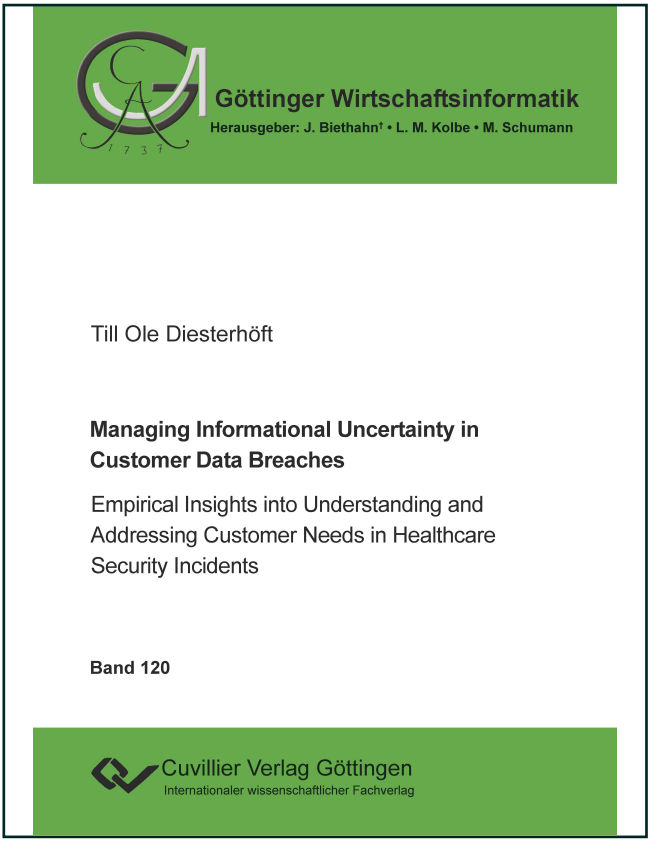
Till Ole Diesterhöft (Autor)

Managing Informational Uncertainty in Customer Data Breaches

Empirical Insights into Understanding and Addressing Customer Needs in Healthcare Security Incidents



https://cuvillier.de/de/shop/publications/9030

A. Foundations

The first part of this cumulative thesis is divided into two subsections: Section A.I, which provides an introductory overview of the thesis objectives and research agenda, and Section A.II, which summarizes and discusses research pertinent in reaching these objectives.

Section A.I motivates this research endeavor by highlighting the current state of research and its shortcomings. Building on this, five research questions (RQ) are formulated, followed by an outline of the thesis structure. The section then delves into the research positioning, including the predominant research paradigm assumed and detailing the design of this dissertation's studies. Finally, the anticipated contributions and expected implications are articulated.

Section A.II begins with an introduction to the concept of customer data breaches, discussing their unique characteristics and recognizing them as a contemporary challenge. This section proceeds to summarize approaches investigated in current research to manage these breaches, focusing primarily on the use of data breach response strategies. Although widely used by companies and extensively studied, recent literature has indicated a notable limitation of these response strategies: the risk of informational uncertainty. Informed by this observation, a review of data breach literature related to uncertainty in customer data breaches is conducted. By synthesizing these findings and adopting a risk management perspective, the section concludes by outlining potential research avenues for managing informational uncertainty.

I. Introduction

The introduction of this dissertation is organized into five distinct sections, each outlining a key aspect of the research endeavor. The first section provides the motivation for the dissertation by situating it within the current scientific discourse on customer data breaches (I.1). This is followed by the identification of research gaps, which includes two overarching and three sub-research questions (I.2). In Section I.3, the structure of the dissertation is outlined, offering a comprehensive overview of its contents. This is succeeded by a discussion on the overall positioning of the thesis (I.4). Finally, the introduction concludes with Section I.5, where the anticipated contributions and implications are presented.

I.1 Motivation

Leveraging customer data has emerged as a key driver of competitive advantage, particularly through personalization for individual customers (Chen et al. 2012; Ho et al. 2011; Lehrer et al. 2018; Xiao and Benbasat 2007). With the increasing use of artificial intelligence and its promising benefits across domains (Berente et al. 2021; Luo et al. 2019), the demand for and utility of substantial customer data are growing more than ever. However, the challenge for companies lies not only in creating value from this data but also in ensuring its security (Angst et al. 2017; Li et al. 2023). When companies fail to adequately secure customer data, customer data breaches can occur, defined as “the theft, loss, or other forms of compromise of personally identifiable information such as credit card and Social Security numbers” (Choi et al. 2016, p. 905).

Customer data breaches are increasingly recognized as one of the major challenges in the era of digitalization, negatively affecting both customers and companies (Bachura et al. 2022; Culnan and Williams 2009; Foerderer and Schuetz 2022). These incidents often lead to detrimental economic outcomes for companies (Goel and Shawky 2009; Malhotra and Malhotra 2011; Rasoulian et al. 2023). Beyond financial losses, customer data breaches also adversely impact customer behavior, for instance by decreasing customer spending and service usage, increasing switching behavior, and inducing the spread of negative word-of-mouth (Janakiraman et al. 2018; Martin et al. 2017; Turjeman and Feinberg 2023). Indeed, recent reports emphasize that the average cost of a data breach per company, encompassing both tangible and intangible expenses, has reached an all-time high of USD 4.45 million (Ponemon Institute 2023). Consequently, managing these customer data breaches becomes of utmost importance (Khan et al. 2021).

While preventive measures against data breaches are crucial and should be rigorously implemented (Baskerville et al. 2014; Li et al. 2023), no system is immune to all threats, and total prevention may not always be possible (Gwebu et al. 2018; Rainer et al. 1991;

Wang et al. 2013). Consequently, in addition to striving for prevention, a key aspect of managing customer data breaches is how companies respond to customers affected by a breach of their data (Choi et al. 2016). In light of this, literature has been investigating how companies can react to these incidents, exploring data breach response strategies[1] such as compensations (Kude et al. 2017; Wang et al. 2022), apologies (Bansal and Zahedi 2015; Bentley and Ma 2020; Masuch, Greve, and Trang 2021), and corrective actions (Nikkhah and Grover 2022). Collectively, these studies indicate the vital role of response strategies in effectively managing customer data breaches, crucial for restoring customer trust and limiting negative customer behaviors (Bansal and Zahedi 2015; Nikkhah and Grover 2022).

However, recent research has introduced a limitation in the application of data breach response strategies that could potentially diminish their effectiveness or even result in adverse effects (Goode et al. 2017; Hoehle et al. 2021, 2022). These studies examine response strategies through the lens of customer expectations, placing the focus on customer needs. They posit that customers form specific expectations regarding a company's response, which are then evaluated against the actual response (Goode et al. 2017; Hoehle et al. 2022). While it is unsurprising that negative effects emerge when a company's response falls short of customer expectations, findings also reveal that exceeding these expectations can paradoxically lead to more adverse customer behavior (Goode et al. 2017; Hoehle et al. 2022). This phenomenon is argued to primarily stem from an information gap; customers feel uncertain about the accuracy or completeness of the information provided by the company (Hoehle et al. 2022).

For example, when a data breach at a company happens, a customer might expect a free one-month credit monitoring service. If these expectations are surpassed, say with a 24-month credit monitoring offering, Hoehle et al. (2022) argue that customers "[…] may become suspicious that some information and procedures about the breach were hidden and not communicated truthfully" (Hoehle et al. 2022, p. 302). Hence, this suspicion is triggered by the discrepancy between 'what the company publicizes about the breach' and 'what the customer believes happened in the breach.' Consequently, a perceived information gap arises between the customers' understanding of the data breach and the information conveyed or indicated by the company's response. As this information gap may lead to uncertainty about the data breach's nature (Goode et al. 2017; Hoehle et al. 2022), and given that the necessary information is either concealed or not readily accessible for customers (Bachura et al. 2022), this phenomenon will henceforth be

[1] In line with existing literature, this dissertation views data breach response strategies as those strategies that companies incorporate into their data breach notifications (Nikkhah and Grover 2022). Consequently, response strategies form a part of the communication process between a company and its customers, initiated following the occurrence of a customer data breach (Choi et al. 2016; Gwebu et al. 2018).

termed *informational uncertainty*. This novel insight casts a different light on previously investigated response strategies, thus demonstrating that informational uncertainty is a critical factor, which has hitherto been overlooked in managing customer data breaches.

Emerging research further enriches the understanding of this informational uncertainty, highlighting its potential negative impact on customer behavior and emphasizing it as a risk that companies must address. Specifically, aspects of informational uncertainty have been linked to increased customer anxiety (Bachura et al. 2022), diminished intentions to continue using a company's services (Madan et al. 2023), and reduced repurchase intentions (Chatterjee et al. 2019). In investigating customer reactions to a data breach, Bachura et al. (2022) identified that the absence of detailed information about a data breach fosters uncertainty, which, in turn, provokes customer anxiety. Moreover, when customers are worried about the occurrence of future data breaches at the same company, their intentions to continue using the company's services can diminish (Madan et al. 2023). This is argued to stem from apprehensions about the possibility of subsequent breaches compromising the customer's data again (Madan et al. 2023), reflecting informational uncertainty regarding the company's internal data management practices. Furthermore, the uncertainty perceived can be amplified by the customer's own fears over the breach situation, potentially leading to reduced repurchase intentions (Chatterjee et al. 2019). Overall, these findings underscore that informational uncertainty, if unmanaged or unaddressed by companies, can trigger negative customer behavior and thus represents a significant risk to their business operations.

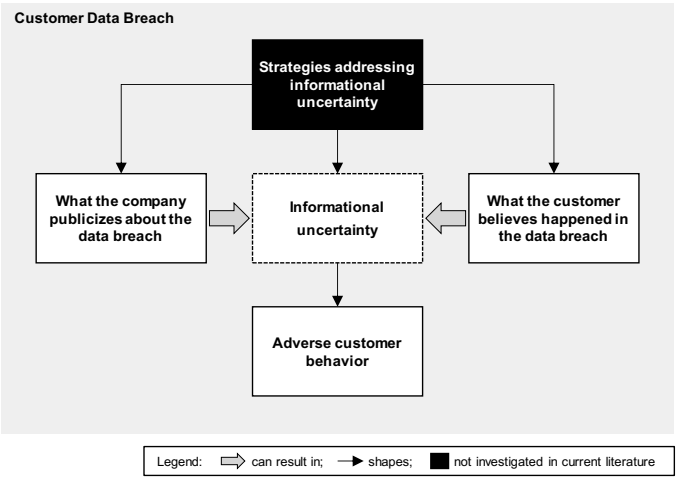


Figure 1. Identifying Strategies to Manage Informational Uncertainty

The review of current literature emphasizes the critical role of informational uncertainty in shaping customer behavior following a data breach. This understanding highlights the need for companies to develop effective strategies to manage this risk and mitigate its negative impacts. However, although research on customer data breaches acknowledges the detrimental role of informational uncertainty as well as its impact on the efficacy of response strategies, a notable gap remains in specifically addressing this aspect of data breach management (see Figure 1). Identifying strategies to manage informational uncertainty can not only help alleviate negative consequences on customer behavior but also provide insights into the dynamics of response strategies, thereby contributing to a deeper understanding of the domain of customer data breaches and their effective management.

By adopting a risk-based perspective to informational uncertainty and by assuming a positivist stance, this dissertation seeks to fill this void in existing research by empirically identifying strategies to manage informational uncertainty in the context of customer data breaches. In pursuit of this goal, it specifically utilizes the risk management framework developed by Hardy and Maguire (2016) and Hardy et al. (2020) to explore three distinct approaches in navigating the risk of informational uncertainty. The primary aim is twofold: to advance the theoretical understanding of customer data breach management and to provide actionable strategies that aid practitioners in effectively addressing customers' informational uncertainty.

I.2 Research Gaps and Research Questions

This thesis aims to contribute to the existing discourse on managing customer data breaches. The investigation involves synthesizing knowledge from related literature, as well as identifying strategies for managing the risk which stems from the informational uncertainty that customers experience in data breaches. The first objective of this dissertation is to analyze related literature for potential ways that could manage this risk. Following this, three risk management approaches are explored to determine their potential application in addressing the risk of informational uncertainty.

Research dedicated to managing the adverse consequences associated with customer data breaches — such as decreased customer spending and service usage, increased switching behavior, and the spread of negative word-of-mouth (Janakiraman et al. 2018; Martin et al. 2017; Turjeman and Feinberg 2023) — primarily concentrates on so-called response strategies (Choi et al. 2016; Goode et al. 2017). These strategies aim to mitigate the damage to customer-business relationships when notifying customers about the occurrence of a data breach (Hoehle et al. 2022). Recent literature has explored various response strategies, including compensating affected customers (Goode et al. 2017; Hoehle et al. 2022), assuming responsibility by apologizing (Bentley and Ma 2020;

Masuch, Greve, and Trang 2021), or announcing which corrective actions will be or have been taken (Nikkhah and Grover 2022).

However, a critical observation in this domain, as indicated by recent studies (see Cram and Mouajou-Kenfack 2023; Diesterhöft et al. 2020), is the prevalence of one-way communication in these strategies, where companies inform customers about the breach and respond to them but do not facilitate customer interaction. Therefore, strategies investigated in the current literature and applied in practice often adopt a unidirectional approach, thus potentially neglecting the significance of including customer perspectives (see Goode et al. 2017; Hoehle et al. 2021, 2022). Yet, in diverse fields such as Information Systems (IS) (Kohler et al. 2011; Winkler and Wulf 2019), marketing (Edvardsson et al. 2011; Grönroos and Voima 2013), and management (Corsaro 2019; Frow et al. 2015), customers have shifted from having a passive to an active role, which has catalyzed substantial positive changes. Today's customers not only anticipate but also expect to be actively involved in processes and in co-creating value (Prahalad and Ramaswamy 2000). Involvement in these processes grants customers a sense of control over how their input shapes the final outcomes (Vargo and Lusch 2004).

Building on this, the service literature underscores that active customer involvement in recovering from service failures leads to positive outcomes, such as increased satisfaction (Dong et al. 2008; Van Vaerenbergh et al. 2018). Through these approaches, customers transcend beyond being mere recipients of corporate communication; they can become integral collaborators in shaping recovery outcomes (Roggeveen et al. 2012; Xu, Marshall, et al. 2014). Given that data breaches are regarded a specific type of service failure (Goode et al. 2017; Hoehle et al. 2022; Malhotra and Malhotra 2011; Nikkhah and Grover 2022), leveraging co-creation principles from service recovery literature has considerable potential. First, empowering customers to co-create solutions, e.g., deciding on the type of compensation, could significantly help to diminish their perceived informational uncertainty following a data breach. This uncertainty reduction can be attributed to the increased customer involvement as well as their influence and control over the outcomes and processes (Bakhsh 2019; Hazée et al. 2017; Jia and Wang 2016; Park and Ha 2016). Second, this customer-centricity provides individuals with the autonomy to shape outcomes that more accurately reflect their needs and perspectives (Guo et al. 2016; Hazée et al. 2017; Joosten et al. 2017). This alignment could, therefore, potentially optimize the effectiveness of current data breach response strategies. As a result, it is crucial to review the related literature of co-creation in service recovery and identify opportunities for the field of data breach management:

> **RQ 1:** What insights from co-creation in service recovery can be applied to enhance data breach response strategies?

While current literature prioritizes organizational response strategies to data breaches, it is this very response that introduces significant uncertainty for affected customers—a critical challenge that must be managed with care (see Astvansh et al. 2023; Bachura et al. 2022; Chatterjee et al. 2019; Madan et al. 2023). Information surrounding a data breach is often not clear-cut. For instance, companies are tasked with identifying a wealth of information about a data breach before disclosure, such as the nature of the data and the scope of the breach (Knight and Nurse 2020). Additionally, due to the complexity inherent in both predicting and reacting to data breaches (Jalali et al. 2019; Khan et al. 2021), companies may find themselves uncertain about the details surrounding the data breach and its potential threats (Gwebu et al. 2018).

Recent literature has indicated that these characteristics can also spill over to customers. It is highlighted that the nature of a company's response to a data breach can potentially lead customers to question whether they are receiving complete and truthful communication about the data breach and its implications (Goode et al. 2017; Hoehle et al. 2022). The resulting information gap between the company and its customers can cause negative customer behavior, fueled by doubts about the company's intentions and worries over the breach's severity (Goode et al. 2017; Hoehle et al. 2022). Such informational uncertainty not only leads customers to reevaluate their relationship with the company due to concerns about future breaches (Madan et al. 2023), but also induces anxiety in them (Bachura et al. 2022). As a result, informational uncertainty can pose a risk to the overall operations of the breached company (see Chatterjee et al. 2019; Madan et al. 2023).

This emerging body of research points to the importance of companies accounting for the risk of informational uncertainty in their data breach management practices to avoid any unintended adverse effects. Should companies fail to address this uncertainty, negative customer behavior can ensue, potentially jeopardizing the future business of the company. Therefore, identifying and implementing strategies to effectively manage the risk of informational uncertainty is not just beneficial—it is essential for restoring confidence and preserving customer relationships in the wake of a data breach:

> **RQ 2:** What strategic approaches can companies adopt to manage the risk of informational uncertainty?

Generally, companies can manage risks through three modes: prospectively, in real-time, and retrospectively (Hardy and Maguire 2016). These modes are intricately linked, each aiming to manage risks at distinct phases: before they occur, as they occur, and after they have occurred (Hardy et al. 2020). For security incidents, traditional risk management approaches that resemble these modes typically involve strategies aimed at prevention (Li et al. 2023), response (Baskerville et al. 2014), and learning from past incidents to forestall future risks (Mehrizi et al. 2022). In the following, each risk

management mode will be elucidated within the broader domain of data breach management. Subsequently, these modes will be specifically contextualized with regard to managing the risk of informational uncertainty in customer data breaches.

Prospective risk management involves strategies to minimize either the likelihood of a risk occurrence or the negative impacts if it does materialize (Hardy and Maguire 2016). Therefore, it primarily anticipates and preempts potential future consequences (Hardy et al. 2020). Specifically, in the realm of data breaches, prospective management encompasses two key aspects. First, measures can be designed to prevent the incident itself, for instance by implementing account control measures (Baskerville et al. 2014). Second, strategies can be developed with the aim of mitigating the adverse impacts following a breach, such as intrusion detection systems (Cavusoglu et al. 2005). In this research domain, considerable emphasis is placed on developing robust preventive technical approaches, including monitoring and encryption, to thwart data breaches (Khan et al. 2021).

However, while these measures are crucial, they largely focus on the technical aspects of safeguarding and securing data and systems. Little is known about leveraging prospective approaches to manage non-technical risks of these incidents, including customers' informational uncertainty. Identifying such strategies could provide companies with options to mitigate the negative effects induced by this uncertainty. For instance, decreasing the potential magnitude of informational uncertainty prospectively could result in less negative customer behavior (see Bachura et al. 2022; Madan et al. 2023). Initial evidence of the success of a similar prospective mechanism is provided by Martin et al. (2017), who demonstrate that customer sentiment can be positively influenced following a data breach when companies offer transparency and control before such an incident occurs. This notion is further corroborated by studies examining the financial impacts of data breaches, which underscore that resources in place prior to a data breach can be effectively utilized to mitigate negative stakeholder reactions in its aftermath (Modi et al. 2015; Rasoulian et al. 2023). Hence, this leads to the formulation of the following research question:

> **RQ 2.1:** How can prospective risk management be leveraged to address the risk of informational uncertainty?

Real-time risk management involves strategies to tackle risks as they unfold (Hardy and Maguire 2016). It includes companies employing a responsive approach to mitigate both ongoing and imminent risks (Hardy et al. 2020). Typically, this mode of risk management capitalizes on pre-established plans and protocols aimed at addressing and neutralizing risks as they emerge, centering on present occurrences (Hardy and Maguire 2016). In instances of security incidents like data breaches, this encompasses, for example, internal operations such as identification, containment, eradication, and recovery (Ahmad

et al. 2020). Moreover, in cases where customer data is compromised, companies are legally required to notify the affected customers (Culnan and Williams 2009; Nikkhah and Grover 2022). As emphasized earlier, optimizing these notifications through dedicated response strategies has been a focal interest in data breach research (Choi et al. 2016; Goode et al. 2017; Masuch, Greve, and Trang 2021).

Much of this academic literature stream on response strategies to customer data breaches stresses a tactical approach targeting customer outcomes (Bansal and Zahedi 2015; Choi et al. 2016). The primary focus lies on accommodative strategies designed to mitigate adverse repercussions, such as decreasing negative word-of-mouth and switching behavior, or increasing positive customer behavior, such as continuance intention and satisfaction (Goode et al. 2017; Kude et al. 2017; Nikkhah and Grover 2022). Hence, companies are frequently advised to have response strategies ready, for instance, offering compensation or apologies.

However, although informational uncertainty has been indicated to be a driver of negative customer behavior (Bachura et al. 2022; Hoehle et al. 2022; Madan et al. 2023), the real-time management of this uncertainty remains an area that has not yet been thoroughly addressed. This omission is particularly significant since feelings of uncertainty have been identified in related literature as a key antecedent of leading customers to not engage in a business relationship (Al-Natour et al. 2020; Pavlou et al. 2007). Therefore, the importance of developing and refining real-time strategies that directly address and manage the risk of informational uncertainty in a customer data breach becomes even more pronounced:

> **RQ 2.2:** How can real-time risk management be leveraged to address the risk of informational uncertainty?

The third mode is retrospective risk management. In this mode, strategies implemented during both prospective and real-time management phases are reviewed and analyzed (Hardy et al. 2020). This involves critically revisiting past actions, assessing alternative measures or approaches that could have been taken (Hardy and Maguire 2016). The eventual goal is to derive improvements, such as best practices, which can enhance current risk management strategies (Hardy et al. 2020). In the broader domain of security incidents, one approach involves companies closely examining past incidents. This review aims to provide insights into how to enhance their risk management strategies for similar situations in the future (Ahmad et al. 2020; Mehrizi et al. 2022).

In the context of informational uncertainty, this implies that companies are able to analyze the causes and progression of this uncertainty, as well as to evaluate the effectiveness of strategies aimed at mitigating it. However, given the personal nature of informational uncertainty in customer data breaches (see Bachura et al. 2022; Chatterjee et al. 2019;

Madan et al. 2023), merely conducting a routine analysis may not suffice to unravel the mechanisms of informational uncertainty in previous risk management efforts. Especially the fundamentally different expectations that customers have towards companies' actions and responses (Goode et al. 2017; Hoehle et al. 2022) call for customizing such analyses on an individual or, at least, less abstract level. Consequently, it becomes imperative to explore how companies can retrospectively reflect on the progression of informational uncertainty. Identifying methods and strategies that can delve into the subtleties of this uncertainty allows for a more comprehensive understanding of this phenomenon, thus enhancing the efficacy of future risk management strategies. Against this background, the following research question is formulated:

> **RQ 2.3:** How can retrospective risk management be leveraged to address the risk of informational uncertainty?

To provide a clearer understanding of the scope of this discussion, Figure 2 provides an overview of the research questions, the associated literature domains, and their interdependencies.

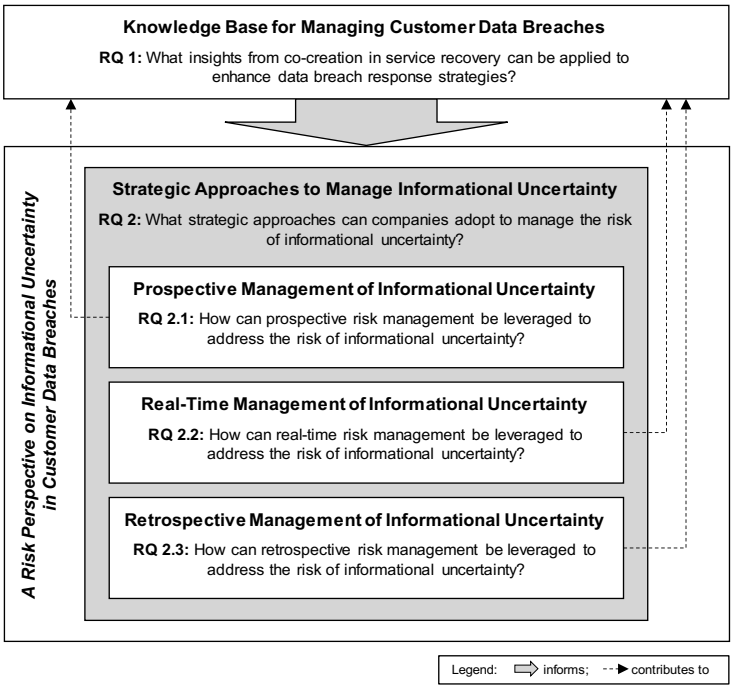


Figure 2. Dissertation Research Framework