The Role of Uncertainty in Data Breach Response Processes - A Reactance Theory Perspective

Till Ole Diesterhöft
University of Goettingen, tillole.diesterhoeft@uni-goettingen.de

Saskia Isabel Schweneker
University of Goettingen, s.schweneker@stud.uni-goettingen.de

Kristin Masuch
University of Goettingen, kristin.masuch@uni-goettingen.de

Aycan Aslan
Georg-August-Universität Goettingen, aycan.aslan@uni-goettingen.de

Marvin Braun
University of Goettingen, marvin.braun@uni-goettingen.de

Recommended Citation

Diesterhöft, Till Ole; Schweneker, Saskia Isabel; Masuch, Kristin; Aslan, Aycan; and Braun, Marvin, "The Role of Uncertainty in Data Breach Response Processes - A Reactance Theory Perspective" (2022). *ICIS 2022 Proceedings*. 11.
https://aisel.aisnet.org/icis2022/security/security/11

The Role of Uncertainty in Data Breach Response Processes - A Reactance Theory Perspective

Completed Research Paper

Till Ole Diesterhöft
University of Goettingen
Humboldtallee 3, 37073 Goettingen, Germany
tillole.diesterhoeft@uni-goettingen.de

Saskia Isabel Schweneker
University of Goettingen
Humboldtallee 3, 37073 Goettingen, Germany
s.schweneker@stud.uni-goettingen.de

Kristin Masuch
University of Goettingen
Platz der Goettinger Sieben 5, 37073 Goettingen, Germany
kristin.masuch@uni-goettingen.de

Aycan Aslan
University of Goettingen
Humboldtallee 3, 37073 Goettingen, Germany
aycan.aslan@uni-goettingen.de

Marvin Braun
University of Goettingen
Humboldtallee 3, 37073 Goettingen, Germany
marvin.braun@uni-goettingen.de

Abstract

Data breaches lead to inherent uncertainty among customers due to the compromise of information and its potential consequences for customers, e.g., identity theft or credit card misuse. Previous research has focused on outcome-based strategies to address these negative impacts. However, informed by reactance theory, we argue that customers feel a loss of control due to the induced uncertainty and that companies need to tackle these impacts. We test our hypotheses in two empirical studies. The results of Study 1 suggest that data breaches indeed lead to an increased perception of uncertainty among customers. Study 2 examines to what extent the establishment of control can mitigate the negative uncertainty effects. We highlight that by providing customers with control, companies can reduce the degree of uncertainty and increase satisfaction with the response. By conceptualizing choice as a catalyst for perceived control, we offer practitioners a novel strategy for responding to data breaches.

Keywords: Data breach response, reactance theory, perceived control

Introduction

Leveraging digitized information between customers and companies has become one of the most prominent drivers for the success and sustainability of service models in recent years (Lehrer et al. 2018; Yoo et al. 2012). Yet, apart from emerging opportunities, accumulated data may be subject to external as well as to internal malicious and inadvertent violations of security, resulting in the emergence of customer data breaches (Bansal and Zahedi 2015; Choi et al. 2016; Janakiraman et al. 2018). In turn, the ever-increasing occurrence and cost of customer data breaches (Ponemon Institute 2021; Seh et al. 2020) has been shown to require a multitude of organizational response capabilities, such as internal forensic activities, containment actions, and implementation of future-oriented preventive measures (Ahmad et al. 2021; West-Brown et al. 2003). While most of these capabilities address the intra-organizational response to data breaches (Ahmad et al. 2020; Baskerville et al. 2014), the data breach notification depicts the first point-of-contact to surrounding customers (Jackson et al. 2019; Janakiraman et al. 2018). Notifications constitute a part of the communicative data breach response process, hereafter referred to as the data breach response process, in which the company and the customer interact. In this interaction, it is also possible for customers to approach the company (Confente et al. 2019), thus establishing a dynamic process. In contrast to the broader internal response to a data breach, this response process refers to all directly customer-related activities that are conveyed through various means of communication (e.g., Hoehle et al. 2022; Goode et al. 2017).

In these notifications, customers are informed that their data has been compromised, for example by external attackers, and is no longer under the company's control (Foerderer and Schuetz 2022; Janakiraman et al. 2018). Due to the unstable state of information in the event of a data breach, customers usually receive notifications that are characterized by uncertainty and ambiguity. For instance, T-Mobile notified its customers in August 2021 and wrote that they "*recognize that many are asking exactly what happened. While we are actively coordinating with law enforcement on a criminal investigation, we are unable to disclose too many details*" (T-Mobile 2021). In addition to this lack of clarity regarding potential further negative consequences, customers are confronted with risks that remain vague. For example, the compromised information, such as financial data or social security numbers, can be used by third parties to commit identity theft or credit card misuse (Choi et al. 2016; Kim and Kwon 2019). Hence, customers lose the ability to manage their information provided to the company because it has fallen into the hands of a third party. As a result, customers are confronted with a certain degree of uncertainty because of the data breach (Hoehle et al. 2022).

Privacy literature suggests that uncertainty represents an elementary role in customers' evaluation of provided services (Al-Natour et al. 2020). Indeed, uncertainty is inherently associated with increased privacy and security risks (Cheng et al. 2021). Accordingly, customers evaluate this uncertainty and rely on it to ultimately decide whether to stay in a business relationship, e.g., with a service provider (Al-Natour et al. 2020; Pavlou et al. 2007). The advent of uncertainty, therefore, poses a key peril to the performance of customer-focused companies (Cheng et al. 2021). These insights indicate that the uncertainties caused by the characteristics of a data breach, such as potential misuse and loss of control over personal information, can negatively impact customers' attitudes towards the breached company, e.g., reduced customer satisfaction. Correspondingly, companies should strive to implement specific data breach responses to decrease the amount of uncertainty and, thus, lessen the adverse impact.

To respond to data breaches, extant literature has focused on an outcome-based perspective (Goode et al. 2017), in which customers are provided with compensation such as product or service offerings (Masuch, Greve, and Trang 2021). Uncertainty, however, is characterized by the inherent uncontrollability and unpredictability of future events (Pfeffer and Salancik 1978). As a result, individuals who experience uncertainty pursue control to cope with this unpleasant situation and reduce the induced loss of control (Hui and Toffoli 2002). Therefore, we argue that given the characteristics of uncertainty, a control-based, process-oriented data breach response is imperative to mitigate the uncertainty caused by a data breach.

In summary, while the existing body of knowledge explores aspects of the uncertainty caused by a data breach, an assessment of its consequences on customer perceptions has yet to be conducted. Therefore, our first research objective is to determine the effects of uncertainty related to the data breach response process. Further, the uniqueness of uncertainty, i.e., induced uncontrollability, calls for a control-based response strategy to deal with the presence of a state of uncertainty among customers. In line with this, our second research objective is to identify how control can be leveraged to respond to the uncertainty induced by data breaches. Our guiding research questions that we aim to answer with our research endeavor are:

RQ1: How does uncertainty affect the data breach response process?

RQ2: How can providing control on the customer's side reduce this uncertainty?

To answer these research questions, we integrate reactance theory as a conceptual framework. We theorize that the uncertainty induced by data breaches leads to a loss of freedom due to a decrease in control over the compromised information and future events (e.g., credit card misuse). Based on reactance theory, we hypothesize that individuals fundamentally strive to restore this freedom and that this freedom can be restored in the context of data breach responses through an alternative control, namely perceived control. Companies may utilize this lever to reduce the possible negative effects of uncertainty, i.e., loss of control and freedom.

To empirically corroborate the previously only anecdotally reported evidence of the increase in uncertainty caused by data breaches, we conducted an initial preliminary Study 1 (n=106). To additionally analyze the explicit effects of uncertainty on customers as well as the potential of perceived control to reduce uncertainty, we conducted our main Study 2 (n=354).

Our results are threefold. First, we demonstrate that data breaches do indeed lead to higher perceived uncertainty among customers. Second, building on these results, we observe with respect to **RQ1** that this uncertainty leads to lower satisfaction with a company's data breach response. Second, we identify that perceived control, conceptualized as compensation choice, can mitigate these negative consequences by establishing an alternative form of control (**RQ2**). In addition to diminishing uncertainty, we find that perceived control directly increases satisfaction with a company's data breach response. Our results provide a first indication of how uncertainty unfolds in a data breach context and the mitigating role of perceived control. Our work contributes to the literature on data breaches and informs both practitioners and researchers about the vital role of uncertainty.

Research Background

Uncertainty in Customer Data Breaches

Uncertainty refers to the inability or limited precision to predict the future occurrence of specific events (Pfeffer and Salancik 1978). This impaired prediction is due to an incomplete state of information (Pavlou et al. 2007). Prior Information Systems (IS) privacy research has demonstrated that uncertainty acts as an inhibitor in the initial engagement with and continued use of a digital good because of increased perceived privacy risks, e.g., apps (Al-Natour et al. 2020; Pavlou et al. 2007). Additionally, in the context of implementing an extensive information analysis of customer data, perceived uncertainty of users has been shown to increase customers perceived security risks (Cheng et al. 2021). These perceived risks, in turn, lead to lower participation in the information system provided. Accordingly, customer uncertainty, especially in the context of privacy risks, has been shown to take a central role in initial and subsequent user engagement. Thus, customers evaluate uncertainty in a customer-company relationship in a digital environment.

In addition to these a priori perceptions of uncertainty, recent literature indicates that leveraging customer data can also lead to uncertainty once business relationships have been established. The use of sensitive information is inherently linked to the risk of leakage through cyberattacks or flawed security practices (Goode et al. 2017; Gwebu et al. 2018). This compromise can cause data breaches, "a phenomenon that is not yet well understood but is characterized by its breadth of impact and uncertainty regarding the ultimate outcomes" (Hoehle et al. 2022, p. 315). As an increasing number of regulatory requirements are forcing companies to inform their customers about any data breach occurrences (Culnan and Williams 2009; Jackson et al. 2019), companies are not able to ignore and conceal such a breach (D'Arcy et al. 2020). Hence, customers are, ultimately, educated about the data breach and on the misappropriation of their data (Janakiraman et al. 2018).

As a result of this misappropriation, data breaches pose uncertain risks to customers, which may entail direct negative consequences (Anderson et al. 2017). Third parties with access to the sensitive customer data may misuse it through identity theft or credit card fraud (Choi et al. 2016; Culnan and Williams 2009). Indeed, the misuse of credentials and mishandling of data is reported as one of the top drivers for malicious third parties gaining access to customer information (Verizon 2021). Accordingly, data breaches cause customers to lose control over how their own data is handled and what the potential impact on them will result from the data breach. This puts customers in a position of uncertainty concerning possible future consequences and risks (Confente et al. 2019; Hoehle et al. 2022).

In addition to these potential information misuse risks, data breaches also lead to uncertainty regarding subsequent security incidents. As an internal response to data breaches, companies need to implement measures to contain and prevent further incidents, such as the incident eradication (Ahmad et al. 2021). For example, CaptureRX, an U.S. based healthcare service provider, stated in a data breach notification to its customers in February 2021 that "all policies and procedures are being reviewed and enhanced and additional workforce training is being conducted to reduce the likelihood of a similar future event" (CaptureRX 2021). From this perspective, the occurrence of security vulnerabilities can be assumed to lead to the anticipation of further data breaches within the company (D'Arcy and Basoglu 2022). As a result of ambiguous information, customers are uncertain as to whether future information exchange may be secure.

This literature stream informs our study in two aspects. First, uncertainty is revealed to be a crucial component in shaping and maintaining a customer-company relationship in a digital environment. Second, data breaches, resulting from this information exchange relationship, are identified as a possible trigger for uncertainty. This is attributable to the loss of control over information and the lack of certainty about possible subsequent security incidents. Building on this unique characteristic of data breaches, we outline the adverse effects that can arise from the emergence of uncertainty in the next chapter.

The Role of Reactance in Uncertain Events

Following a data breach, customers must cope with the knowledge that their information is out of their control for an uncertain period of time (Hoehle et al. 2022). As opposed to the customer-company relationship prior to a data breach, customers have no ability to change or remove information that has been made available to the company. Accordingly, customers are deprived of their right to initiate decisions concerning their own information. Hence, customers are restricted in the degree of freedom they enjoyed prior to the data breach. Additionally, they are unable to determine what will happen to their information or how it is (mis)used in the future. Credit card information breaches are one example of such a situation (Foerderer and Schuetz 2022). Once credit card information falls into the hands of third parties, customers must expect fraud or misuse to occur (Choi et al. 2016). The resulting loss of control is reflected in the purchase of a credit card monitoring service (Hoehle et al. 2022) or the continuous monitoring of one's own bank account. Such a loss of control is described by the reactance theory as a fundamental cause for individuals to respond adversely (Brehm and Brehm 1981). In particular, the concept of psychological reactance suggests that individuals resist when they are restricted in their freedom or control by certain events (Brehm 1966). Thus, individuals act in opposition to a loss of freedom when they experience such a loss.

Brehm and Brehm (1981) describe restrictions of freedom as all occurrences that prevent the individual from realizing a particular behavior in the same way as before the occurrence. They identify possible causes as social influences and intentional threats, but also as events that were caused unintentionally. When such threats cause individuals to feel that their freedom is being restricted, an unpleasant emotional state of reactance arises (Brehm 1966). In a customer-related context, this reactance can cause various negative consequences for a company, such as negative word-of-mouth, lower customer engagement, or hostile behavior (Amarnath and Jaidev 2021). In other words, customer reactance can lead to a deterioration of the company's situation.

Reactance, when induced in an individual, is associated with an inherent need and aspiration for restoration of lost control and freedom (Brehm 1966). Accordingly, a change in behavior arises, counteracting the impact of the original event (Bierhoff and Frey 2011). Thus, "when reactance is aroused, the motivation to engage in the behavior that has been eliminated or threatened with elimination is increased" (Brehm and Brehm 1981, p. 62). For instance, in the context of information security policies, Lowry and Moody (2015) show that while the implementation of security policies (freedom restrictions) leads to noncompliance (reactance), designing them to be more flexible with respect to employee freedom leads to less reactance. Thus, highlighting the role of control and freedom in alleviating adverse effects.

Considering the phenomenon of data breaches, the psychological reactance theory informs our understanding that the loss of freedom through uncertainty has a fundamental negative effect. This effect, however, can be mitigated by fulfilling the customer's desire to regain freedom. From this reactance perspective, companies can therefore establish a way to reduce the negative effects of a data breach by reinstating control to customers.

A Control Perspective on Responding to Data Breach Uncertainty

Based on our literature-based pre-understanding of uncertainty in data breaches we argue that data breaches lead to feelings of uncertainty among customers. This is due to the uncertain outcome of any data breach (Hoehle et al. 2022). The pervasiveness of an unstable state of information leads to a non-predictability of future events (Pfeffer and Salancik 1978). This holds with a data breach due to the leakage of information that has fallen into the hands of third parties (Culnan and Williams 2009). Companies are unable to accurately predict actual consequences. Thus, it is impractical to provide accurate information about potential misuse or future data breaches. Accordingly, customers feel a loss of control over various components, e.g., control over their own information, due to the uncertainty of the data breach. IS literature suggests that this uncertainty is particularly triggered by privacy concerns (Al-Natour et al. 2020; Pavlou et al. 2007), e.g. in the case of a data breach potential data theft. Thus, we argue that these data breach characteristics will serve as a stimulus to lead to an internal evaluation of uncertainty on the customer side. Hence, we are hypothesizing the following:

> **Hypothesis 1**: The occurrence of a data breach leads to an increase in perceived uncertainty for customers.

Informed by reactance theory, this perception of uncertainty can be expected to lead to a negative resistance effect, a so-called boomerang effect (Clee and Wicklund 1980). The boomerang effect induces an adverse change that opposes the loss of control caused by a specific negative event (Brehm and Brehm 1981). These boomerang effects can be attributed to diminishing or eliminating degrees of freedom and control over future events (Brehm and Brehm 1981). As a consequence of this dispossession of freedom, individuals strive to regain control (Amarnath and Jaidev 2021). This can lead to churn and negative attitudes if freedom is not restored by the original initiator of the negative event (Wendlandt and Schrader 2007). Thus, the corresponding boomerang effect ultimately triggers activities that are contrary to the loss of control and freedom (Clee and Wicklund 1980).

In the context of customer-related activities, various negative behavioral effects of reactance have been identified, for instance, negative word-of-mouth, reduced trust, and diminished repurchase intentions (Amarnath and Jaidev 2021; Wendlandt and Schrader 2007). Considering the findings of the data breach domain, customer satisfaction in particular could be identified as a central antecedent for these different behavioral intentions (Masuch, Greve, and Trang 2021). Accordingly, satisfaction provides an integrative perspective on all potential negative cognitive and affective customer behaviors (Chang 2006; Oliver 1980). This corresponds to the negative effects ascribed by reactance theory to the loss of control (Wendlandt and Schrader 2007). We therefore argue that in the context of data breaches, the occurrence of the boomerang effect caused by a loss of control due to the emergence of uncertainty leads to a negative attitude towards the breached company. Drawing on satisfaction as a salient predictor of these negative attitudes, we, therefore, hypothesize:

> **Hypothesis 2**: Higher perceived uncertainty leads to a decrease in customer satisfaction with the data breach response.

To reduce these negative consequences, companies would have to give customers the opportunity to regain control. Following the reactance theory, this could be, for example, the freedom initially withdrawn. However, control cannot be easily restored in the event of a data breach. Consider the information security policy example of Lowry and Moody (2015). According to the reactance theory, when companies introduce a certain policy, the demand for control and freedom against this policy arises. Organizations might repeal the policy, thereby satisfying employees' demand for control. Conversely, in the case of data breaches, the affected customer data over which control is sought is irrevocably compromised. Companies are unable to regain control because external third parties possess access to this data. Thus, customers may not be provided with control over their breached information.

However, reactance theory states that providing a control that differs from the originally eliminated control also leads to an overall better situation for an individual (Brehm 1966), e.g., breached person. The rationale behind this phenomenon is that individuals tend to focus more on the freedom they have gained and less on the control they have lost (Brehm 1966). Indeed, although the original control may not be restored, the provision of a distinct control improves the proportion of freedom to control loss (Esmark et al. 2016). As a result, to satisfy customers' demand for control, companies need to address alternative forms of control in their interaction with customers after a data breach. By influencing the belief that outcomes can be shaped and adjusted by one's own choice (Loss and Reactance 1993), perceived control represents a potentially fruitful approach in this context.

Perceived control can be characterized as the extent to which an individual believes that outcomes can be shaped to increase desired outputs and decrease undesired ones (Hinds 1998; Skinner et al. 1988). Representing an essential element of human motivation towards performing activities (Friedman and Lackey 1991), perceived control characterizes the ability to influence the environment (White 1959), the ability to modify matters in an event (Thompson 1981), and the ability to demonstrate potential individual competence (Hui and Bateson 1991). By drawing on concepts from psychology, we can describe perceived control in a customer-facing context as an element driven by the perceived level of controllability resulting from activities potentially actuated by the customer (Lacey 1979; Steiner 1979). In consumer settings control is shown to increase consumers' positive emotions and ultimately customer satisfaction (Hui and Bateson 1991; Hui and Toffoli 2002). This positive effect can be explained by the mechanism of direct influence on the achieved outcome, beneficially impacting the perceptions of the individual (Hui and Bateson 1991; Skinner et al. 1988).

These implications of perceived control, i.e., the possibility to influence an outcome of the data breach response process, are twofold in their contextualization in the data breach environment. First, the concept of perceived control provides a means to reduce uncertainty arising from data breaches. This is rooted in the loss of control by individuals over their data as well as the lack of control over potential future misuse of the breached information (Choi et al. 2016; Hoehle et al. 2022). According to the reactance theory, individuals now strive to regain this control (Brehm 1966; Brehm and Brehm 1981). In **H2**, we hypothesized that this urge to control will initially manifest in an adverse manner since the original control over the compromised data may never be restored. Nevertheless, we argue that perceived control provides a means to address an alternative dimension of control. This control is instantiated in the ability to actively participate in and contribute a decision to the data breach response process by shaping the eventual outcome. In other words, while customers' underlying desire for control is not fully satisfied (negative uncertainty effect through the loss of control over the compromised information), perceived control over the data breach response (e.g., influencing outcomes and decisions in the process) exerts a partial positive impact on customers' perceptions of the control, i.e., magnitude of perceived uncertainty.

Second, based on our reviewed related literature, we can argue that customers will be more satisfied with a companies' handling of a data breach when experiencing an increased degree of perceived control (Thompson 1981). Thus, perceived control may not only reduce lost control, but also directly affect the perception towards the data breach response itself. By enabling individuals to directly adjust the outcomes of a data breach, favorable perceptions towards these outcomes will be enhanced (Hui and Bateson 1991). Thus, the more the individual is in control over outcomes, the more likely it is that he or she will find them desirable (Hinds 1998; Skinner et al. 1988). Findings from the literature on data breaches support this relationship. For instance, Masuch et al. (2021) demonstrate that fulfilling customer expectations regarding the outcome of a data breach response will increase the overall satisfaction with the companies' data breach handling. Against this background, we pose the following two hypotheses:

> **Hypothesis 3**: Higher perceived control over the data breach response leads to a decrease in customers' perceived uncertainty.
>
> **Hypothesis 4**: Higher perceived control over the data breach response leads to an increase in customer satisfaction with the data breach response.

As perceived control represents an individual-specific psychological perception (Averill 1973), its direct manipulation is limited by natural constraints (Chang 2006). However, our study aims to disentangle the role of uncertainty by exploring ways in which it can be shaped by companies' data breach responses. In this context, we argue that the possibility to offer a choice represents a fruitful opportunity in achieving this goal. Literature on perceived control identified that granting a choice to customers and individuals is a major predecessor of customers' perceptions of control (Chang 2008; Esmark et al. 2016; Hui and Bateson 1991; Wortman 1975). Choice refers to the freedom to select alternatives instead of getting the alternative assigned externally (Botti and Iyengar 2004), or the perception that an outcome is caused by a person's own decision (Wortman 1975). Choice has the potential to positively impact psychological and behavioral outcomes (Wortman 1975). According to Averill (1973), the opportunity to have a choice depicts a fundamental part of control and, therefore, is inherently associated with the overall level of perceived control (Averill 1973). This gain of control through choice makes the outcomes appear more satisfactory to the individual (Hui and Bateson 1991; Thibaut and Walker 1975). As choice increases, control additionally enhances customers' positive emotions (Hui and Bateson 1991).

By contextualizing choice in data breaches, we leverage the concept of compensation. Compensation constitutes a response strategy to data breaches and has been extensively analyzed in data breach research in recent years (e.g., Choi et al. 2016; Goode et al. 2017; Greve et al. 2020; Gwebu et al. 2018; Hoehle et al. 2022; Masuch et al. 2021; Rasoulian et al. 2017; Wang et al. 2022). Compensation is defined as "material or immaterial payments that a customer receives in exchange for losses from a data breach" (Masuch, Greve, and Trang 2021, p. 5). Providing this type of financial redress has been shown to have a mitigating effect on the negative impacts of data breaches (Goode et al. 2017). Research suggests that offering compensation improves a company's financial situation (Rasoulian et al. 2017). In addition to this financial improvement, compensation also leads to positive reactions among customers (Choi et al. 2016). As a result of an improved outcome through compensation, customers' behavioral intentions as well as their satisfaction may be increased (Hoehle et al. 2022; Masuch, Greve, and Trang 2021). Given its central purpose in a company's response to data breaches and its inherent ability to be adapted (e.g., changing the form of compensation), we suggest that compensation is suitable for integrating choice possibilities in the context of data breaches. Given the relationship of choice to perceived control and its contextualization by compensation, we hypothesize:

> **Hypothesis 5**: The opportunity to choose a compensation leads to an increase in customers' perceived control over the data breach response.

To test the developed hypotheses, we conduct two studies. Study 1 examines how and in what form the occurrence of data breaches actually leads to an increased perception of uncertainty among customers. In Study 2, the effects of uncertainty on customer satisfaction are assessed in the context of data breaches. We further integrate perceived control and compensation choice as a means to mitigate these negative consequences. The research models for Study 1 & 2 are depicted in Figure 1.

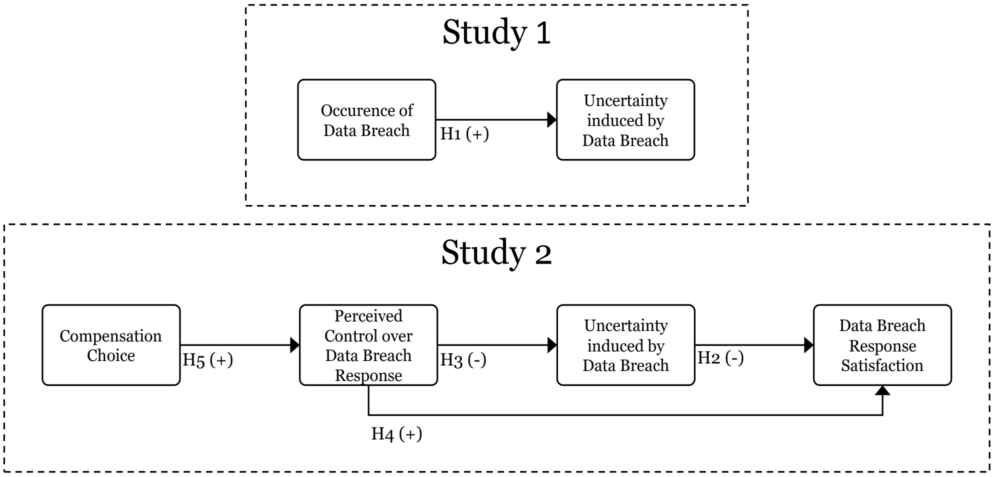

Study 1
Occurence of Data Breach
H1 (+)
Uncertainty induced by Data Breach
Study 2
Compensation Choice
H5 (+)
Perceived Control over Data Breach Response
H3 (-)
Uncertainty induced by Data Breach
H2 (-)
Data Breach Response Satisfaction
H4 (+)

Figure 1. Research Model of Study 1 and Study 2

Study 1

Research and Experimental Design

Fundamental to our research model is the assumption that data breaches lead to higher uncertainty among customers (**H1**). To empirically confirm this relationship, we conduct a preliminary Study 1. We deliberately opted to conduct the two studies separately. The rationale for this is that when evaluating perceptual changes before and after an event (e.g., data breach) within an experimental design, as is done in Study 1, a pre- and post-measurement must be conducted (Goode et al. 2017). Since these measurements may differ systematically in a vignette-study, e.g., due to a change in the perception of one of the treatments because of a pre-measurement, a bias may occur (response-shift bias). Given the inherent need for Study 2 to be a vignette-study to answer the hypotheses posed, this bias was conceivable. Accordingly, we decided to perform a preliminary study (Study 1) and a main study (Study 2).

To test the impact of the occurrence of data breaches on perceived uncertainty, we performed a digital experiment. The survey was implemented via Prolific (Palan and Schitter 2018). Information Systems (IS) research indicates that the use of this or similar platforms leads to valid and reliable random samples (Hibbeln et al. 2017; Schuetz et al. 2021). In addition, the platform's inherent link to the Internet enables us to survey individuals who have been engaged in digital experiences, such as the breach of digital information. Survey participants faced the situation of a fictitious data breach in the healthcare sector. The rationale for situating the experiment in the field of healthcare is because healthcare lies within our aim to particularly analyze personal rather than general data breaches. With its increased information sensitivity, the healthcare context offers a suitable scope for our endeavor (Kwon and Johnson 2018). Before initiating the survey, the authors calculated the required sample size. We decided to achieve the power of 0.95 with an effect size of 0.5 (Yazdanmehr et al. 2020). Using G*Power for paired, two-tailed, t-tests (Erdfelder et al. 2009), we identified that the required sample size was n=54. The experiment was conducted in 2022. To generate a consistent sample, only English-speaking, U.S. citizens were eligible to complete the survey. After analyzing the attention checks, the sample size of our first study was n = 106, thus fulfilling the calculated minimum size. The average age of participants was 44 years (SD=14.77), and the sample included 43.4% women and 54.72% men. 55% of the participants hold a bachelor's degree or higher academic degree.

The experiment started with a description of the given situation. Participants were asked to assume the role of an electronic health record (EHR)-app user. They were told that they use the app routinely to record different types of information from a range of medical practitioners. This data included personal information, such as address and name, as well as health information, such as allergies or medical history. After this introduction, the participants were faced with a breach of the EHR-app. This involved being personally contacted via mail by the company of the app. That company said it had been the victim of a cyberattack. Compromised information included health insurance ID number, medical history, as well as diagnosis information. As a response to the data breach, the company stated that each user is compensated for the cost of the app for one month. The description of the scenario and the data breach were adapted based on recent literature and practice (Masuch, Greve, and Trang 2021; Prisma Health 2019). We decided to use monetary compensation as the company's response to the data breach due to its practical and theoretical relevance (Goode et al. 2017; Hoehle et al. 2022).

To operationalize the measurement of the impact of a data breach on uncertainty, we measured uncertainty before and after the data breach. The surveyed construct of uncertainty was adapted from existing literature (see Table 1). We further incorporated attention checks, collected demographic information, and retrieved a construct for common method bias (CMB). Measurements were obtained using a 7-Likert scale ranging from strongly agree to strongly disagree.

Uncertainty (based on Pavlou et al. 2007)		**Loadings**	
		Pre-Breach	Post-Breach
Un. 1	I feel that using the EHR-app involves a high degree of uncertainty.	.972	.966
Un. 2	I feel that the uncertainty associated with the EHR-app is high.	.939	.963
Un. 3	I am exposed to many uncertainties because of the EHR-app.	.967	.948
Un. 4	There is a high degree of uncertainty because of the EHR-app.	.945	.963

Table 1. Operationalization of Uncertainty

Data Analysis & Results

Since we surveyed a latent construct, we initially assessed the indicator reliability. This reliability is given when the item loadings of a construct exceed 0.708 (Hair et al. 2021). Table 1 shows that this is given for our case. To examine the reliability of the construct, we measured Cronbach's alpha (α) and the composite reliability (CR). With the values α_{pre} = 0.969, α_{post} = 0.972, CR_{pre} = 0.977, and CR_{post} = 0.979 our construct exceeds the critical thresholds of 0.7 (Hair et al. 2021; Nunnally and Bernstein 1994). Lastly, we verified the convergent validity by means of the average variance extracted (AVE). For this to be met, a construct must explain at least half of the variance, i.e., must be above 0.5 (Henseler et al. 2009). With an AVE_{pre} of 0.914 and an AVE_{post} = 0.921 our construct also satisfies this threshold.

Considering the temporal dependency between post and pre-data breach timing, we opted to use the paired t-test. Consequently, we conducted a pairwise t-test of pre-breach uncertainty and post-breach uncertainty. The values of the pre- (M = 3.62, SD = 1.45) and post-measurement (M = 5.63, SD = 1.20) exhibit a significant difference, t(104) = 12.99, p < .001 (see Figure 2). Thus, in **support of H1**, we find empirical evidence that the event of a data breach leads to an increase in perceived uncertainty among customers.

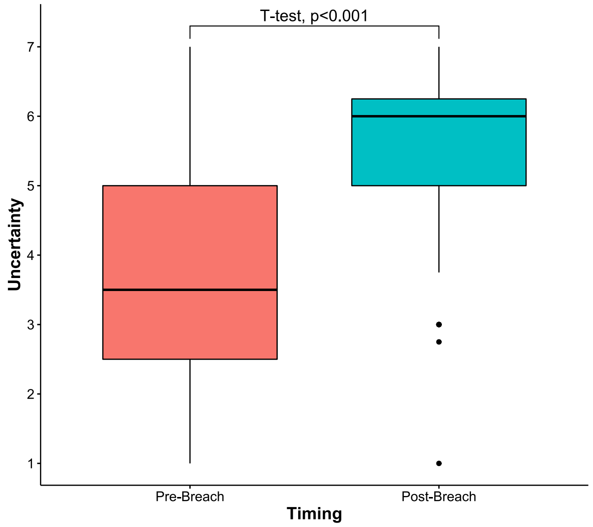


Figure 2. Boxplots of Customers' Uncertainty Before and After the Occurrence of a Data Breach

Study 2

Research and Experimental Design

Expanding on the results of preliminary Study 1, Study 2 aims to empirically validate the effects of uncertainty (control loss) in data breaches and explore the role of perceived control (control gain). As in Study 1, we conducted a digital experiment.

Study 2 was situated in the same healthcare context as Study 1. The survey was conducted in 2022 and distributed via the same platform with identical screening criteria. To calculate the required sample size, we used Kock and Hadaya's (2018) inverse square root approach. At a path coefficient of 0.2 and a confidence interval of 99%, a sample size of 251 is sufficient. After participants were discarded according to attention and manipulation checks, our sample size was n = 354. Thus, meeting the calculated sample size. The sample included 56.21% women, and 42.65% men. 62.14% hold a bachelor's degree or higher academic degree. The average age of participants was 40 years (SD = 12.95)

As in Study 1, participants were asked to put themselves in the role of an EHR app user. Hence, the introductory scenario is identical to our preliminary study. However, to manipulate perceived choice and thus perceived control of customers, a 1x2 between-subjects design was employed. The first scenario (no choice) was replicated from Study 1. Customers were offered a fixed compensation, which was provided by the EHR-app company (see Table 2). Due to the specific context of data breaches, i.e., asynchronous communication and monetary refund, compensation in particular serves as a manipulable object for control purposes. Therefore, customers were given the opportunity to make a choice of a specific compensation in the second scenario (choice) (see Table 2). The selection of compensation choice options was guided by related literature (Gabisch and Milne 2014; Hoehle et al. 2022; Masuch, Greve, and Trang 2021). Participants were randomly assigned to one of the two scenarios. Attention was paid to ensure that the compensation received had the same value in both scenarios (10 USD). Thus, unintended effects caused by a higher compensation can be excluded (see Goode et al. (2017)). Furthermore, we can establish that the financial input into the response of the company is identical in both scenarios. Therefore, establishing a similar value exchange in both experimental settings. Additionally, we incorporated the compensation from the no choice scenario into the choice scenario ("EHR-app payments") to eliminate effects regarding preferences on the provided compensation.

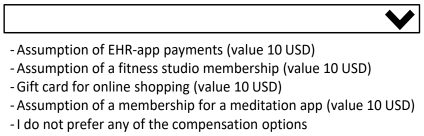
	No Choice	**Choice**
Data breach response from the EHR-app company	*"After careful consideration, we have decided to compensate you with the assumption of EHR-app payments (value 10 USD)."*	*"After careful consideration, we have decided to compensate you with one of the following options below."*  - Assumption of EHR-app payments (value 10 USD) - Assumption of a fitness studio membership (value 10 USD) - Gift card for online shopping (value 10 USD) - Assumption of a membership for a meditation app (value 10 USD) - I do not prefer any of the compensation options
Reasoning according to the reactance theory	Customers receive a **predetermined outcome** for an event that limits the individual's freedom and control.	Customers are given the **ability to choose an outcome** from a set of options for an event that limits the individual's freedom and control.
	The urge to be in control, stimulated by reactance, is not satisfied.	The urge to be in control, stimulated by reactance, is satisfied through choice options.

Table 2. Data Breach Response Scenarios

The manipulation of compensation choice was included in the model as a dummy coded binary variable (0=no choice, 1=choice) . All other hypothesis-relevant constructs were adapted based on prior literature (see Table 3). We used the same scaling as well as the same construct for uncertainty in Study 1. To assess the indicator reliability of our model, we adopted the thresholds from Study 1. Accordingly, the item loadings must be greater than 0.705. This is given for both perceived control over the data breach response (M = 2.38, SD = 1.62) and satisfaction with the data breach response (M = 2.48, SD = 1.52) as well as for uncertainty (M = 5.91, SD = 1.06) (see Table 3).

Constructs and Items		**Loadings**
Uncertainty (based on Pavlou et al. 2007)		
Un. 1	I feel that using the EHR-app involves a high degree of uncertainty.	.915
Un. 2	I feel that the uncertainty associated with the EHR-app is high.	.933
Un. 3	I am exposed to many uncertainties because of the EHR-app.	.917
Un. 4	There is a high degree of uncertainty because of the EHR-app.	.920
Perceived Control over the Data Breach Response (based on Hui and Bateson 1991 and Chang 2006)		
PC. 1	The efforts of the EHR-app gave me a sense of control over how the data breach will be resolved.	.942
PC. 2	The EHR-app allowed me to have input on the final solution to this data breach.	.960
PC. 3	I had some sense of control over how this data breach would be resolved.	.964
Satisfaction with the Data Breach Response (based on Maxham and Netemeyer 2002)		
Sat. 1	In my opinion, the EHR-app provided a satisfactory resolution to the data breach on this particular occasion.	.963
Sat. 2	Regarding this particular data breach, I am satisfied with the EHR-app.	.973
Sat. 3	I am not satisfied with the EHR-app's handling of this particular data breach incident. (reverse coded)	.960

Table 3. Operationalization of Measures

As in Study 1, we examine the composite reliability ($\alpha \geq 0.7$ and CR ≥ 0.7) and the convergent validity (AVE ≥ 0.5). Since we aim to simultaneously integrate and analyze different constructs in our research model, discriminant validity needs to be established. Discriminant validity ensures that theoretically different constructs are in fact different (Henseler 2015). In short, it assures that no correlations exist that cannot be justified by the measurement theory. In line with current IS literature, we apply the Fornell-Larcker Criterion (FL) and the heterotrait-monotrait ratio (HTMT) (Karwatzki et al. 2022; Trenz et al. 2020). The FL criterion is met if the root of an AVE of a construct is larger than the correlation with all other constructs in the model (Fornell and Larcker 1981). The HTMT also analyzes the similarity between different latent variables, it is considered fulfilled if the values are below 0.85 (Henseler et al. 2015). Table 4 demonstrates that composite reliability, convergent reliability, and discriminant validity are established, indicating a robust model. We additionally tested for the occurrence of a CMB in our research model. By drawing on Chin et al. (2013), we performed the measured latent marker variable approach with a predefined marker construct. Our results indicate that a CMB is not present for our study.

	AVE	α	CR	PC.	Un.	Sat.	CC.
PC.	0.952	0.969	0.913	**0.956**	0.508	0.711	0.363
Un.	0.941	0.957	0.849	-0.482	**0.921**	0.607	0.166
Sat.	0.963	0.976	0.932	0.681	-0.578	**0.965**	0.099
CC.	n/a	n/a	n/a	0.353	-0.097	0.163	**n/a**

PC. = Perceived Control, Un. = Uncertainty, Sat. = Satisfaction, FL criterion highlighted in bold, HTMT shaded grey, CC. = Compensation Choice

Table 4. Correlation Analysis and Construct Validation

Data Analysis & Results

Having assessed the reliability and validity of our measurement characteristics, we tested our research model using the partial least squares structural equation modeling (PLS-SEM) approach. PLS-SEM is gaining considerable attention in the recent years in the IS literature (Guo et al. 2021; Ostermann et al. 2020; Schuetz et al. 2021; Yazdanmehr et al. 2020). We opted for PLS-SEM based on two aspects. First, our study aims at identifying relationships rather than pinpointing their magnitude (Goodhue et al. 2012). Second, our model consists of complex relationships between constructs, supporting the application of PLS-SEM (Hair et al. 2019). We used SmartPLS 3.3.3 for data analysis (Ringle et al. 2015). The bootstrapping resampling method with 10000 subsamples was used (Hair et al. 2021).

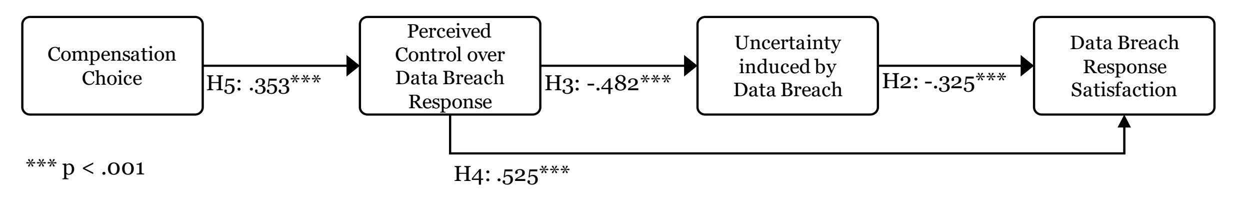

Compensation Choice
H5: .353***
Perceived Control over Data Breach Response
H3: -.482***
Uncertainty induced by Data Breach
H2: -.325***
Data Breach Response Satisfaction
H4: .525***
*** p < .001

Figure 3. Structural Model Results

Figure 3 reports the results of our structural model. Our control variables include age, gender, ethnicity, and EHR experience. We identified significant paths from age on perceived control (β = .209, p < .001), and age on uncertainty (β = -.126, p < .001). A significant negative effect is observed between perceived uncertainty and customer satisfaction (β = -.325, p < .001). In other words, customers who perceive the data breach as more uncertain are more dissatisfied with the company's response. Consequently, lending **support to H2** and highlighting the impact of the evaluations of uncertainty of customers on the response (**RQ1**). Moreover, we find a negative significant effect of perceived control on uncertainty (β = -.482, p < .001). Accordingly, an increase in perceived control in a data breach response context leads to a reduction in perceived uncertainty (**RQ2**). Thus, providing empirical **support for H3.** We further hypothesized that customers experience higher satisfaction when they sense increased perceived control. We find **empirical evidence for this assumption (H4)** in the significant positive effect of perceived control on satisfaction (β = .525, p < .001). The design of the response strategy (choice and no-choice) exhibits a significant impact on control (β = .353, p < .001). Consequently, we demonstrate that providing a choice in the data breach context leads to higher perceived control, **supporting H5**. The structural model explains 54.3% of the variance in satisfaction, 23% of the variance in uncertainty, and 12.2% of the variance in perceived control. We further assessed the effect size f^2, i.e., the change in the explained variance of a latent variable after omitting a specific predecessor (Hair et al. 2021). The effect size is close to medium for choice on control ($f^2 = .143$), medium for control on uncertainty ($f^2 = .303$), and uncertainty on satisfaction ($f^2 = .178$), and large for control on satisfaction ($f^2 = .466$). A post-hoc analysis further shows that perceived control, in addition to its direct positive effect, also exerts a positive mediation effect through uncertainty on satisfaction (Perceived Control → Uncertainty → Satisfaction: $\beta = .157$, $p < .001$). By alleviating the negative effect of uncertainty on satisfaction and increasing satisfaction through its own positive direct effect, perceived control yields a positive total effect ($\beta = .682$, $p < .001$).

Discussion

Although uncertainty is an inherent aspect of data breaches with respect to the compromised customer information, little empirical work has been conducted on its impact on customers. Informed by psychological reactance theory, the objective of this study was to investigate the role of uncertainty in the data breach response process and to fill this void. In two empirical studies, we first confirmed the impact of data breaches on uncertainty and subsequently investigated its differential effects on customers and companies.

Theoretical Contributions

Our study offers several contributions to literature and theory. First, our work reveals that the perceived uncertainty can have negative effects on established business relationships between companies and their customers. In this regard, recent data breach literature has identified that customers exhibit profoundly individualized expectations and perceptions towards the company's response (Hoehle et al. 2022; Masuch, Greve, and Trang 2021). If these customer expectations are surpassed or underperformed, negative effects can arise (Goode et al. 2017). Uncertainty, viewed as a subjective and customer-specific construct, offers a novel view for why such divergent demands for a company's response arise. Our findings suggest that higher perceived uncertainty leads to lower satisfaction with the firm's response to the data breach. Accordingly, a higher perceived uncertainty can be argued to simultaneously lead to higher expectations regarding the company's response. Thus, we offer a first explanation for ambiguous findings in prior research.

Second, by integrating perceived control and reactance theory, we introduce a new perspective on a company's response strategy to data breaches. While previous literature has focused on outcome-based responses, such as providing compensation (Kude et al. 2017), offering an apology (Chan and Palmeira 2021; Masuch, Greve, Trang, et al. 2021), or promising to introduce new security measures (Gwebu et al. 2018), providing perceived control provides an alternative effort. We show that customers seek control in data breaches and that this control helps them be more positive towards a company's response. This can be explained in particular by the unique nature of data breaches, which leads to a loss of control due to unleashed uncertainty. We thus provide a first approach to analyze and design response strategies not only at the outcome-based level, but also at the process level of outcome involvement.

Third, we contribute to the privacy and security literature by revealing that uncertainty affects not only engagement and continuance (Al-Natour et al. 2020; Pavlou et al. 2007), but also disengagement of business relationships between customers and companies. As a result of stolen user information, data breaches lead to uncertainty regarding future risks, e.g., misuse of the data or other security incidents (Choi et al. 2016). According to our findings, customers assess these incidents and incorporate the induced uncertainty into their evaluation of their relationship with a company. Indeed, our results show that this internal evaluation causes negative consequences for the company. Given that data breaches can be viewed in the broader context of security incidents, these findings inform privacy and security researchers about the potential risk of uncertainty established by security incidents.

Managerial Implications

The management of data breaches can benefit from our findings in three ways. First, we demonstrate that providing customers with a choice of compensation options has a positive impact. Traditionally, practitioners offer only one type of compensation to customers. These include predefined services or products, such as identity theft protection services or coupons (Greve et al. 2020; Seybold and Sony 2011; Wang et al. 2022), with which the affected customer has to settle. In our experiment, we contrasted both one-dimensional, single compensation and compensation with multiple choices. Although customers received different compensation options, the value of these was identical in both scenarios. Despite this, we were able to show that customers were more satisfied with the company's response when given the option to choose, due to the increased perceived control. From a practitioner's perspective, this suggests that higher levels of customer satisfaction can be achieved by compensation choices even though the financial input into the data breach response process remains identical. Accordingly, data breach response strategies should be adapted to meet these needs of customers.

Second, our findings indicate that practitioners should adopt distinct, unambiguous statements in their data breach response strategy to mitigate the overall perceived uncertainty among customers. Companies regularly rely on the justification strategy, i.e., trying to whitewash or relativize a data breach (Gwebu et al. 2018; Masuch, Greve, Trang, et al. 2021). However, uncertainty is more likely to be created among customers as a result of these imprecise statements referring to the critical security incident of data breaches. Our results contradict this approach and indicate that this strategy may actually have negative consequences. Instead, our findings recommend that certain, definitive information should be published containing conclusive results of the company's internal data breach response.

Third, we inform practitioners that customers seek control in the data breach response process and that this control has positive influences on the customer-company relationship. Our results show that customers' perceived control is a central pillar in reducing the negative impact of data breaches. In addition to increasing control through choice, practitioners are encouraged to identify what capabilities they have to empower customers in this process. For instance, active integration through the ability to have a voice and provide feedback (Dong et al. 2008; Karande et al. 2007), or the integration of technologies such as conversational agents (Diederich et al. 2022), may lead customers to sense an increased control over the data breach response process. Accordingly, companies should utilize data breach responses not as a mere tool for providing information, but more as a collaborative way of finding solutions.

Limitations and Opportunities for Future Research

Our research also has limitations, which should be addressed by future research. We have situated both of our experimental scenarios in the context of healthcare. While this is particularly appropriate for our study due to the high sensitivity of the compromised information (Seh et al. 2020), future studies should replicate the findings and explore them in different contexts. Moreover, future researcher should adapt the manner of the data breach notification to assess how it relates to the perceived uncertainty of customers. In particular, as indicated earlier, the content and framing of the available information requires scrutiny. In this context, researchers should address the extent to which strategies such as the justification strategy (Gwebu et al. 2018) increase actual perceived uncertainty. This could provide a new perspective on existing strategies and further disentangle the role of uncertainty in the context of data breach responses. Reactance research further suggests that individuals are more likely to feel a loss of freedom (i.e., uncertainty) the more serious and substantial the perceived threat. Previous data breach research reveals that data breaches can vary in severity (Martin et al. 2017; Posey et al. 2017). From this point of view, differences in severity could influence the level of perceived uncertainty. Moreover, based on the observed link between data breaches and the emergence of uncertainty, future research should further explore this relationship by incorporating privacy-related mediators such as lack of information or lack of control over the compromised data. This may provide insights into the differential effects of data breaches on uncertainty. Additionally, the integration of such privacy related constructs may provide valuable guidance for the strategic data breach response management of companies.

Conclusion

Data breaches are an everyday phenomenon that cause damage to companies in various aspects. Therefore, in mitigating these effects, conceptualizing an appropriate communicative data breach response strategy has become an important part of any companies' data breach response. By conducting two studies in online experiments (n=106; n=354), we investigate how uncertainty unfolds in a data breach context and how it can be mitigated by companies. Informed by data breach literature and reactance theory, we hypothesize that the uncertainty inherent in a data breach has negative effects on a company, but that these effects can be mitigated by providing customers with control. Our results confirm that uncertainty is a key factor in influencing the satisfaction of data breach responses. However, we demonstrate that perceived control can reduce these effects and, indeed, exhibits a direct positive effect on customer satisfaction. By conceptualizing choice as a catalyst for perceived control, we offer practitioners a novel strategy for responding to data breaches.

References

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., and Baskerville, R. L. 2020. "How Integration of Cyber Security Management and Incident Response Enables Organizational Learning," *Journal of the Association for Information Science and Technology* (71:8), pp. 939–953.

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., and Baskerville, R. L. 2021. "How Can Organizations Develop Situation Awareness for Incident Response: A Case Study of Management Practice," *Computers & Security* (101), p. 102122.

Al-Natour, S., Cavusoglu, H., Benbasat, I., and Aleem, U. 2020. "An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps," *Information Systems Research* (31:4), pp. 1037–1063.

Amarnath, D. D., and Jaidev, U. P. 2021. "Toward an Integrated Model of Consumer Reactance: A Literature Analysis," *Management Review Quarterly* (71:1), Springer International Publishing, pp. 41–90.

Anderson, C., Baskerville, R. L., and Kaul, M. 2017. "Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information," *Journal of Management Information Systems* (34:4), Routledge, pp. 1082–1112.

Averill, J. R. 1973. "Personal Control over Aversive Stimuli and Its Relationship to Stress," *Psychological Bulletin* (80:4), pp. 286–303.

Bansal, G., and Zahedi, F. M. 2015. "Trust Violation and Repair: The Information Privacy Perspective," *Decision Support Systems* (71), pp. 62–77.

Baskerville, R., Spagnoletti, P., and Kim, J. 2014. "Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response," *Information and Management* (51:1), pp. 138–151.

Bierhoff, H.-W., and Frey, D. 2011. "Sozialpsychologie -- Individuum Und Soziale Welt," *Sozialpsychologie -Individuum Und Soziale Welt*, Göttingen: Hogrefe.

Botti, S., and Iyengar, S. S. 2004. "The Psychological Pleasure and Pain of Choosing: When People Prefer Choosing at the Cost of Subsequent Outcome Satisfaction," *Journal of Personality and Social Psychology* (87:3), pp. 312–326.

Brehm, J. W. 1966. *A Theory of Psychological Reactance*, New York: Academic Press.

Brehm, S. S., and Brehm, J. W. 1981. *Psychological Reactance. A Theory of Freedom and Control*.

CaptureRX. 2021. *Data Breach Notification*.

Chan, E. Y., and Palmeira, M. 2021. "Political Ideology Moderates Consumer Response to Brand Crisis Apologies for Data Breaches," *Computers in Human Behavior* (121), Elsevier Ltd, pp. 1–7.

Chang, C.-C. 2006. "When Service Fails: The Role of the Salesperson and the Customer," *Psychology and Marketing* (23:3), pp. 203–224.

Chang, C. C. 2008. "Choice, Perceived Control, and Customer Satisfaction: The Psychology of Online Service Recovery," *Cyberpsychology and Behavior* (11:3), pp. 321–328.

Cheng, X., Su, L., Luo, X., Benitez, J., and Cai, S. 2021. "The Good, the Bad, and the Ugly: Impact of Analytics and Artificial Intelligence-Enabled Personal Information Collection on Privacy and Participation in Ridesharing," *European Journal of Information Systems* (00:00), Taylor & Francis, pp. 1–25.

Chin, W. W., Thatcher, J. B., Wright, R. T., and Steel, D. 2013. "Controlling for Common Method Variance in PLS Analysis: The Measured Latent Marker Variable Approach," in *New Perspectives in Partial Least Squares and Related Methods* (Vol. 56), A. Krishnan, N. Kriegeskorte, and H. Abdi (eds.), pp. 231–239.

Choi, B. C. F., Kim, S. S., and Jiang, Z. 2016. "Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior," *Journal of Management Information Systems* (33:3), pp. 904–933.

Clee, M. A., and Wicklund, R. A. 1980. "Consumer Behavior and Psychological Reactance," *Journal of Consumer Research* (6:4), p. 389.

Confente, I., Siciliano, G. G., Gaudenzi, B., and Eickhoff, M. 2019. "Effects of Data Breaches from User-Generated Content: A Corporate Reputation Analysis," *European Management Journal* (37:4), pp. 492–504.

Culnan, and Williams. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly* (33:4), pp. 673–687.

D'Arcy, J., Adjerid, I., Angst, C. M., and Glavas, A. 2020. "Too Good to Be True: Firm Social Performance and the Risk of Data Breach," *Information Systems Research* (31:4), pp. 1200–1223.

D'Arcy, J., and Basoglu, K. A. 2022. "Cybersecurity Disclosures The Influences of Public and Institutional Pressure on Firms ' Cybersecurity Disclosures," *Journal of the Association for Information Systems*, pp. 1–29.

Diederich, S., Brendel, A. B., Morana, S., and Kolbe, L. 2022. "On the Design of and Interaction with Conversational Agents: An Organizing and Assessing Review of Human-Computer Interaction Research," *Journal of Assoziation for Information Systems* (23), pp. 96–138.

Dong, B., Evans, K. R., and Zou, S. 2008. "The Effects of Customer Participation in Co-Created Service Recovery," *Journal of the Academy of Marketing Science* (36:1), pp. 123–137.

Erdfelder, E., Faul, F., Buchner, A., and Lang, A. G. 2009. "Statistical Power Analyses Using G*Power 3.1: Tests for Correlation and Regression Analyses," *Behavior Research Methods* (41:4), pp. 1149–1160.

Esmark, C. L., Noble, S. M., Bell, J. E., and Griffith, D. A. 2016. "The Effects of Behavioral, Cognitive, and Decisional Control in Co-Production Service Experiences," *Marketing Letters* (27:3), pp. 423–436.

Foerderer, J., and Schuetz, S. W. 2022. "Data Breach Announcements and Stock Market Reactions: A Matter of Timing?," *Management Science* (February).

Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), p. 39.

Friedman, M. I., and Lackey, G. H. 1991. *The Psychology of Human Control: A General Theory of Purposeful Behavior*, New York, NY: Praeger Publishers.

Gabisch, J. A., and Milne, G. R. 2014. "The Impact of Compensation on Information Ownership and Privacy Control," *Journal of Consumer Marketing* (31:1), pp. 13–26.

Goode, S., Hoehle, H., Venkatesh, V., and Brown, S. A. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach," *MIS Quarterly* (41:3), pp. 703–727.

Goodhue, D. L., Lewis, W., and Thompson, R. 2012. "Does PLS Have Advantages for Small Sample Size or Non-Normal Data?," *MIS Quarterly* (36:3), pp. 981–1001.

Greve, M., Masuch, K., Hengstler, S., and Trang, S. 2020. "Overcoming Digital Challenges: A Cross-Cultural Experimental Investigation of Recovering from Data Breaches," in *Forty-First International Conference on Information Systems*, pp. 1–17.

Guo, W., Straub, D., Zhang, P., and Cai, Z. 2021. "How Trust Leads to Commitment on Microsourcing Platforms: Unraveling the Effects of Governance and Third-Party Mechanisms on Triadic Microsourcing Relationships," *MIS Quarterly* (45:3), pp. 1309–1348.

Gwebu, K. L., Wang, J., and Wang, L. 2018. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management," *Journal of Management Information Systems* (35:2), pp. 683–714.

Hair, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. 2021. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, (3rd ed.), SAGE.

Hair, J. F., Risher, J. J., Sarstedt, M., and Ringle, C. M. 2019. "When to Use and How to Report the Results of PLS-SEM," *European Business Review* (31:1), pp. 2–24.

Henseler, J., Ringle, C. M., and Sarstedt, M. 2015. "A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling," *Journal of the Academy of Marketing Science* (43:1), pp. 115–135.

Henseler, J., Ringle, C. M., and Sinkovics, R. R. 2009. "The Use of Partial Least Squares Path Modeling in International Marketing," *Advances in International Marketing* (20), pp. 277–319.

Hibbeln, M., Jenkins, J. L., Schneider, C., Valacich, J. S., and Weinmann, M. 2017. "How Is Your User Feeling? Inferring Emotion Through Human-Computer Interaction Devices," *MIS Quarterly* (41:1), pp. 1–21.

Hinds, P. J. 1998. "User Control and Its Many Facets: A Study of Perceived Control in Human-Computer Interaction," *HP Laboratories Technical Report*, California: Hewlett Packard Laboratories.

Hoehle, H., Venkatesh, V., Brown, S. A., Tepper, B. J., and Kude, T. 2022. "Impact of Customer Compensation Strategies on Outcomes and the Mediating Role of Justice Perceptions: A Longitudinal

Study of Target's Data Breach," *MIS Quarterly* (46:1), pp. 299–340.

Hui, M. K., and Bateson, J. E. G. 1991. "Perceived Control and the Effects of Crowding and Consumer Choice on the Service Experience," *Journal of Consumer Research* (18:2), p. 174.

Hui, M. K., and Toffoli, R. 2002. "Perceived Control and Consumer Attribution for the Service Encounter," *Journal of Applied Social Psychology* (32:9), pp. 1825–1844.

Jackson, S., Vanteeva, N., and Fearon, C. 2019. "An Investigation of the Impact of Data Breach Severity on the Readability of Mandatory Data Breach Notification Letters: Evidence From U.S. Firms," *Journal of the Association for Information Science and Technology* (70:11), pp. 1277–1289.

Janakiraman, R., Lim, J. H., and Rishika, R. 2018. "The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer," *Journal of Marketing* (82:2), pp. 85–105.

Karande, K., Magnini, V. P., and Tam, L. 2007. "Recovery Voice and Satisfaction After Service Failure: An Experimental Investigation of Mediating and Moderating Factors," *Journal of Service Research* (10:2), pp. 187–203.

Karwatzki, S., Trenz, M., and Veit, D. 2022. "The Multidimensional Nature of Privacy Risks: Conceptualisation, Measurement and Implications for Digital Services," *Information Systems Journal* (March 2020), pp. 1–32.

Kim, S. H., and Kwon, J. 2019. "How Do EHRs and a Meaningful Use Initiative Affect Breaches of Patient Information?," *Information Systems Research* (30:4), pp. 1184–1202.

Kock, N., and Hadaya, P. 2018. "Minimum Sample Size Estimation in PLS-SEM: The Inverse Square Root and Gamma-Exponential Methods," *Information Systems Journal* (28:1), pp. 227–261.

Kude, T., Hoehle, H., and Sykes, T. A. 2017. "Big Data Breaches and Customer Compensation Strategies: Personality Traits and Social Influence as Antecedents of Perceived Compensation," *International Journal of Operations & Production Management* (37:1), pp. 56–74.

Kwon, J., and Johnson, M. E. 2018. "Meaningful Healthcare Security: Does Meaningful-Use Attestation Improve Information Security Performance?," *MIS Quarterly* (42:4), pp. 1043–1067.

Lacey, H. M. 1979. "Control, Perceived Control, and the Methodological Role of Cognitive Constructs," in *Choice and Perceived Control*, L. C. Perlmuter and R. A. Monty (eds.), Hillsdale, NJ: Lawrence Erlbaum Associates.

Lehrer, C., Wieneke, A., vom Brocke, J., Jung, R., and Seidel, S. 2018. "How Big Data Analytics Enables Service Innovation: Materiality, Affordance, and the Individualization of Service," *Journal of Management Information Systems* (35:2), pp. 424–460.

Loss, I., and Reactance, P. 1993. *Control, Its Loss, and Psychological Reactance*, pp. 3–30.

Lowry, P. B., and Moody, G. D. 2015. "Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies," *Information Systems Journal* (25:5), pp. 433–463.

Martin, K. D., Borah, A., and Palmatier, R. W. 2017. "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing* (81:1), pp. 36–58.

Masuch, K., Greve, M., and Trang, S. 2021. "What to Do after a Data Breach? Examining Apology and Compensation as Response Strategies for Health Service Providers," *Electronic Markets* (31), pp. 829–848.

Masuch, K., Greve, M., Trang, S., and Kolbe, L. M. 2021. "Apologize or Justify? Examining the Impact of Data Breach Response Actions on Stock Value of Affected Companies," *Computers & Security*, pp. 1–18.

Maxham, J. G., and Netemeyer, R. G. 2002. "Modeling Customer Perceptions of Complaint Handling over Time: The Effects of Perceived Justice on Satisfaction and Intent," *Journal of Retailing* (78:4), pp. 239–252.

Nunnally, J. C., and Bernstein, I. H. 1994. "The Assessment of Reliability," in *Psychometric Theory* (3rd ed.), New York, NY: McGraw-Hill, pp. 248–292.

Oliver, R. L. 1980. "A Cognitive Model of the Antecedents and Consequences of Satisfaction Decisions," *Journal of Marketing Research* (17:4), pp. 460–469.

Ostermann, U., Holten, R., and Franzmann, D. 2020. "The Influence of Private Alternatives on Employees' Acceptance of Organizational IS," *Communications of the Association for Information Systems* (47:1), pp. 764–792.

Palan, S., and Schitter, C. 2018. "Prolific.Ac—A Subject Pool for Online Experiments," *Journal of Behavioral and Experimental Finance* (17), Elsevier B.V., pp. 22–27.

Pavlou, P. A., Liang, H., and Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), pp. 105–136.

Pfeffer, J., and Salancik, G. R. 1978. *The External Control of Organizations: A Resource Dependence Perspective*, New York: Harper Row.

Ponemon Institute. 2021. "Cost of a Data Breach Report 2021," *IBM Security*. (https://www.ibm.com/security/data-breach).

Posey, C., Raja, U., Crossler, R. E., and Burns, A. J. 2017. "Taking Stock of Organisations' Protection of Privacy: Categorising and Assessing Threats to Personally Identifiable Information in the USA," *European Journal of Information Systems* (26:6), Palgrave Macmillan UK, pp. 585–604.

Prisma Health. 2019. "Data Breach Notification." (https://www.doj.nh.gov/consumer/security-breaches/documents/prisma-health-20191104.pdf, accessed February 16, 2021).

Rasoulian, S., Grégoire, Y., Legoux, R., and Sénécal, S. 2017. "Service Crisis Recovery and Firm Performance: Insights from Information Breach Announcements," *Journal of the Academy of Marketing Science* (45:6), pp. 789–806.

Ringle, C. M., Wende, S., and Becker, J.-M. 2015. *SmartPLS 3*, SmartPLS GmbH.

Schuetz, S. W., Lowry, P. B., Pienta, D. A., and Thatcher, J. B. 2021. "Improving the Design of Information Security Messages by Leveraging the Effects of Temporal Distance and Argument Nature," *Journal of the Association for Information Systems* (22:5), pp. 1376–1428.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., and Khan, R. A. 2020. "Healthcare Data Breaches: Insights and Implications," *Healthcare* (8:2), pp. 1–18.

Seybold, P., and Sony. 2011. *Sony Offering Free `AllClear ID Plus' Identity Theft Protection in the United States through Debix, Inc.* (https://blog.playstation.com/2011/05/05/sony-offering-free-allclear-id-plus-identity-theft-protection-in-the-united-states-through-debix-inc/).

Skinner, E. A., Chapman, M., and Baltes, P. B. 1988. "Control, Means-Ends, and Agency Beliefs: A New Conceptualization and Its Measurement During Childhood," *Journal of Personality and Social Psychology* (54:1), pp. 117–133.

Steiner, J. E. 1979. "Human Facial Expressions in Response to Taste and Smell Stimulation," *Advances in Child Development and Behavior* (13), pp. 257–295.

T-Mobile. 2021. "The Cyberattack Against T-Mobile and Our Customers." (https://www.t-mobile.com/news/network/cyberattack-against-tmobile-and-our-customers, accessed May 3, 2022).

Thibaut, J. W., and Walker, L. 1975. *Procedural Justice : A Psychological Analysis*, Hillsdale, NJ: Lawrence Erlbaum Associates.

Thompson, S. C. 1981. "Will It Hurt Less If I Can Control It? A Complex Answer to a Simple Question," *Psychological Bulletin* (90:1), pp. 89–101.

Trenz, M., Veit, D. J., and Tan, C. W. 2020. "Disentangling the Impact of Omnichannel Integration on Consumer Behavior in Integrated Sales Channels," *MIS Quarterly* (44:3), pp. 1207–1258.

Verizon. 2021. *Data Breach Investigations Report*.

Wang, Xuhui, Wang, Xuequn, Liu, Z., Chang, W., Hou, Y., and Zhao, Z. 2022. "Too Generous to Be Fair? Experiments on the Interplay of What, When, and How in Data Breach Recovery of the Hotel Industry," *Tourism Management* (88), Elsevier Ltd, p. 104420.

Wendlandt, M., and Schrader, U. 2007. "Consumer Reactance against Loyalty Programs," *Journal of Consumer Marketing* (24:5), pp. 293–304.

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R., and Zajicek, M. 2003. *Handbook of Computer Security Incident Response Teams (CSIRTs)*, (2nd ed.).

White, R. W. 1959. "Motivation Reconsidered: The Concept of Competence," *Psychological Review* (66:5), pp. 297–333.

Wortman, C. B. 1975. "Some Determinants of Perceived Control.," *Journal of Personality and Social Psychology* (31:2), pp. 282–294.

Yazdanmehr, A., Wang, J., and Yang, Z. 2020. "Peers Matter: The Moderating Role of Social Influence on Information Security Policy Compliance," *Information Systems Journal* (30:5), pp. 791–844.

Yoo, Y., Boland, R. J., Lyytinen, K., and Majchrzak, A. 2012. "Organizing for Innovation in the Digitized World," *Organization Science* (23:5), pp. 1398–1408.