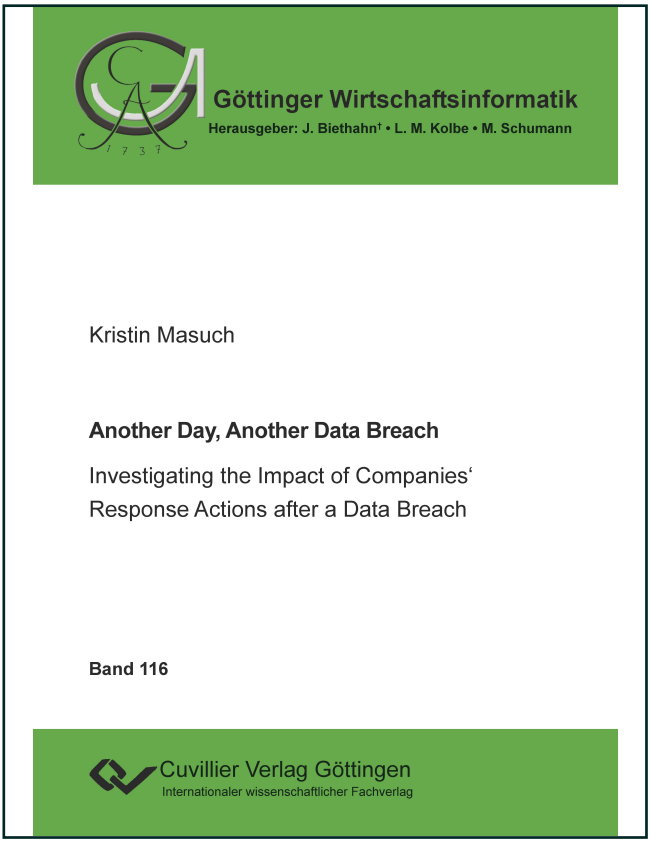
Kristin Masuch (Autor)

Another Day, Another Data Breach

Investigating the Impact of Companies‘ Response Actions after a Data Breach



https://cuvillier.de/de/shop/publications/8673

Copyright:
Cuvillier Verlag, Inhaberin Annette Jentzsch-Cuvillier, Nonnenstieg 8, 37075 Göttingen, Germany
Telefon: +49 (0)551 54724-0, E-Mail: info@cuvillier.de, Website: https://cuvillier.de

A. Introduction and Foundations

The first part of the dissertation lays out the basis and state of the art of the research conducted, comprising five parts that demonstrate the topic's relevance, as well as defines and delineates the terminology used, research background, literature gaps, and research questions addressed. It concludes with a summary of how the four studies answer the research questions.

In the first section (A.I.), the topic's motivation and relevance are described, followed by the overarching research question to be answered. Subsequently, the dissertation's overall aim is stated.

In the second section (A.II.), the research topic is classified and delimited regarding its content. The terminology used continuously in the research is highlighted, defined, and contextualized.

The third section (A.III.) presents the literature streams and their findings that inform the topic of data breach response. First, a summary of the literature on the economic aspects of security incidents is presented, highlighting which factors are relevant to the present research. Second, an overview of the literature on service failure recovery points out trends and their underlying impact. Finally, a summary of previous data breach response literature findings is provided.

In the fourth section (A.IV.), the dissertation's framework is derived from extant literature. For this purpose, detailed research questions are presented based on literature gaps.

In the fifth section (A.V.), the research studies are summarized. In doing so, it is outlined which study addresses which research question, with explanations on how each study's results help close the research gap. In conclusion, the chapter provides an overview of the study's key findings and key contributions and facts about study type, influence variable, data, sample, context, and analytical approach.

I. Relevance

In recent years, the increase in the number of digital processes within companies and the associated dependence on the Internet have led to disruptive changes in the business world associated mainly with the sharp rise in collecting and storing sensitive data (e.g., Kraus et al. 2021; Nadkarni and Prügl 2021). On one hand, rapid growth in data volumes contains high value for companies, but on the other hand, it also carries high risks (e.g., Piccoli et al. 2018; Schlackl et al. 2022), manifested in increasing numbers of security incidents (e.g., Cavusoglu et al. 2004; Ponemon Institute 2021; Schlackl et al. 2022; Verizon Business 2015; Whitman 2004). Former Federal Bureau of Investigation (FBI) Director Robert Mueller III described the emerging problem back in 2012:

"There are only two types of companies:
those that have been hacked and those that will be" (Barnes 2018).

Over half of United States (U.S.) Chief Executive Officers (CEO) similarly have expressed extreme concern about these developments, ranking security concerns as the single biggest threat to their companies (PwC 2020). In particular, security managers have assessed the problem of security incidents affecting data confidentiality, so-called data breaches, as the most critical issue on the security incident front (Dhillon et al. 2021). Therefore, prevention and detection of data breaches, as well as management of data breach consequences, have become a priority for these managers (Schlackl et al. 2022), particularly because the costs from a data breach are high and have been increasing for years (e.g., Gatzlaff and McCullough 2010; Kannan et al. 2007; Ponemon Institute 2021). Without countermeasures, the damage from a data breach can lead to losses that can threaten a company's very existence.

The damage and thus the cost-causing factors are multifaceted (Ponemon Institute 2021), with initial costs incurred after the discovery of a data breach (Ponemon Institute 2021). As a specific security incident, data breaches are characterized explicitly by a breach of confidentiality of the affected data (Dadhich 2020). Data integrity and availability may not be compromised in this case necessarily. Since the data is usually unchanged by this type of attack, companies often register incident late. Currently, it takes an average of 287 days for a data breach to be discovered and contained. The later a data breach is identified and contained, the higher its costs are since the data can be viewed and used without obstruction for longer (Ponemon Institute 2021). Therefore, long detection and remediation with data breaches reinforces the cost problem.

After detection and restoration operations, companies must comply with disclosure requirements (NCSL 2020). Thus, due to potential direct harm to affected customers, such as identity theft (Sen and Borle 2015), companies must publicly announce data breaches (Culnan and Williams 2009; Knight and Nurse 2020), incurring costs to the company from

the announcement itself and its consequences (Ponemon Institute 2021). In particular, the costs and problems arising from the consequences of a data breach announcement are devastating and can be divided into direct costs from loss of market value (e.g., Cavusoglu et al. 2004; Goldstein et al. 2011; Gwebu et al. 2018) and indirect costs from loss of reputation and, thus, loss of customers (e.g., Goode et al. 2017; Kude et al. 2017; Ponemon Institute 2021). This can lead to layoffs of responsible managers and customer churn (e.g., Culnan and Williams 2009; Knight and Nurse 2020; Schlackl et al. 2022).

The annual "Cost of a Data Breach Report" (Ponemon Institute 2021) provides an overview of the average cost per affected company caused by data breaches. It can be used to quantify the costs of detection, notification, and the actual loss of market value or customers after a data breach. Overall, costs from data breaches have been increasing steadily (Schlackl et al. 2022), including a sharp increase in costs in the recent past. From 2020 to 2021, the average cost per affected company increased by 10%, from US $3.86 million to US $4.24 million (Ponemon Institute 2021). It should be noted that the average cost of a data breach per affected company varies across industries (see Figure 1).

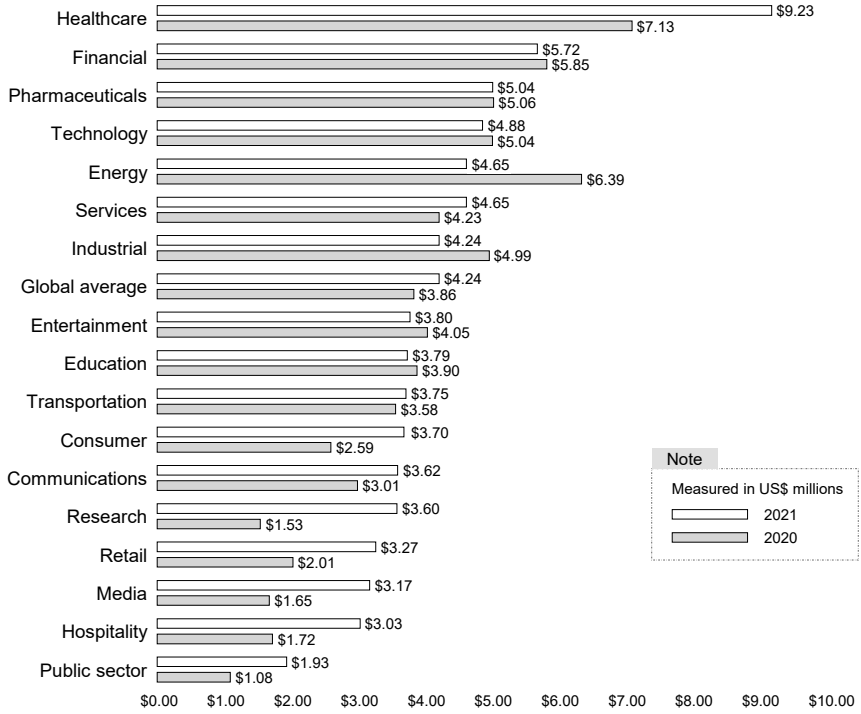


Figure 1: Average Total Cost of a Data Breach by Industry (Ponemon Institute 2021)

Companies in the critical infrastructure sector, such as healthcare and financial institutions, are particularly vulnerable, as they often handle susceptible data. For example, the healthcare industry has incurred the highest average costs after data breaches for 11 years. The overall increase in the cost of a data breach per company from 2020 (see the lower bar in Figure 1) to 2021 (see the upper bar in Figure 1) is almost three times higher in the healthcare industry, with an increase of 29.5% compared with the average value (Ponemon Institute 2021).

However, average total costs in the figure clearly indicate that companies in every industry should prevent data breaches to avoid these costs. Nevertheless, years of efforts by companies to prevent data breaches clearly demonstrate that not every data breach can be prevented (Sen and Borle 2015), which is why managing the consequences of a data breach is essential to averting significant damage to the company.

The literature also identifies these two main approaches of prevention and reaction to address data breach costs (see Figure 2) (Baskerville et al. 2014; Yue and Cakanyildirim 2007). Prevention represents operational capabilities, such as policies and safety processes (Kwon and Eric Johnson 2013). It involves implementing measures, either based on experience or quantitative predictive models, to prevent future data breaches (Baskerville et al. 2014). Preventive measures can reduce the number of data breaches significantly (Kwon and Eric Johnson 2013). Nevertheless, as mentioned above, it is virtually impossible to ensure absolute data breach prevention (Sen and Borle 2015). Consequently, the second literature stream, which focuses on the reaction after a data breach, becomes more critical. Reactive measures include the appropriate handling of data breaches after they occur because preventive measures could not prevent them. These include identification measures, restoring systems and processes to regular operation, and proper data breach communication (Ahmad et al. 2020; Goode et al. 2017; Hoehle et al. 2022; Kude et al. 2017).

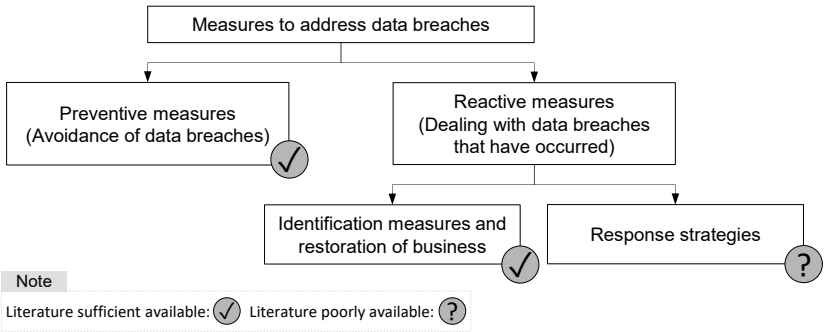


Figure 2: Main Measures for Managing Data Breaches

Extant research already has developed established mechanisms and procedures for handling a data breach within a company, providing important recommendations for detecting breaches and restoring business continuity (e.g., Ahmad et al. 2020). However, due to legal requirements for disclosure, it has become necessary to create a suitable external strategy for reacting to data breaches. It becomes clear that this is currently lacking and that research on data breach communication that provides actionable recommendations for externally communicating the breach is underrepresented (Goode et al. 2017; Hoehle et al. 2022; Kude et al. 2017).

Consequently, companies face the challenge of responding to data breaches, but lack recommendations on how best to respond to minimize consequences. Due to this lack of guidance, companies are using two cues to shape their response strategies: mandatory legal disclosure of data breaches and cost drivers after announcing data breaches. For example, the legal requirement to disclose data breaches provides initial guidance through basic guidelines on how data breaches must be announced at a minimum (NCSL 2020). Nevertheless, some ambiguity and interpretive leeway remain in legal terms, leaving open more design options. Thus, cost drivers provide more guidance on the design of response strategies by illustrating that two main cost drivers exist: direct costs due to affected market value (e.g., Chen et al. 2012; Yayla and Hu 2011) and indirect costs due to damaged relationships with customers (e.g., Sherr & Wingfield, 2011).

With the legal latitude on how to disclose a data breach and the knowledge of what causes consequences to the company, affected companies seek to use this legal latitude to design response strategies meant to reduce the negative consequences of announcing a data breach. For this purpose, response actions are added in the announcement of a data breach, which is intended to influence market value positively on one hand (Gwebu et al. 2018) and the relationship with customers on the other (e.g., Goode et al. 2017). However, systematics, uniform standards, and efficient instructions on data breach response strategies are lacking, so affected companies are choosing actions on an ad hoc and situational basis to develop response strategies without knowing whether and how these strategies impact the consequences that arise after a data breach (McKinsey 2019). This raises an overall research question (RQ):

How do response strategies following a data breach impact its consequences?

In order to answer this research question, this dissertation aims to provide recommendations for possible data breach response strategies based on how data breach response actions operate. For this purpose, the essential terminology in the context of data breach responses is defined and delineated. The research background then is highlighted to point out insights into related topics and initial findings on the data breach response literature. This overview allows the positioning of this dissertation in the literature and the derivation of detailed research questions that can inform and, thus, answer the

overarching research question. Four studies are used to address these detailed research questions, resulting in increased knowledge on how response strategies can be derived, as well as implications for data breach response literature and data breach management that companies can extract.

II. Conceptualization

A uniform conceptualization through a clear definition of a data breach and a schematization of the possible communication strategies form the basis for making meaningful recommendations on the communication of data breaches. For this reason, the terms related to data breach responses are identified and defined below.

Data breaches entail violation of data confidentiality and can be divided into categories based on the affected data: unauthorized access to either customers or employees' data (Yayla and Hu 2011). Because of its external impact, an attack on customer data can weaken customer loyalty significantly, while the loss of employee data usually elicits no noticeable consequences (Yayla and Hu 2011). Therefore, this dissertation solely focuses on data breaches that affect customer data.

In this dissertation, the term data breach refers only to customer data breaches, which are security incidents in which companies' personally identifiable customer data are compromised, resulting in a violation of data confidentiality and, thus, customers' privacy through unauthorized access (Choi et al. 2016; Culnan and Williams 2009; Hong and Thong 2013). This form of data breach often culminates in identity theft or fraud that directly impacts customers (Sen and Borle 2015). Because of this threat, companies are required by law to announce data breaches of customer information publicly (Culnan and Williams 2009; Knight and Nurse 2020). This disclosure includes a legal duty requires informing customers in an all-inclusive manner about breaches (NCSL 2020). Publicizing information about breaches entails negative news, leading to negative market value and customer relationships (e.g., Campbell et al. 2003; Chen et al. 2012; Telang and Wattal 2007; Yayla and Hu 2011). To minimize these negative impacts, companies increasingly are incorporating strategic elements, known as response strategies, into their announcements (in addition to simply fulfilling their legal obligation to inform) (Goode et al. 2017; Kude et al. 2017; Rasoulian et al. 2017). These response strategies comprise one or more response actions. Some of them can already can be observed in practice, while others are emerging (see Figure 3).

These response actions demonstrate that companies have tried to address two assets, the market value and and the relationship with the customer. First, some response actions aim to mitigate negative consequences on market value. In the past, companies often tried to mitigate the consequences by denying that the data breach occurred or blaming others *(denial and excuse*) (Gwebu et al. 2018). Denials and excuses are not linked to

any actual measures by the company and, therefore, are of passive nature (Gwebu et al. 2018).

However, these responses are no longer or are rarely practiced, based on recent data breaches, because they usually conflict with the legally enshrined obligation to publicize information (NCSL 2020). Thus, data breaches must be communicated, and third parties can be blamed only if they were at fault.

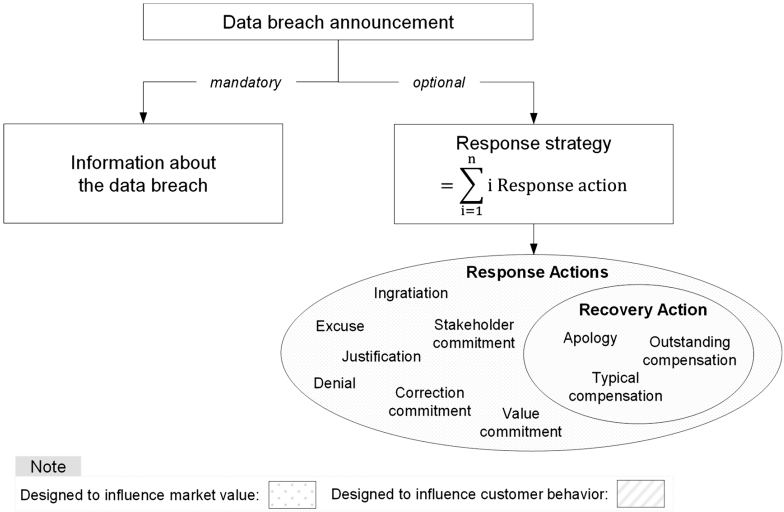


Figure 3: Conceptualization of Data Breach Response Strategies

Another response action, justification, has proven to be very popular during recent data breaches. It allows companies to publicize the necessary information, but not take any actual measures, while downplaying incidents by glossing over the actual data breaches (Gwebu et al. 2018). Some companies have intensified this whitewash by ingratiating themselves with stakeholders (*ingratiation*) (Gwebu et al. 2018).

Occasionally, more active response actions also can be observed, in which the company implements improvement measures and communicates them. As a response action, the company points to agreed-upon measures within the company designed to minimize the risk of future data breaches and to ensure the company's continuation. By making commitments, the company underpins a willingness to change and the continuity of the actions announced (*value commitment, correction commitment, and stakeholder commitment*) (Gwebu et al. 2018).

Second, some response strategies are designed to influence customer behavior (e.g., loyalty, trust, or intention to continue the relationship with the company) and, thus, the

relationship with the customer positively. These so-called recovery actions are a subcategory of response actions that target the individual customers affected. Recovery actions address aggrieved customers directly, aiming to reassure them and, therefore, stabilize and repair the relationship (Goode et al. 2017). In practice, the use of two recovery actions can be identified: apologizing to the customer regarding the data breach (*apology*) and providing compensation to the customer (e.g., *typical and outstanding compensation*). It can be observed that apologizing and typical compensation (e.g., low compensation) often are used. Outstanding compensation (e.g., high compensation) currently is used rather infrequently, but is increasing.

Finally, it should be noted that response actions without recovery actions focus on stabilizing market value and also are read and observed by customers. The same is valid for recovery actions, which are aimed at positively influencing customer behavior, but stakeholders also notice them simultaneously.

III. Research Background

The conceptualization section indicated that response actions impact market value and customer behavior. Companies affected by data breaches attempt to influence the two types of impact with different response actions.

Initial approaches can be found in the literature on data breach response strategies that describe the influences and degree of efficacy in response strategies and actions in the context of data breaches (see Section A.III.3). Two established literature streams inform these approaches. First, the literature on the economic aspects of security incidents influences the data breach response literature. This area focuses on researching the information that impacts market value. The literature investigates the influencing variables of company characteristics, type of security incident, data affected, and time horizon (see Section A.III.1). Second, the literature on service failure recovery informs the data breach response literature, addresses ways to influence customer behavior, and provides more detailed insights into the possible recovery actions apology and compensation. For this purpose, it sheds light on these recovery actions' impact on customer behavior (see Section A.III.2). Figure 4 shows which parts of these research findings contribute to the data breach response strategy literature.

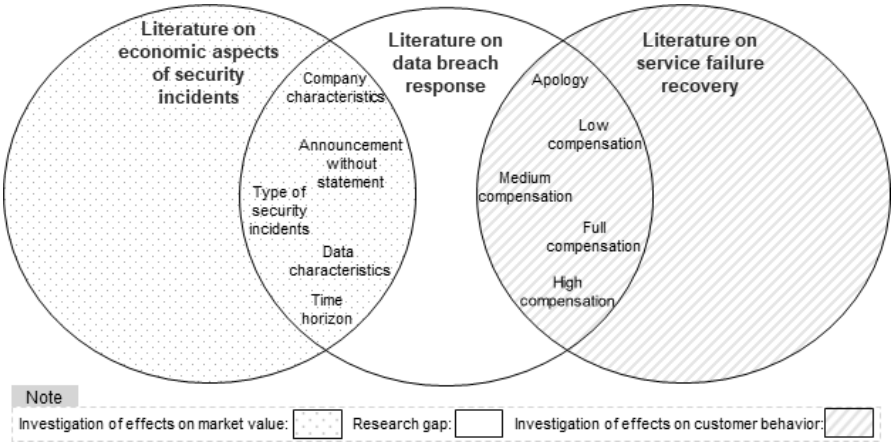


Figure 4: Overview of Research Streams that Influence the Literature on Data Breach Response

III.1 Security Incidents' Economic Aspects

The literature on security incidents' economic aspects long has focused on security incidents' impact on market value. It indicates that the announcement of a security breach significantly affects market value negatively (e.g., Cavusoglu et al. 2004; Ettredge and Richardson 2003; Garg et al. 2003; Gatzlaff and McCullough 2010; Yayla and Hu 2011; Foerderer and Schuetz 2022; Michel et al. 2020). This negative influence generally can be confirmed, but often is viewed as more differentiated (see Figure 5).

For this purpose, other characteristics that impact market value are examined in addition to the information about a security incident. It can be concluded that company characteristics change market value after a security incident (e.g., Cavusoglu et al. 2004; Hovav and D'Arcy 2003; Telang and Wattal 2007; Michel et al. 2020). For example, it has been demonstrated that security incidents strongly impact the company negatively if it is an IT-related company (e.g., Internet or technology companies) (e.g., Cavusoglu et al. 2004; Ettredge and Richardson 2003; Yayla and Hu 2011) or it is in the financial and retail sectors (Chen et al. 2012; Morse et al. 2011). Furthermore, it has been demonstrated that industry, size, and the company's growth potential influence the impact on market value negatively (Goldstein et al. 2011; Telang and Wattal 2007).

In addition to company characteristics, early research has demonstrated that the type of security incident also affects market value (e.g., Andoh-Baidoo et al. 2010; Kannan et al. 2007; Zafar et al. 2012). For example, it has been demonstrated that denial of service (DoS) attacks and credit card data breaches negatively affect market value (Ettredge and Richardson 2003; Garg et al. 2003; Hovav and D'Arcy 2003).

Some studies also have focused on security incidents that affect data availability or integrity, but no consistent picture of the impact has been established (Goldstein et al. 2011; Gordon et al. 2011; Kannan et al. 2007; Telang and Wattal 2007).

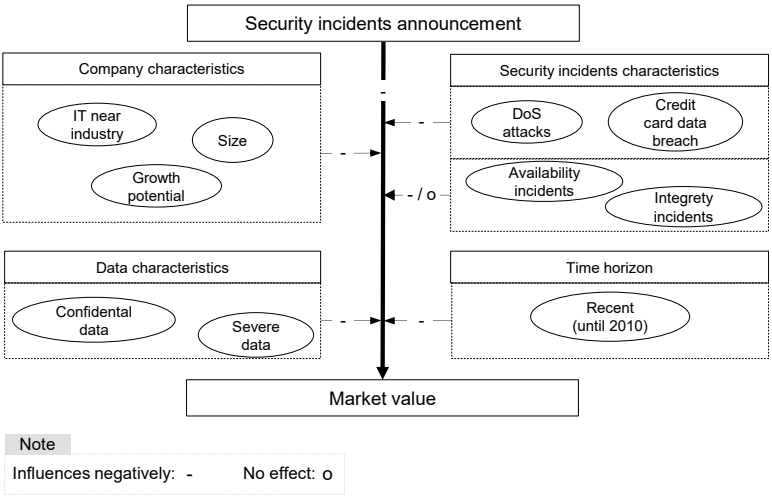


Figure 5: Economic Aspects of Security Incidents

Another characteristic has been found to impact the market value in a security incident. Based on the type of data involved, a difference in market value can be found (Campbell et al. 2003; Chen et al. 2012; Telang and Wattal 2007). It can be demonstrated that security incidents involving confidential data or large data volume in general strongly impact market value negatively (e.g., Campbell et al. 2003; Telang and Wattal 2007; Martin et al. 2017). Furthermore, a few other studies considered different time horizons in which security incidents occur, with most concluding that recent incidents make a more substantial impact on market value. Thus, security incidents are perceived more negatively over time (e.g., Gatzlaff and McCullough 2010; Hovav and D'Arcy 2004; Ko, K. M. Osei-Bryson, et al. 2009).

The literature on security incidents' econometric aspects informs this dissertation insofar as data breaches are relevant events that harm a company's market value. Different company characteristics or security incidents can trigger these adverse effects. Overall, it has become clear that all the characteristics examined in prior literature depend on the circumstances of the company or data breach and cannot be influenced by the company to change the consequences on market value.