,60*	*0,57*	*0,73*	*0,80*
Maximum	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*
Degree in business														
Mean	*0,43*	*0,44*	*0,45*	*0,47*	*0,46*	*0,46*	*0,48*	*0,54*	*0,55*	*0,56*	*0,55*	*0,51*	*0,51*	*0,51*
Median	*0,45*	*0,46*	*0,48*	*0,49*	*0,48*	*0,47*	*0,45*	*0,53*	*0,61*	*0,52*	*0,55*	*0,55*	*0,55*	*0,50*
Minimum	*0*	*0*	*0*	*0*	*0*	*0*	*0,12*	*0,20*	*0,20*	*0,14*	*0,17*	*0,16*	*0,17*	*0,17*
Maximum	*0,82*	*0,82*	*0,80*	*0,80*	*0,80*	*0,83*	*0,75*	*0,81*	*0,86*	*0,89*	*0,85*	*0,84*	*0,85*	*0,86*
Degree in law														
Mean	*0,13*	*0,12*	*0,11*	*0,12*	*0,12*	*0,10*	*0,09*	*0,09*	*0,10*	*0,09*	*0,08*	*0,09*	*0,07*	*0,06*
Median	*0*	*0*	*0*	*0,02*	*0*	*0*	*0*	*0*	*0,02*	*0*	*0*	*0,05*	*0*	*0*
Minimum	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Maximum	*0,67*	*0,51*	*0,52*	*0,58*	*0,60*	*0,50*	*0,33*	*0,33*	*0,25*	*0,25*	*0,25*	*0,25*	*0,27*	*0,22*
Degree in IT sciences														
Mean	*0,05*	*0,05*	*0,03*	*0,02*	*0,03*	*0,03*	*0,04*	*0,03*	*0,03*	*0,03*	*0,03*	*0,03*	*0,03*	*0,03*
Median	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Minimum	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Maximum	*0,24*	*0,25*	*0,25*	*0,25*	*0,25*	*0,25*	*0,25*	*0,25*	*0,24*	*0,21*	*0,20*	*0,19*	*0,21*	*0,17*
PhD (all areas)														
Mean	*0,49*	*0,45*	*0,46*	*0,47*	*0,49*	*0,47*	*0,45*	*0,43*	*0,44*	*0,38*	*0,34*	*0,35*	*0,35*	*0,37*
Median	*0,47*	*0,51*	*0,54*	*0,55*	*0,54*	*0,47*	*0,46*	*0,41*	*0,48*	*0,35*	*0,33*	*0,31*	*0,24*	*0,26*
Minimum	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Maximum	*1*	*0,97*	*0,70*	*0,96*	*1*	*1*	*0,88*	*0,80*	*0,80*	*0,95*	*1*	*0,89*	*0,94*	*1*
PhD in business														
Mean	*0,12*	*0,12*	*0,13*	*0,13*	*0,14*	*0,12*	*0,13*	*0,12*	*0,12*	*0,10*	*0,09*	*0,08*	*0,10*	*0,12*
Median	*0,04*	*0,03*	*0,11*	*0,12*	*0,14*	*0,09*	*0,13*	*0,13*	*0,13*	*0,10*	*0,06*	*0,02*	*0,00*	*0,00*
Minimum	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Maximum	*0,50*	*0,46*	*0,42*	*0,40*	*0,44*	*0,43*	*0,33*	*0,33*	*0,29*	*0,30*	*0,33*	*0,32*	*0,43*	*0,50*
PhD in law														
Mean	*0,10*	*0,09*	*0,07*	*0,08*	*0,09*	*0,08*	*0,06*	*0,05*	*0,07*	*0,07*	*0,06*	*0,07*	*0,06*	*0,05*
Median	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Minimum	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Maximum	*0,50*	*0,49*	*0,38*	*0,44*	*0,50*	*0,50*	*0,30*	*0,20*	*0,25*	*0,25*	*0,25*	*0,25*	*0,27*	*0,22*
PhD in IT sciences														
Mean	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0,01*	*0,01*	*0,01*	*0,01*	*0,01*	*0,01*
Median	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Minimum	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Maximum	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0,13*	*0,14*	*0,14*	*0,14*	*0,14*	*0,14*

Source: annual reports; observation period = 2005-2018, sample = 16 firms, HE = higher education, IT = information technology

In line with our research question, we also studied the proportion of top executives with a higher education degree (graduate or undergraduate) in IT-related disciplines. Surprisingly, the results show a high level of homogeneity among management boards regarding the absence of IT education backgrounds, with a very low average in 2005 (5%) that declined even further over time (3% in 2018). While this finding is already surprising, a closer look reveals that only two companies (Merck and Volkswagen) had IT graduates on their management board in 2018, while the remaining 14 firms had no board members with a computer science degree. Given the increasing relevance of IT risk-related management since the millennium, such low representation of IT backgrounds among top executives throws serious doubt on whether cybersecurity skills are sufficiently represented on the firms' highest decision-making instances. An in-depth analysis of the areas of responsibility of our sample firms' management board members confirms this. In 2018, only four of the 18 groups studied explicitly mention IT security as an area included in the scope of responsibilities of at least one member of their executive team. In three other companies, IT security was added to the CEO's responsibilities as an additional function. In the remaining 11 firms, however, IT security was not explicitly mentioned among the board members' responsibilities. The frequently observed absence of IT backgrounds may also be linked to another specific aspect of the German governance system: far more than a Bachelor's or Master's degree, a PhD is considered a highly prized criterion with regard to top management positions in Germany (Hartmann, 2007; Prinz, 2011). This is corroborated by the high proportion of executives holding a PhD in the companies in our sample. Even though we observed a significant decrease over time, with the average number falling from 49% in 2005 to 37% 13 years later, the percentage was still comparatively high, notably in comparison with other countries where doctorates are typically a precursor to an academic rather than a managerial career. Consequently, the number of

firms in which no executive holds a PhD is very low (three out of 18 in 2015). A closer look at our data shows that management board members with a PhD generally gained their degree in business or economics. This share remained quite stable during the study period, averaging out at 12%. It is followed by managers with a PhD in law, even though their percentage decreased over time from 10% to 5% of all board members. Finally, our data show that top executives holding a PhD in IT are very rare. Only one company (FMC) in our sample had one member with a PhD in IT science among its top managers, and this was only since 2013. The scarcity of such executives may be explained by the fact that IT science is a comparatively new field of study that offered only very few programs when most of the top executives in our sample companies were studying. This argument, however, cannot be confirmed by the low and even slightly decreasing number of executives with IT degrees (between 3% and 5%) during the observation period.

4.3 Post CSI reactions in companies

In addition to the presentation of the characteristics of all the management boards and their members' profiles, we ran a comprehensive analysis of companies that had experienced a CSI during the observation period and, in its wake, modified governance aspects related to their management board (composition, restructuration of functional units or change in profiles/responsibilities) or explicitly addressed the topic of IT security in their annual report(s). In total, we were able to identify just four firms and five IT-related incidents that addressed the issue in some way. For the 12 remaining companies, representing 14 incidents, no reaction (disclosure or changes to their management board) could be observed. In the following cases we analyze the adjustments made in each of the four companies identified and present the post-CSI measures adopted.

Beiersdorf

Beiersdorf, an almost 140-year-old multinational manufacturer of personal-care products and pressure-sensitive adhesives, headquartered in Hamburg (Beiersdorf, 2021) was one of a large number of international companies that fell victim to NotPetya, a malicious malware exploiting a Windows operating system vulnerability called "Eternal Blue". This malware was deployed the same year in two other attacks, namely "WannaCry" and "Adylkuzz". NotPetya blocked several hundred thousand computers in order to blackmail firms. A bitcoin blockchain suggests that about 30 individual entities paid the $300 ransom demanded to decrypt the infected hard drives. Among the victims were large groups like the French construction and material firm Saint Gobain, the U.S. Drugmaker Merci & Co., and the food manufacturer Mars Inc. With regard to Beiersdorf, India-based employees of Nivea Skin care products reported a direct impact on their systems (Stubbs and Polityuk, 2017). As a consequence of the malware attack, Beiersdorf announced that €35 million of sales revenues would be shifted to the next quarter (Kovacs, 2017).

Although Beiersdorf's annual report for the fiscal year 2017 (pp. 5-6) mentioned that both its supervisory board and the audit committee had explicitly dealt with the cyber-attack in June 2017, no information could be found on the scope of the IT-incident or its impact. It further did not appear to result in any direct changes to the composition of the company's management board either. However, Beiersdorf's CFO, a male manager who graduated in business administration and whose expertise also included IT, left the group one year later in June 2018 as his contract was not renewed. He was replaced by a female manager, who was also a graduate in business administration, with responsibilities covering the areas of audit, compliance, law, quality assurance and IT remaining unchanged. While no explicit reason was put forward for the CFO's departure, the economic press suggested that the non-renewal of his contract was related to the experienced CSI (Finance Magazin, 2018/02/16).

BMW

Bayerische Motoren Werke is a German multinational manufacturer of automobiles and motorcycles founded in 1916, which currently employs around 135,000 people worldwide (BMW, 2021). In 2015, BMW cars were found to be vulnerable due to a remote hack flaw in their "ConnectedDrive" tool. The problem was discovered by Germany's leading automobile association, ADAC, which discovered the vulnerability during a white hat exercise. It enabled researchers to use reverse engineering to build a copy of BMW's servers that could send remote unlocking instructions to

cars. A patch was consequently sent to 2.2 million cars potentially vulnerable to the attack (Williams, 2015). The connection of devices to the internet, often treated in the context of the "Internet of Things" (IoT), is a major issue in the automotive industry. Other automobile manufacturers experienced similar media coverage, e.g., Volkswagen was exposed to serious allegations in 2015 which claimed that hackers could easily unlock about 100 million vehicles (Greenberg, 2015).

One consequence observed with respect to the CSI was a slightly greater focus on the topic of cyber-attacks in the group's annual reports from 2016 onward, pointing in particular to the relevance of cybersecurity as well as the potential consequences of cyber-attacks. Otherwise, no direct impact on BMW's corporate governance system was found. The areas of responsibility of the group's management board members - which surprisingly comprised no term related to IT - remained unchanged in the three years following the incident. Similarly, none of the changes in the management board's composition that occurred after 2015 could be related directly to the CSI.

Deutsche Telekom

Deutsche Telekom is one of Europe's largest telecommunication companies that currently employs about 216,000 people worldwide (Deutsche Telekom, 2021). In 2008, the firm experienced a high-profile IT security scandal that led to extensive national and international media coverage (Spiegel 2008/22; Wirtschaftswoche 2008; Handelsblatt 2008; Manager Magazin 2008; New York Times 2008; Le Monde 2008). The scandal dated back to the early 2000s when several top executives and members of the group's supervisory board decided to launch an investigation into repeated leaks regarding plans for massive layoffs. The investigation was led by an internal corporate security unit called 'KS3' that (legally and illegally) analyzed communication data to identify the origins of the leak. As a result, at least 55 people were monitored for almost two years, including several members of the group's supervisory board, one of its largest subsidiaries (T-Mobile), one member of the groups' management board, several members of work councils, including their families, external labor union representatives and journalists (Spiegel, 2008/27; Wirtschaftswoche 2008/05/04). In addition, the firm experienced several outages from 2008 onwards, and one particularly successful hack which left 900,000 of its UK customers without access to numerous services (BBC, 2016), although these incidents obtained far less press coverage than the 2008 spy scandal.

As news coverage of the group's eavesdropping controversy only occurred in May 2008, no reason was given in the annual report for the departure of the CEO in November 2006 after more than five and a half years on the group's management board. The president of the company's supervisory board also resigned without any explicit reason in February 2008, three months before the scandal broke. It appears that the only internal measures taken by the new CEO were to fire the firm's security chief and several leading employees of the internal security unit in 2007, before the controversy became public knowledge in the second quarter of 2008. Surprisingly, even after the affair did become public, it was not explicitly mentioned in the group's subsequent annual reports. Likewise, no changes were noted regarding the composition of the management board or the scope of the members' responsibilities, and issues of compliance and risk management were only addressed in 2010 by the group's supervisory board and audit committee. That said, a new management position covering data security, legal affairs and compliance was created at the end of 2008 (Georg, 2017). The position was attributed to a German manager with a PhD in law, who already was the group's general counsel since 1997. This change was designed to reassure stakeholders about the firm's compliance and sensibilization with respect to the issue. The position was dissolved 11 years later at the end of 2019, with the security governance function returning to the manager in charge of technology and innovation (Deutsche Telekom, 2020).

FMC

Fresenius Medical Care (FMC) is a German healthcare company employing in 2019 more than 120,000 people. FMC provides products and services for dialysis, hospitals, and inpatient and outpatient medical care kidney dialysis services via worldwide patient centers and production sites in the U.S., Germany and Japan. In 2018, the North American branch of FMC was fined for filing breach reports in 2013 concerning five separate CSIs linked to electronically protected health information that occurred in 2012. The company agreed to pay $3.5 million to the U.S. Department of Health and Human Services (HHS) and to adopt a comprehensive corrective action plan designed to address potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules (HHS,

2018a). The incidents included failure to “implement policies and procedures to address security incidents”, failure to “govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility”, failure to “safeguard their facilities and equipment from unauthorized access, tampering, and theft”, and failure to “implement a mechanism to encrypt and decrypt ePHI, when it was reasonable and appropriate to do so under the circumstances" (HHS, 2018b p.1). The fine showed that the U.S. regulator treated the protection of medical customer data seriously, in line with findings from Acquisiti et al. (2006) and Nicholas-Donald et al. (2012) regarding negative market reactions in cases of privacy breaches.

Even though FMC explicitly addressed IT security questions in the annual reports following the CSIs, no documentation about the incidents or changes to the composition of the company’s management board or the scope of responsibilities of their members was observed. This is even more surprising as one top executive holds a PhD in computer science and may thus be assumed to have sound expertise in this area. That said, several operational measures were introduced at lower hierarchical levels. In the year prior to disclosure of the CSIs, FMC thus announced the creation of a new worldwide operating function in charge of data- and cybersecurity questions, which was incorporated into the group’s law department and completed by a working team of internal risk, security and compliance IT specialists (FMC, 2017, p. 84). One year later, the company further reconfirmed its focus on privacy and data security and set up a global data protection program defining minimum personal data protection requirements. The program is monitored by the group’s management board that provides updates on the program’s status twice a year as well as relevant data protection concerns (FMC, 2018, p. 97). To guarantee adherence to these measures, a global head of data protection and cybersecurity law as well as a privacy team ensure further support.

5. Discussion

Our study presents four principal findings. First, we found that a comparatively low percentage (37.2%) of German blue-chip companies fell victim to at least one major and publicly documented CSI during the observation period (2005-2018). Given that only about half of all IT incidents appear to be detected (Kutscher, 2017) and in light of a survey by McAfee (2020) according to which 96% of a total of 1,500 organizations contacted said they experienced IT incidents in 2019, we believe that a much larger number of CSIs can be assumed to have occurred in the period in question, which did not reach the public sphere. In addition, only a quarter of the companies covered by the media displayed a noticeable post-incident governance reaction, either by documenting the respective CSI in the annual report, changing the management board’s composition or altering the scope of their members’ responsibilities (Table 5). Our findings support the assumption of a somewhat slow and reluctant governance reaction to IT-related incidents that do not seem to be considered as issues requiring major changes at top executive level. Consequently, annual reports, serving by definition as an interface to company stakeholders, appear to be only marginally used as a communicative medium with respect to CSIs in Germany.

Secondly, alongside the finding that CSIs do not seem to result in firms noticeably modifying the composition or the scope of their top management team’s responsibilities, our qualitative analysis also shows that while some changes were made after IT-related incidents, these adjustments went against the general trend. The most powerful post-incident signal - the departure of a senior executive board member - was only observed in one case (Beiersdorf), where the CSI led to the non-renewal of the CFO’s contract. A less powerful response was noted at Deutsche Telekom where, unlike most groups that keep the status quo regarding the number of business units on their management board after an IT-incident, the firm added a new unit following the eavesdropping controversy detected in 2008. It was in fact dissolved 11 years later as the group annually publishes updates on data security and privacy and has introduced some seemingly successful remediation measures, making the unit redundant. Furthermore, our findings on post-CSI effects in German firms did not confirm prior research on U.S. firms according to which CSIs result in higher senior executive turnover, except for Beiersdorf and Deutsche Telekom where, in the case of the latter, reactions occurred prior to disclosure of the incident (Haislip et al., 2016; Masli et al., 2016; Benaroch and Chernobai, 2017; Li et al., 2019).

Table 5. Summary of IT incidents identified which led to a governance reaction

Company	Changes in board composition	Restructuration of board functional units	Changes in profiles/ responsibilities	Mentioning of topic in annual reports
Beiersdorf	yes	no	no	yes
BMW	no	no	no	yes
Deutsche Telekom	yes	yes	yes	no
FMC	no	no	yes	yes

Source: our own analysis

Thirdly, an IT-related educational background seems to be the exception rather than the norm among top executives in German firms that have experienced CSIs. Depending on the years, no more than three to five of the 16 companies have at least one top manager with an IT degree on their board, with the average percentage varying over time between 3% and 5%. These results are similar to those of Haislip and Richardson (2018) who found that only 3% of U.S. CEOs can be considered as IT experts (when measured by IT-related degrees or prior professional experience). In contrast to the low number of managers with IT backgrounds, our sample shows somewhat stable homogeneity relative to management board members with a degree in business or economics (between 43% and 56%). Although the number of top executives with law degrees appears to decline over time in our sample firms, two of the four identified companies with a governance reaction (Deutsche Telekom and FMC) indicated that cybersecurity issues are confined to units with a focus on legal matters or functional units led by professionals with a legal background. Firms therefore seemed to consider most of the damage from a CSI to be predominantly on the legal side. In other words, IT incidents appeared more liable to be treated as failures of compliance rather than technical security issues that put a firm's business model at risk. In the case of Deutsche Telekom, a new management board position was created following the CSI in 2008. Responsibility for security was then rapidly transferred from the manager in charge of IT (an executive with an engineering background) to that of the new board position headed by a lawyer with no specific IT expertise. Likewise, FMC extended the responsibilities of their compliance department that continued to be run by an executive without specific IT skills. Treating the CSIs as a compliance issue, it is interesting that both firms happened to be the only German blue chips breached that were simultaneously listed on the U.S. stock exchange at the time of the incidents. This suggests that the changes observed may have been the result of greater pressure from both regulatory bodies and investors in the United States. In light of the low number of German management board members with an educational background in IT science, our findings do not enable us to either confirm or reject previous studies suggesting that top executives' IT skills determine a firm's response to CSIs (Haislip et al., 2017; Vincent et al., 2019).

A fourth result is that the German companies analyzed seemed to avoid discussing IT-related weaknesses and incidents in their annual reports. Only one firm (Beiersdorf) explicitly mentioned the CSI in their documentation (without presenting any concrete post-incident measures). We assume that the lack of clear communication on CSIs is due to two factors: fear of negative reactions after disclosing such incidents and a lack of adequate methodologies to quantify the damage. Both explanations support former research on stock market reactions following the disclosure of CSIs (Campbell et al., 2003; Johnson et al., 2017) and the difficulty of quantifying the impact of any post-incident actions taken due to a lack of data (Kvochko and Pant, 2015). In addition, we observed that when companies do react to incidents, their responses seem to be driven by legal motives such as underlying lawsuits rather than concerns about reputation. Even though CSIs cost huge amounts in remediation actions, lead to a loss of both reputation and competitive advantage, and entail other legal consequences, German firms appear to fail to quantify and communicate the consequences of the CSIs adequately to their stakeholders. Our results confirm the recent findings of a survey conducted by McAfee (2020) according to which most organizations have no plans in place to prevent or respond to CSI incidents, and those that do mostly develop action plans without involving their executives or the board of directors.

To sum up, and with regard to our research question, our findings do not allow us to confirm any changes in the composition or scope of responsibilities on German management boards in response to CSIs. Accordingly, we indirectly confirm Upper Echelons Theory in that the relative stability of top executive teams after experienced IT incidents does not lead to substantial changes in strategic measures with respect to IT-related risk management. In addition, our qualitative analysis shows that the few companies that did undertake visible measures tend to treat CSIs at top executive level as a legal rather than an operational issue, as reflected by the structure of business units and related responsibilities.

6. Conclusion

Given the growing rise in IT-related incidents that particularly concern multinational groups, we have addressed the research question of how far CSIs impact management board composition as well as the profiles and responsibilities of their members. Based on Upper Echelons Theory, our study offers for the first time for Germany an in-depth analysis of top management teams in the country's blue-chip companies regarding their reactions on CSIs and, therefore, contributes to the application of UET in the area of security governance. The following four main findings are eminent Firstly, our results confirm the increasing trend in the frequency of CSIs, the percentage of German firms that publicly disclose IT-related incidents yet being comparatively low. Secondly, and contrary to previous research in the U.S. (Higgs et al., 2016; Haislip et al, 2017; Vincent et al., 2019), CSIs do not seem to engender major changes at executive level in German companies, thereby suggesting regulations to be the central driver for adjustments to management boards following such incidents. Thirdly, top managers of German firms that experienced CSIs almost never have an IT background, but frequently hold higher education degrees in business administration and law. Accordingly, IT-related incidents seem to be handled by German managers more under a juridical angle and appear to be considered as failures of compliance rather than technical security issues. Finally, German companies seem to avoid both disclosing and discussing CSIs in their annual reports which seems to be due to fears of negative reactions as well as difficulties to quantify the damage of such incidents.

Considering our findings, two practical contributions may be noted. The first relates to the fact that despite the public's growing interest in the topic of CSIs, external communication and documentation of German companies on IT-related incidents seems to be relatively limited, possibly due to the absence of any national or European equivalent to S-OX 404 or SEC compliance requirements.[2] Accordingly, the analysis of corporate documentation alone does not give investors a clear picture of CSI risks and their potential outcomes, and therefore is insufficient as a tool to strengthen managerial monitoring. As a consequence, policy designs regarding official documentation requirements should be adapted to further promote and value transparency, since both the disclosing company and its stakeholders benefit from improved corporate communication.

The second implication emanates from the observation that German firms tend to handle IT security predominantly as a legal matter in the aftermath of CSIs. In addition, top executives appear to delegate - maybe due to fear of legal consequences or other personal risk dispositions - accountability to lower operational levels instead of accepting it as a management board concern. By doing so, firms not only downplay the strategic relevance of such incidents but also limit themselves to manage the (juridical and technical) consequences rather than focussing on prevention through strategic planning and a proactive risk management policy. Given the growing damage potential of CSIs, however, it is in the companies' interest to use all their governance instruments to avoid such issues from happening while assuring an effective reaction in case they do. Consequently, IT-related risk management must be located at and proactively directed by the management board which puts the focus on aspects such as the representation of the topic of cybersecurity in the different areas of responsibility as well as the

[2] While ESMA guidelines require European listed firms to disclose a specific risk report including cyber risks since 2019, when such quantifications cannot be provided, these guidelines allow companies to limit their assessment to a qualitative description of the risk.

profile of top executives with respect to IT expertise. Given these considerations, our study provides some evidence that German blue-chip companies need to anchor both pre- and post-management of IT-related incidents more firmly at their management board level.

7. Limitations and Further Research

A first limitation of our study concerns the availability of data on the CSIs experienced during our observation period. In spite of the general understanding that the Internet, by definition, never forgets, public search engines tend to select more recent information with high click rates. Older news from websites with lower visiting rates (that automatically suffer further from the steadily growing number of internet users) therefore tend not to show up. Moreover, modern corporate communication policies are usually based on search engine optimization designed to bring favorable news to the fore rather than reputation-damaging information. As a consequence, even high impact IT incidents may not be published or will only have low visibility, complicating exhaustive identification of CSIs, or even making it infeasible and contingent on chance. We assume that this issue is also a factor in the relatively low number of IT-related problems we identified for German blue-chip companies. The fact that 15 of the 19 IT incidents (78.9%) occurred in 2015 or later supports this point. Further adding to the problem of information asymmetry, and in contrast to the regulatory requirements in the U.S., European firms are not obliged to disclose CSIs at present. Consequently, pressure on European executives to take appropriate measures with respect to IT-related incidents and thus protect investors remains rather limited. That said, we believe that the lack of strict disclosure requirements significantly hampered the detection of IT material weaknesses in our sample firms. Our analysis only focused on externally visible measures taken after the disclosure of a CSI, but we are well aware that internal responses to incidents are possible without any form of public communication, particularly when the actions are limited to levels not covered by disclosure requirements. Such reactions may be similar to the one identified in our analysis of FMC (2017, p. 84), where the incident led to the creation of a new operating unit within an existing department, completed by a team of internal IT specialists.

Alongside this limited availability of data on CSIs, unobserved variables may explain the absence of noticeable changes on German management boards in response to CSIs. Several scholars have thus demonstrated that factors such as experience in IT firms (Masli et al., 2016; Haislip and Richardson, 2018), board members' individual style (Qu, 2020), CEOs' reputation (Francis et al., 2008), ''superstar CEOs'' (Koh, 2011), overconfidence (Schrand and Zechman, 2012) and even a manager's facial structure (Jia et al., 2014) or their off-the-job behavior (Davidson et al., 2013) can also determine organizational outcomes. Given that our analysis only takes the directly observable characteristics of executives such as age, gender, tenure and educational background into account, these aspects may not be sufficient proxies to evaluate CSI risks in German groups, or how such incidents are likely to be handled. Consequently, extending the set of variables to cognitive aspects might be helpful in future surveys since cognitive bias, especially with regard to IT security, can play a decisive role in decision-making.

Beside insufficient communication about CSIs, corporate disclosure about the characteristics of German top managers, particularly with respect to their profile and skills, still appears to be limited or even non-existent. This issue was addressed several years ago by Prinz and Schwalbach (2014) who noted that German blue-chip companies do not usually justify the appointment of new executives from a competency perspective, restricting communication on their skills and professional expertise, partially due to reasons of confidentiality. Even though we cross-checked data from corporate annual reports with publicly available information, it is highly likely that the profiles of the executives from our sample companies are incomplete. Stronger disclosure requirements with respect to management board member profiles, and particularly their professional skills, would be a substantial help in advancing research on the link between a management board's IT expertise and CSIs.

Since the European Securities and Monitoring Authority (2019) published its new guidelines on (cyber) risk reporting, there is good reason to believe that the latter will compel companies to disclose IT-related incidents more frequently, as well as present any subsequent governance measures to their

stakeholders. That said, a first analysis of the 2019 annual reports of CAC 40 companies listed in France shows that firms almost exclusively use qualitative metrics and focus their explanations of governance measures at the level of the Chief Information Security Officer (Georg-Schaffner et al., 2021), while failing to demonstrate substantial changes in governance tools and decision-making teams. As regulatory and fiscal/accounting authorities such as ESMA also work to protect the value of intangibles, information in the form of valuable data is central to this challenge, and the literature has already indicated several measures that can help such data to be quantified (Laney, 2017). Consequently, once the asset value of information can be determined, both loss and damage to these assets will be more visible, making cybersecurity (incidents) a quantifiable metric for organizational performance and hence corporate governance. Further research can help to develop this aspect and contribute to clearer insights into the impact of corporate governance strategies on CSIs, thereby improving the way they are handled in the digital age.

References

Abatecola, G., Mandarelli, G., & Poggesi, S. (2013). The personality factor: how top management teams make decisions. A literature review. *Journal of Management and Governance*, *17*(4), 1073-1100. https://doi.org/10.1007/s10997-011-9189-y

Abatecola, G., & Cristofaro, M. (2018). Hambrick and Mason's "Upper Echelons Theory": evolution and open avenues, *Journal of Management History*, *26*(1), 116-136. https://doi.org/10.1108/JMH-02-2018-0016

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost of privacy breaches? An event study. *Proceedings of the 3rd International Conference on Information Systems*, Milwaukee, WI.

Akey, P., Lewellen, S., & Liskovich, I. (2018). Hacking corporate reputations. *Working paper*. Retrieved May 5, 2019, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143740.

Auden, W. C., Shackman, J. D., & Onken, M. H. (2006). Top management team international risk management factor and firm performance. *Team Performance Management, 12*(7/8), 209-224. https://doi.org/10.1108/13527590610711778

Aytes, K., Byers, S., & Santhanakrishnan, M. (2006). The economic impact of information security breaches: Firm value and intra-industry effects. *12th Americas Conference on Information Systems (AMCIS) Proceedings (Paper 399)*, 3305-3312.

Banker, R. D., & Feng, C. (2019). The impact of information security breach incidents on CIO turnover. *Journal of Information Systems*, *33*(3), 309-329. https://doi.org/10.2308/isys-52532

Bantel, K. A., & Jackson, S. E. (1989). Top management and innovations in banking: Does the composition of the top team make a difference? *Strategic Management Journal*, *10*(1), 107-124. https://doi.org/10.1002/smj.4250100709

Bédard, J., Chtourou, S., & Courteau, L. (2004). The effect of audit committee expertise, independence, and activity on aggressive earnings management. *Auditing: A Journal of Practice & Theory,* 23(2), 13-35. https://doi.org/10.2308/aud.2004.23.2.13

Benaroch, M., & Chernobai, A. (2017). Operational IT failures, IT value destruction, and board-level IT governance changes. *MIS Quarterly*, *41*(3), 729-762. https://doi.org/10.25300/MISQ/2017/41.3.04

Bertrand, M., & Schoar, A. (2003). Managing with style: The effect of managers on firm policies. *The Quarterly Journal of Economics*, *118*, 1169-1208. http://dx.doi.org/10.1162/003355303322552775

Bose, I., & Leung, A. C. M. (2014). Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems, 64*, 67-78. https://doi.org/10.1016/j.dss.2014.04.006

Blustein, D., Walbridge, M., Friedlander, M., & Palladino, D. (1991). Contributions of psychological separation and parental attachment to the career development process. *Journal of Counseling Psychology*, *38*, 39-50. https://doi.org/10.1037/0022-0167.38.1.39

Campbell K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448. https://dl.acm.org/doi/10.5555/876661.876669

Carpenter, M. A., & Fredrickson, J. W. (2001). Top management teams, global strategic posture, and the moderating role of uncertainty, *Academy of Management Journal, 44*(3), 533-545. https://doi.org/10.2307/3069368

Certo, S. T., Lester, R. H., Dalton, C. M., & Dalton, D. R. (2006). Top management teams, strategy and financial performance: A meta-analytic examination. *Journal of Management Studies, 43*(4), 22-2380. https://doi.org/10.1111/j.1467-6486.2006.00612.x

Cook, D. J., Mulrow, C. D., & Haynes, R. B. (1997). Systematic reviews: Synthesis of best evidence for clinical decisions. *Annals of Internal Medicine, 126*(5), 376-380. https://doi.org/10.7326/0003-4819-126-5-199703010-00006

Cooper, H. (1998). *Synthesizing research* (3rd ed.). Sage Publications.

Cyert, R. M., & March, J. G. (1963). *A behavioral theory of the firm.* Prentice-Hall.

Davidson, R., Dey, A., & Smith, A. (2013). Executives' ''off-the-job'' behavior, corporate culture, and financial reporting risk. *Journal of Financial Economics, 117*(1), 5-28. https://doi.org/10.1016/j.jfineco.2013.07.004

Denyer, D., & Tranfield, D. (2008). Producing a systematic review. In D. Buchanan (Ed.), *The S++age handbook of organizational research methods* (pp. 671-689). Sage.

Dezsö, C. L., & Ross, D. G. (2012). Does female representation in top management improve firm performance? A panel data investigation. *Strategic Management Journal*, *33*(9), 1072-1089. https://doi.org/10.1002/smj.1955

European Commission. (2016). *The Directive on security of network and information systems (NIS Directive*).

European Parliament & Council (2016). *Directive 95/46/EC General Data Protection Regulation*. 2016/679.

European Union Agency For Network And Information Security ENISA (2016). *The cost of incidents.*
German Stock Corporation Act.

Fang, C., Kim, J.-H. J., & Milliken, F. J. (2014). When bad news is sugarcoated: Information distortion, organizational search and the behavioral theory of the firm. *Strategic Management Journal, 35*(8), 1186-1201. https://doi.org/doi:10.2307/24037305

Finkelstein, S., & Hambrick, D. C. (1996). *Strategic leadership: Top executives and their effects on organizations*. St. Paul, West. https://doi.org/10.2307/259414

Francis, J., Huang, A. H., Rajgopal, S., & Zang, A. Y. (2008). CEO reputation and earnings quality. *Contemporary Accounting Research, 25*, 109-147. https://doi.org/10.1506/car.25.1.4

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review, 13*(1), 61-83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

Ge, W., Matsumoto, D., & Zhang, J. (2011). Do CFOs have style? An empirical investigation of the effect of individual CFOs on financial reporting practices. *Contemporary Accounting Research, 28*, 1141-1179. https://doi.org/10.1111/j.1911-3846.2011.01097.x

Georg, L. (2017). Information security governance: Pending legal responsibilities of non-executive boards. *Journal of Management and Governance*, *21*(4), 793-814. https://doi.org/10.1007/s10997-016-9358-0

Georg-Schaffner, L., Behnam, E., & Pallud, J. (2021). Cyber risk disclosure: How transparent are CAC40 companies in their annual reports?, submitted to *Association of Information Management Conference 2021*.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly, 41*(3), 703-727. https://doi.org/10.25300/MISQ/2017/41.3.03

Gordon, A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, *34*(3), 567-594. https://doi.org/10.5555/2017470.2017479

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

Haislip, J. Z., Masli, A., Richardson, V. J., & Sanchez, J. M. (2016). Repairing organizational legitimacy following information technology (IT) material weaknesses: Executive turnover, IT expertise, and IT system upgrade, *Journal of Information Systems, 30*(1), 41-70. https://doi.org/10.25300/MISQ/2017/41.3.04

Haislip, J. Z., Lim, J.-H., & Pinsker, R. (2017). Do the roles of the CEO and CFO differ when it comes to data security breaches, *Twenty-Third Americas Conference on Information Systems, Boston*, 1-10.

Haislip, J. Z., & Richardson, V. J. (2018). The effect of CEO IT expertise on the information environment: Evidence from earnings forecasts and announcements, *Journal of Information Systems, 32* (2), 71-94. https://doi.org/DOI:10.2308/isys-51796

Hambrick, D. C. (2007). Upper echelons theory: An update. *Academy of Management Review, 32*(2), 334-343. https://doi.org/10.2307/20159303

Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: The organization as a reflection of its top managers. *Academy of Management Review, 9*(2), 193-206. https://doi.org/10.2307/258434

Hambrick, D. C., & Snow, C. C. (1977). A contextual model of strategic decision making in organizations in: R. L. Taylor, M. J. O'Connell, R. A. Zawacki, & D.D. Warrick (Eds.), Academy of Management Proceedings, 109-112.

Hartmann, M. (2007). *Eliten und Macht in Europa - Ein internationaler Vergleich*. Campus.

He, C. Z., Frost, T., & Pinsker, R. E. (2020). The impact of reported cybersecurity breaches on firm innovation. *Journal of Information Systems*, *34*(2), 187-209. https://doi.org/10.2308/isys-18-053

Higgs, J.-L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016), The relationship between board-level technology committees and reported security breaches, *Journal of Information Systems*, *30* (3), 79-98. https://doi.org/10.2308/isys-51402

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. http://www.jstor.org/stable/2781022

Hurtz, G., & Donovan, J. (2000). Personality and job performance: The big five revisited. *Journal of Applied Psychology*, *85*, 869-879. http://dx.doi.org/10.1037/0021-9010.85.6.869

Jarvenpaa, S. L., & Ives, B. (1991). Executive involvement and participation in the management of information technology. *MIS Quarterly, 15*(2), 205-227. https://doi.org/10.2307/249382

Jia, Y., Lent, L., & Zeng, Y. (2014). Masculinity, testosterone, and financial misreporting. *Journal of Accounting Research 52*(5), 1195-1246. https://doi.org/10.1111/1475-679X.12065

Johnson, M. S., M. J. Kang, & Lawson, T. (2017). Stock price reaction to data breaches. *Journal of Finance Issues, 16*(2), 1-13.

Judge, T., Erez, A., & Bono, J. (1998). The power of being positive: The relationship between positive self-concept and job performance. *Human Performance, 11*, 167-187. http://dx.doi.org/10.1080/08959285.1998.9668030

Kearns, G. S., & Sabherwal, R. (2007). Antecedents and consequences of information systems planning integration. *IEEE Transactions on Engineering Management, 54*(4), 628-643. https://doi.org/10.1109/TEM.2007.906848

Koh, H., & Boo, E. (2001). The link between organizational ethics and job satisfaction: A study of managers in Singapore. *Journal of Business Ethics, 29*, 309-324. https://doi.org/10.1023/A:1010741519818

Koh, K. (2011). Value or glamour? An empirical investigation of the effect of celebrity CEOs on financial reporting practices and firm performance. *Accounting and Finance 51*, 517-547. https://doi.org/10.1111/j.1467-629X.2010.00357.x

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

Kvochko, E., & Pant, R. (2015). Why data breaches don't hurt stock prices. *Harvard Business Review*. Retrieved September 12, 2020, from https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

Laney, D. B. (2017). *Infonomics: How to monetize, manage, and measure information as an asset for competitive advantage*. Gartner.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review, 53*, 413-455. https://doi.org/10.1111/fire.12160

Leung, A., & Bose, I. (2008). Indirect financial loss of phishing to global market. *ICIS Proceedings*.

Li, W., Phang, S.-Y., & Ho S. Y. (2019). CEO/CFO turnover and subsequent remediation of information technology material weaknesses. *Accounting and Finance, 59*(4), 2553-2577. https://doi.org/10.1111/acfi.12299

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly, 31*(1), 59-87. https://doi.org/10.2307/25148781

Lim, J. H., Stratopoulos, T. C., & Wirjanto, T. (2013). Sustainability of a firm's reputation for information technology capability: The role of senior IT executives. *Journal of Management Information Systems 30*(1), 57-96. https://doi.org/10.2753/MIS0742-1222300102

Lok, J. (2010). Institutional logics as identity projects. *Academy of Management Journal, 53*(6), 1305-1335. https://doi.org/10.5465/AMJ.2010.57317866

Maholtra, A., & Maholtra, C. K. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research, 14*(1), 44-59. https://doi.org/10.1177/1094670510383409

March, J. G., & Simon, H. A. (1958). *Organizations*. Wiley.

Masli, A., Richardson, V. J., Weidenmier Watson, M., & Zmud, R. W. (2016). Senior executives' IT management responsibilities: Serious IT-related deficiencies and CEO/CFO turnover. *MIS Quarterly, 40*(3), 687-708. https://doi.org/10.25300/MISQ/2016/40.3.08

Michel, J. G., & Hambrick, D. C. (1992). Diversification posture and top management team characteristics. *Academy of Management Journal, 35*(1), 9-37.

Mischel, W. (1977). The interaction of person and situation. In D. Magnusson & N. S. Endler (Eds.), *Personality at the crossroads: Current issues in interactional psychology* (pp. 217-247). Erlbaum.

Naranjo-Gil, D., Hartmann, F., & Maas, V. S. (2008). Top management team heterogeneity, strategic change and operational performance. *British Journal of Management, 19*, 222-234. https://psycnet.apa.org/doi/10.1111/j.1467-8551.2007.00545.x

Neely Jr., B. H., Lovelace, J. B., Cowen, A. P., & Hiller, N. J. (2020). Meta-critiques of upper echelons theory: Verdicts and recommendations for future research, *Journal of Management*, 46(6), 1029-1062. https://doi.org/10.1177%2F0149206320908640

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

Nicholas-Donald, A., Matus, J. F., Ryu, S., & Mahmood, A. M. (2011). The economic effect of privacy breach announcements on stocks: A comprehensive empirical investigation. *AMCIS 2011 Proceedings - All submissions*. 341.

Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security Applications, 19*(4), 257-271. https://doi.org/10.1016/j.jisa.2014.07.001

Prinz, E. (2010). *Les effets des liens personnels interconseils sur la performance de l'entreprise: Une analyse comparée entre France et Allemagne*. Peter Lang.

Prinz, E., & Schwalbach, J. (2014). 10 Anmerkungen zur laufenden Debatte um Aufsichtsräte. *Der Aufsichtsrat*, 10, 138-140.

Purvis, R. L., Sambamurthy, V., & Zmud, R. W. (2001). The assimilation of knowledge platforms in organizations: An empirical investigation. *Organization Science, 12*(2), 117-135. https://doi.org/10.1287/ORSC.12.2.117.10115

Qu, C. T. (2020) Board members with style: The effect of audit committee members and their personal styles on financial reporting choices, *Journal of Accounting, Auditing & Finance, 35*(3), 530–557. https://doi.org/10.1177/0148558X17752804

Raithel, S., & Schwaiger, M. (2015). The effects of corporate reputation perceptions of the general public on shareholder value. *Strategic Management Journal, 36*(6), 945-956. https://doi.org/10.1002/smj.2248

Rockart, J. F. (1988). The line takes the leadership: IS management in a wired society. *Sloan Management Review, 29*(4), 57-64.

Schrand, C., & Zechman, S. (2012). Executive overconfidence and the slippery slope to financial misreporting. *Journal of Accounting & Economics 53*, 311-329. https://doi.org/10.1016/j.jacceco.2011.09.001

Securities and Exchange Commission (2018). Commission statement and guidance on public company cybersecurity disclosures. Release Nos. 33-10459; 34-82746.

Sharma, R., & Yetton, P. (2003). The contingent effects of management support and task interdependence on successful information systems implementation. *MIS Quarterly, 27*(4), 533-555. https://doi.org/10.2307/25148789

Smith, T. J., Higgs, J. L., & Pinsker, R. E. (2019). Do auditors price breach risk in their audit fees? *Journal of Information Systems, 33*(2), 177-204. https://doi.org/10.2308/isys-52241

Stern, I., & James, S. D. (2016). Whom are you promoting? Positive voluntary public disclosures and executive turnover. *Strategic Management Journal, 37*(7), 1413-1430. https://doi.org/10.1002/smj.2393

Vincent, N. E., Higgs, J. L., & Pinsker, R. E., (2019). Board and management-level factors affecting the maturity of IT risk management practices, *Journal of Information Systems*, *33*(3), 117-135. https://doi.org/10.2308/isys-52229

Wally, S., & Baum, R. J. (1994). Personal and structural determinants of the pace of strategic decision making. *Academy of Management Journal, 37*(4), 932-956. https://doi.org/10.2307/256605

Wang, G., Holmes Jr., R. M., Oh, I.-S., & Zhu, W. (2016). Do CEOs matter to firm strategic actions and firm performance? A meta-analytic investigation based on upper echelon theory. *Personnel Psychology, 69*, 775-862. https://doi.org/10.1111/peps.12140

Wiersema, M. F., & Bantel, K. A. (1992). Top management team demography and corporate strategic change. *Academy of Management Journal, 35*(1), 91-121. https://doi.org/10.2307/256474

Winkler, H. J., Rieger, V., & Engelen, A. (2020), Does the CMO's personality matter for web traffic? Evidence from technology-based new ventures. *Journal of the Academy of Marketing Science, 48* (2), 308-330. https://doi.org/10.1007/s11747-019-00671-9

Xu, H., Guo, S., Haislip, J. Z., & Pinsker, R. E. (2019). Earnings management in firms with data security breaches. *Journal of Information Systems, 33*(3), 267-284. https://doi.org/10.2308/isys-10715

Additional sources:

BBC News (2016). *Deutsche Telekom fault affects 900,000 customers*. Retrieved May 3, 2019, from https://www.bbc.com/news/technology-38130352

Beiersdorf (2021). *A Propos*. Retrieved January 6, 2021, from https://www.linkedin.com/company/beiersdorf

BMW Group (2021). *BMW Group History*. Retrieved January 6, 2021, from https://www.bmwgroup-classic.com/en/history.html

Center for Strategic & International Studies (2020): *The Hidden Costs of Cybercrime*. Retrieved January 18, 2021, from, https://www.csis.org/analysis/hidden-costs-cybercrime

CybersecurityVentures (2018). *2019 Official Annual Cybercrime Report*. Retrieved January 4, 2021, from

https://www.prnewswire.com/news-releases/cyberattacks-are-the-fastest-growing-crime-and-predicted-to-cost-the-world-6-trillion-annually-by-2021-300765090.html

Deutsche Telekom (2020). *Interim Report Q3 2020*. Retrieved February 15, 2021, from https://report.telekom.com/interim-report-q3-2020/management-report/group-organization-strategy-and-management.html

Deutsche Telekom (2021). *Facts and Figures*. Retrieved January 6, 2021, from https://www.telekom.com/en/company/details/facts-and-figures-355192

Finance Magazin (2018). *Beiersdorf trennt sich von CFO Jesper Andersen*. Retrieved October 1, 2019, from https://www.finance-magazin.de/cfo/cfo-wechsel/beiersdorf-trennt-sich-von-cfo-jesper-andersen-2010151/

Fresenius Medical Care (2021). *Investors Operating Figures*. Retrieved February 6, 2021, from https://www.freseniusmedicalcare.com/en/investors/operating-figures/

Godden, M. (2017). *Low Energy - E.ON hit with IT failures leaving frantic customers unable to access their accounts or pay their bills online*. Retrieved May 20, 2019, from https://www.thesun.co.uk/news/3694254/eon-it-failures-customers-unable-to-access-accounts-online/

Greenberg, A. (2016). *A New Wireless Hack Can Unlock 100 Million Volkswagens*. Retrieved July 6, 2019, from https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/

Health and Human Services, Department of (2018a). *Resolution agreement and corrective action plan*. Retrieved June 14, 2019, from http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/FMCNA/index.html.

Health and Human Services, Department of (2018b). *Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules*. Retrieved June 14, 2019, from https://www.hhs.gov/about/news/2018/02/01/five-breaches-add-millions-settlement-costs-entity-failed-heed-hipaa-s-risk-analysis-and-risk.html

Hodges, J. (2019). *E.ON Switches All U.K. Customers to 100% Renewable Power*. Retrieved October 1, 2019, from https://www.bloomberg.com/news/articles/2019-07-09/eon-switches-millions-of-u-k-customers-to-100-renewable-power

Kaspersky Lab (2016). *Measuring Financial Impact of IT Security on Businesses*. Retrieved October 1, 2019, from https://media.kaspersky.com/.../kaspersky-it-security-risks-report-2016.pdf

Kovacs, E. (2017). *NotPetya Attack Costs Big Companies Millions*. Retrieved July 5, 2019, from https://www.securityweek.com/notpetya-attack-costs-big-companies-millions

Kutscher, J. (2017). *M-Trends 2017: A View From the Front Lines. Mandiant*. Retrieved February 26, 2021, from https://www.fireeye.com/blog/threat-research/2017/03/m-trends-2017.html

McAfee (2021). *Risk Based Security (2021). 2020 Year End Report - Data Breach QuickView*. Retrieved February 6, 2021.https://pages.riskbasedsecurity.com/en/en/2020-yearend-data-breach-quickview-report

Stubbs, J., & Polityuk, P. (2017). *Cyber Attacks Cripple Companies Worldwide*. Retrieved September 30, 2019, from https://www.huffpost.com/entry/cyber-attacks-europe_n_595270c5e4b0da2c731ead25?ncid=engmodushpmg00000006

Williams, M. (2015). *BMW cars found vulnerable in Connected Drive hack*. Retrieved September 30, 2019 from https://www.pcworld.com/article/2878437/bmw-cars-found-vulnerable-in-connected-drive-hack.html

Declarations:

Funding: Not applicable
Conflicts of interest/ competing interests: Not applicable
Availability of data and material: Public
Code availability: Not applicable