OPENNESS ALWAYS PAYS OFF – INVESTIGATION OF DIVERSE ACTIONS IN RESPONSE STRATEGIES TO DATA BREACHES

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

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

Maike Greve
*University of Goettingen*, maike.greve@uni-goettingen.de

Steffen Massanneck
*University of Goettingen*, steffen.massanneck@stud.uni-goettingen.de

Duy Khang Nguyen
*University of Goettingen*, duykhang.nguyen@stud.uni-goettingen.de

See next page for additional authors

Follow this and additional works at: https://aisel.aisnet.org/ecis2021_rp

Recommended Citation
Masuch, Kristin; Diesterhöft, Till Ole; Greve, Maike; Massanneck, Steffen; Nguyen, Duy Khang; Trang, Simon; and Kolbe, Lutz M., "OPENNESS ALWAYS PAYS OFF – INVESTIGATION OF DIVERSE ACTIONS IN RESPONSE STRATEGIES TO DATA BREACHES" (2021). ECIS 2021 Research Papers. 126.
https://aisel.aisnet.org/ecis2021_rp/126

This material is brought to you by the ECIS 2021 Proceedings at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2021 Research Papers by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
OPENNESS ALWAYS PAYS OFF – INVESTIGATION OF DIVERSE ACTIONS IN RESPONSE STRATEGIES TO DATA BREACHES

Research Paper

Kristin Masuch, University of Goettingen, Goettingen, Germany, kristin.masuch@uni-goettingen.de
Till Ole Diesterhöft, University of Goettingen, Goettingen, Germany, tillole.diesterhoeft@uni-goettingen.de
Maike Greve, University of Goettingen, Goettingen, Germany, maike.greve@uni-goettingen.de
Steffen Massanneck, University of Goettingen, Goettingen, Germany, steffen.massanneck@stud.uni-goettingen.de
Duy Khang Nguyen, University of Goettingen, Goettingen, Germany, duykhang.nguyen@stud.uni-goettingen.de
Simon Trang, University of Goettingen, Goettingen, Germany, simon.trang@wiwi.uni-goettingen.de
Lutz M. Kolbe, University of Goettingen, Goettingen, Germany, lutz.kolbe@wiwi.uni-goettingen.de

Abstract

Data breaches have become a daily problem and cause immense damage to the affected companies in their customer relationship with the impacted customers. Research has shown that this effect can be positively influenced by applying response strategies. Our study focuses on three main actions that can be identified from data breach response strategies: an apology for the incident, the visibility of the CEO, and high readability of the message. To investigate the impact on transnational and cumulative customer satisfaction, a scenario-based experiment was conducted with 567 participants. Our results show that all three actions have a strong positive effect on transaction satisfaction. Moreover, these response actions have a positive effect on cumulative satisfaction, although the effects are not as strong. Finally, the results are discussed in the context of justice theory and situational crisis communication theory, and practical implications, limitations, and possible future research options are derived.

Keywords: Data Breach Response Strategies, Apology, Readability, CEO Visibility

1 Introduction

On 19th May 2020, the British multinational airline EasyJet announced that it became the victim of a data breach resulting from a cyber-attack. The intruders accessed 9 million data records including
information about travel data, email addresses and sensitive credit card details. In a public statement, CEO Johan Lundgren personally addressed customers with the following words: "We would like to apologise to those customers who have been affected by this incident." (easyJet, 2020). He additionally explained that the company implemented security measures, which however were overcome by the data breach as they are an "[...] evolving threat as cyber attackers get ever more sophisticated." (easyJet, 2020). The mentioned incident and resulting company reaction is one example of manifold that have recently occurred (Sen and Borle, 2015). Companies are regularly expected to inform affected customers and publically respond to security incidents. As in the example above, companies distribute messages of this kind on an almost daily basis (State of California, 2020).

Managerial approaches to address such events can be classified into two fundamental areas: preventing and responding (Yue and Çakanyildirim, 2007; Baskerville, Spagnoletti and Kim, 2014). While prevention deals with what systems and processes can be implemented to prevent such an incident (Yue and Çakanyildirim, 2007), responding refers to the plan of what to do if a data breach occurs (Baskerville et al., 2014). Although preventive measures are necessary for a company to mitigate and control the occurrence of data breaches (Kwon and Johnson, 2011, 2013; Khan, Kim, Moore and Mathiassen, 2019), actual breaches show that prevention is not sufficient to ensure absolute avoidance (Sen and Borle, 2015). The recent cases of Sony (2011), Hyatt (2017) and Adobe Systems Inc. (2013) show that these incidents affect a wide range of companies, including listed and internationally operating corporations. While the legal situation in the United States and Europe forces enterprises to inform their customers in the event of a data breach (Culnan and Williams, 2009; Council of the European Union, 2016), significant differences in the individual response strategies to such breaches can be identified (Breach et al., 2020). For example, Hyatt’s global president of operations personally apologises to his customers and expresses remorse (Hyatt, 2017). The question arises whether and how far these answers lead to divergent effects on customers. In this context, the literature shows that authors recommend studying companies’ post-breach behaviour, especially regarding the management of response strategies towards affected customers (Malhotra and Kubowicz Malhotra, 2011). This has since been advanced by several publications that focus on individual response actions and the resulting customer behaviour (Bansal and Zahedi, 2015; Choi, Kim and Jiang, 2016; Goode, Hoehle, Venkatesh and Brown, 2017). Within this research, it was shown that different response strategies lead to varying levels of customer satisfaction, which, in turn, mediates customer relationship (Greve, Masuch, Hengstler and Trang, 2020). However, it is noticeable that merely the transactional satisfaction with the response strategy itself is examined, but not the cumulative satisfaction, that is, the overall satisfaction of a customer with a company (Varela-Neira, Vázquez-Casielles and Iglesias-Argüelles, 2008; Orsingher, Valenti and de Angelis, 2010). A distinct examination of those concepts can be motivated by the service failure literature, which shows that both types are influenced to a different extent by varying response strategies (Gelbrich and Roschk, 2011). Their divergent effects on customers further support this. Cumulative satisfaction has been shown to increase repurchase intention and loyalty to the company (Orsingher et al., 2010; Gelbrich and Roschk, 2011), while transactional satisfaction promotes positive word-of-mouth (WOM) and trust (Tax, Brown and Chandrashekaran, 1998; Gelbrich and Roschk, 2011). This implies that additional research of response strategies and their consequences is necessary in order to assess their effectiveness as well as their potential to support management in their post-breach strategy development. Drawing on the service failure literature and the three fundamental components of a data breach response, apology, readability and CEO visibility, we aim to answer the following research question:

*RQ: How do the company’s response actions apology, CEO visibility and readability impact the transactional and cumulative satisfaction of a customer?*

To answer this question, we conduct an experiment with 567 participants in which they are introduced to the situation of being an affected customer of an online banking data breach. They received a message from this company informing them about the incident. The obtained data breach notification is one of the eight response strategies resulting from the 2x2x2 factorial design of the three fundamental response actions apology, CEO visibility and readability. As a theoretical framework for
describing and hypothesizing the effects of the three response actions, we draw on justice theory and situational crisis communication theory (SCCT).

This paper holds various implications for theory and practice and contributes to the scientific literature. We demonstrated that varying response actions influence the two investigated satisfaction levels in different ways. While extending the theoretical scope of response strategies in the current research stream on data breaches, which focuses solely on transactional satisfaction, we also provide management with insightful findings. In this respect, we can show that the governance of response strategies has a multifaceted influence on customer satisfaction, which in turn strengthens the consideration of the development of context- and corporate-specific data breach response strategies. The paper is structured as follows: First, we present the theoretical and conceptual background of the paper, highlighting the current data breach literature and discussing justice theory and SCCT. The three hypotheses for testing the model are then derived from literature. Subsequently, the design of the experiment is explained, followed by the analysis and discussion of the results obtained. Implications and limitations are presented, and a conclusion is drawn.

2 Theoretical Lens for Data Breach Response Strategies

2.1 Research on Data Breach Response Strategies

When examining studies from the data breach response research stream, the emphasis on concepts from the service failure literature is striking (Choi et al., 2016; Kude, Hoehle and Sykes, 2017). This adoption is derived by the view on data breaches as special service failures that expose sensitive data (Goode et al., 2017). While the link to service failure is almost ubiquitous, the exploration of specific data breach response actions is rather heterogeneous (Bansal and Zahedi, 2015; Gwebu, Wang and Wang, 2018). Goode et al. (2017) explore the influence of compensation on the perceived level of service performance and factors that shape subsequent customer relationships based on the Sony data breach. Kude et al. (2017) also employ this strategy but study its effect on the consumer experience concerning different characteristics of personality. Another literature branch deals with the role of response strategies on stock market value. While Gwebu et al. (2018) examine several ad-hoc defined strategies, Masuch, Greve and Trang (2020) explicitly apply the strategies whitewash and apology. Another publication deals with an apology as well as the denial and no-response strategy in the context of re-establishing customer trust after a data breach (Bansal and Zahedi, 2015). Furthermore, the actions of apology and compensation are analysed for the transactional satisfaction of consumers (Masuch, Greve and Trang, 2019; Greve, Masuch and Trang, 2020; Masuch, Greve, Cyrenius, et al., 2020).

In this respect, transactional satisfaction can be defined as the concrete short-term satisfaction with the performed action of a company (Olsen and Johnson, 2003) and cumulative satisfaction as the summary of experiences of all transactions that have been carried out across a long-term period of time (Varela-Neira et al., 2008; Orsingher et al., 2010; Gelbrich and Rosch, 2011). Both concepts show different effects on aspects of the customer-provider relationship, such as loyalty, word-of-mouth (WOM) and trust (Tax et al., 1998; Kau and Wan-Yiun Loh, 2006; Gelbrich and Roschk, 2011). While different perspectives of response strategies and their effects are studied in the data breach literature, it is noticeable that the direct effects on consumers are only researched on the transactional level (e.g. Masuch et al., 2020). In contrast to the related literature, there exists, at least to the knowledge of the authors, no consideration of the aggregate of all transactional experiences, which constitutes the cumulative satisfaction (Orsingher et al., 2010; Gelbrich and Rosch, 2011).

The review of current literature additionally reveals that there is no consensus on the strategies under examination. Nevertheless, it becomes evident that compensation and apology form a substantial part of the studied actions. Analysis of practical responses of companies to data breaches reveals that compensation, as defined in the literature, is not commonly applied as opposed to an apology (Breach et al., 2020). Drawing on the service failure literature, one can argue that offering an apology is almost inevitable to respond to a data breach (Baker, Meyer and Johnson, 2008; Mattila, 2009). Accordingly,
we view this component as an essential part of a real response strategy. When observing corporate data breach strategies, two other repeating elements become apparent, which must be incorporated in a response.

<table>
<thead>
<tr>
<th>Data Breach</th>
<th>Data Breach Response</th>
</tr>
</thead>
</table>
| 12.10.2017, Hyatt, Payment Card Incident | "Dear Hyatt Guest, We understand the importance of protecting customer information and securing our systems, and we regret to inform you that we discovered signs of and then resolved unauthorized access to payment card information [...]"
| | Sincerely, Chuck Floyd
| | Global President of Operations
| | Hyatt Hotels Corporation" |
| 09.07.2018, Timehop, Network Intrusion | "On July 4, 2018, Timehop experienced a network intrusion that led to a breach of some of your data. [...]"
| | We log IP addresses for network audit purposes as disclosed in our Terms of Service. The servers that we run, like all web servers, log incoming traffic information, including IP addresses. At the scale at which Timehop operates, the servers generate millions of log lines."

Table 1. Actual Data Breach Response Strategies

First, the way in which the content of the incident is depicted can be vastly different. While Hyatt talks very superficially, Timehop discusses technical details (see Table 1). Regardless of the different content, a variation in the complexity of the presentation form can be recognised. In line with current literature (Jackson, Vanteeva and Fearon, 2019; Zou, Danino, Sun and Schaub, 2019), we call this component readability, that is the degree of simplicity with which a text can be grasped based on the way it is written (Klare, 1963). Furthermore, it must be assumed that such a response always possesses an original author. In the case of Hyatt, this is the Global President of Operations. Contrary to this, Timehop does not indicate by whom the response was written. The decision of publishing the author is independent of the circumstances of the data breach and therefore constitutes part of the basic response structure. Drawing on the literature of crisis response, we will refer to this component as CEO visibility (Turk et al., 2012; Y. Kim and Park, 2017). While other components and response actions exist (e.g., Bansal and Zahedi, 2015; Goode et al., 2017), by examining the practice we see that readability, visibility, and apology are fundamental components of a response. Having introduced three components of a prototypical data breach response strategy, we will now provide their theoretical foundations.

**2.2 Reviewing Justice Theory**

Service failure literature shows that the application of justice theory as an overarching framework has emerged as an integral part of the investigation of recovery strategies following the occurrence of a service failure (Goodwin and Ross, 1992; Smith, Bolton and Wagner, 1999; Mccollough, Berry and Yadav, 2000; Karande, Magnini and Tam, 2007; Gelbrich and Roschk, 2011). Justice theory differentiates between three dimensions: distributive justice, examining the extent to which received benefits or results of decisions are regarded to be fair (Adams, 1965; Smith et al., 1999), procedural justice, relating to the perceived fairness of decision processes (Leventhal, 1980; Greenberg, 1990), and interactional justice, dealing with the perceived justice of interpersonal procedures, treatments and interactions (Bies and Shapiro, 1987; Tax et al., 1998). The practice of conducting specific strategies for recovery had been assigned different effects on these dimensions (Smith et al., 1999; Karande et al., 2007).

Various research studies have been able to show that strategies have varying effects on the justice dimensions (Smith et al., 1999; Mccollough et al., 2000; Gelbrich and Roschk, 2011). One of the strategies studied within the framework of justice theory is an apology. It “[…] is defined as a statement that acknowledges both responsibility and regret for a trust violation” (P. H. Kim, Ferrin, Cooper and Dirks, 2004). Thus, an apology is dependent on its context (Roschk and Kaiser, 2013) and can also be accompanied by remorse (Fehr and Gelfand, 2010). Apologising to consumers indicates that a company explains the incident and acknowledges the potential damage caused by the data...
breach (Bansal and Zahedi, 2015). Consistent with the research findings of Smith et al. (1999), we conceive an apology as an action primarily related to interactional justice.

Table 1 shows two recent practical examples of companies applying this response action. In early 2020, the American company PIH Health announced that personally identifiable information (PII) and protected health information (PHI) were potentially breached by a phishing attack on employees’ mail accounts (PIH Health, 2020). In addition to providing a credit monitoring service, the company expressed its apologies to its customers for any discomfort the incident might cause. Following the discovery of a faulty configuration of a database, the CEO of British company Virgin Media announced in March 2020 that contact data of 900,000 customers are potentially at risk of being compromised (Virgin Media, 2020). The company subsequently emphasised the security of its customers and apologised to those affected.

<table>
<thead>
<tr>
<th>Justice Dimension</th>
<th>Response Action</th>
<th>Example &amp; Data Breach Response Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactional Justice</td>
<td>Apology: An apologetic message that “[...] acknowledges both responsibility and regret for a trust violation.” (P. H. Kim et al., 2004)</td>
<td>10.01.2020; potentially PHI and PII compromised “PHI Health deeply regrets any inconvenience or concern this incident may cause.” (PIH Health, 2020)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>05.03.2020; 900,000 potentially affected contact data “Protecting our customers’ data is a top priority and we sincerely apologise.” (Virgin Media, 2020).</td>
</tr>
</tbody>
</table>

Table 2. Apology and Practical Examples

2.3 Reviewing Situational Crisis Communication Theory

By leveraging concepts from the image restoration theory (Benoit, 1997), Coombs (2007) developed the SCCT. It is a framework for protecting and repairing the reputation in post-crisis communication through choosing effective crisis communication response strategies (Coombs and Holladay, 2002; Coombs, 2007; Wang and Park, 2017; N. Kim and Lee, 2018). The primary goal is the protection of the affected people from damage by using communication possibilities, and afterwards, the consideration to protect their reputation (Coombs, 2007; Kriyantono, 2012). A crisis situation in the SCCT is defined as an unexpected event that poses a physical, emotional or financial threat to stakeholders, including customers (Coombs, 2007). The uncertainty of the potential damage creates a stressful situation for the customers. Possible negative effects of a crisis are that customers cut ties with the company or spread negative WOM (Coombs, 2007). To cope with it, they need information about the event and what will be done to protect them in the future (Coombs, 2007). Response strategies are applied to reduce these negative effects on the reputation and the behavioural intention (Coombs, 2007). In this context, the transparency of a response strategy is particularly important, since the most important goal in SCCT is to protect the affected customer (Coombs, 2007). Within this literature, one can also find the response action which is derived from real data breach response strategies. For our purpose, the following two response strategies can be derived. One of them is the visibility of a CEO. Turk et al. (2012) analysed the effect of this specific strategy and found that the attitudes toward companies with a visible CEO in crisis response are higher than the attitude toward companies without a visible CEO. Moreover, it was shown that the CEO, as a spokesperson, is perceived as a more credible source of information than the company as a whole (Kim and Park, 2017). Research shows that a positive CEO reputation can protect the company’s corporate image, which complements the results of these two studies (Sohn and Lariscy, 2012; Y. Kim and Park, 2017). Overall, this suggests that using a visible CEO is a viable response action. However, not only the conveyor of a message is essential. Clear, understandable messages are needed in crisis communication since easier to understand messages lead to positive customer behaviour (Rennekamp, 2012; Temnikova et al., 2015). Hence, transparency constitutes another option for a response action (S. Kim and Sung, 2014; Dulaney and Gunn, 2017). By increasing transparency, research has shown an improvement in credibility and trust for the existing company (Kim and Sung, 2014). The dimensions of information quality can be considered to describe this mechanism (Schnackenberg and Tomlinson, 2016). Clarity is one of the most important aspects of what is perceived as transparent
Openness Always Pays Off

(Kundeliene and Leitoniene, 2015). It describes the perceived understanding of information that a recipient receives (Snackenberg and Tomlinson 2016). To make clarity and thus transparency measurable, the readability of a text message can be used as an association (Hartley, 2003; Goel and Chengalur-Smith, 2010a), which has already been considered in the context of data breaches. However, so far only in the context as to why notifications of data breaches by individuals are ignored (Zou and Schaub, 2019). The following table highlights four actual data breach responses applying those strategies.

<table>
<thead>
<tr>
<th>Definition based on SCCT</th>
<th>Example &amp; Data Breach Response Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO visibility: The presence of the CEO in the Data Breach Notification</td>
<td>&quot;While I am grateful that the perpetrator has been caught, I am deeply sorry for what has happened,&quot; said Richard D. Fairbank, Chairman and CEO. (Capital One, 2019)</td>
</tr>
<tr>
<td>Readability: &quot;the ease of understanding or comprehension due to the style of writing&quot; (Klare, 1963)</td>
<td>Incidence regarding user data from Toyota Financial Services (Toyota Financial Services, 2016). A national manager signs data breach notification.</td>
</tr>
<tr>
<td>High readability: &quot;[…] a Chase employee improperly downloaded customer information […]&quot; (JP Morgan Chase Bank, 2018).</td>
<td>Low readability: For some, the information also includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128).&quot; (Marriott International, 2018)</td>
</tr>
</tbody>
</table>

Table 3. SCCT and Actual Data Breach Response Strategy Examples

3 Hypotheses Development and Research Model

Based on the justice theory and the SCCT, a research model was developed to study the effects of three different reaction actions (see Figure 1). The research model aims to investigate whether there is a short-term change in behaviour due to the different reaction actions with the measurement of transactional customer satisfaction. Moreover, it investigates whether cumulative satisfaction, i.e., a subsequent change in behavioural intention towards the company, can be identified.

![Research Model Diagram]

Figure 1. Research Model

As already highlighted, the exploration of the action apology is a widespread research topic. It is noticeable that apologies are not viewed in a completely uniform manner, but rather in a manifold way (e.g. Mccollough, Berry and Yadav, 2000; Gelbrich and Roschk, 2011). Literature indicates that in complaint handling, an apology has a positive effect on the transactional satisfaction of service recipients (Tax et al., 1998; Smith et al., 1999; Gelbrich and Roschk, 2011). These research results are primarily based on the assumption that an apology is treated as a form of restorative action (Tax et al., 1998; Gelbrich and Roschk, 2011). In addition, another literature stream indicates that perceived apology has a positive impact on the confirmation, which in turn is positively correlated with the satisfaction with a response strategy (Masuch, Greve, Cyrenius, et al., 2020). Since this satisfaction with a specific strategy can be regarded as equivalent to the satisfaction with a transaction, it can be

assumed that a positive relationship between perceived apology and transactional satisfaction exists. The consideration of this interrelation can be described as follows:

**H1a: The response action apology has a positive effect on transactional satisfaction.**

In addition to the aforementioned influence of an apology on the satisfaction with a specific response strategy, research has also demonstrated the influence on cumulative satisfaction (Gelbrich and Roschh, 2011). Authors were able to show that a pure apology, detached from compensation, can be assigned primarily to the interactional justice (Smith et al., 1999; Mccollough et al., 2000). Furthermore, it could be shown that the interactional dimension has the greatest effect on this specific satisfaction level (Gelbrich and Roschh, 2011). The combination of both outcomes implies that there is an influence between apology and cumulative satisfaction. Furthermore, it was shown that an apology has a positive effect on the restoration of trust (Bansal and Zahedi, 2015), which in turn positively affects loyalty (DeWitt, Nguyen and Marshall, 2008) and thus is mediated by cumulative satisfaction (Gelbrich and Roschh, 2011). We hypothesize the following:

**H1b: The response action apology has a positive effect on cumulative satisfaction.**

The CEO is one of the key players in the successful management of a crisis, as the CEO is closely linked to the company or its reputation (Murray, E.; Shohen, 1992; Alsop, 2004). Previous studies have shown that the CEO is the most trusted source to deliver a notification (Kim and Park, 2017). Turk et al. (2012) concluded that the appearance of a CEO leads to a positive attitude, which leads to higher satisfaction with the response. Based on this, we make the following hypothesis:

**H2a: The response action visibility of the CEO has a positive effect on transactional satisfaction.**

A possible explanation could be that the recipient of the message is shown humanity by a high-level individual as opposed to a faceless company so that a higher perception of respect is expressed (Turk et al., 2012; Grundy and Moxon, 2013; Tang and Gray, 2018). Turk et al. (2012) also stated that purchase intention increases with the visibility of the CEO. It can be determined that purchase decisions and intentions are a reflection of cumulative satisfaction (Olsen and Johnson, 2003). Therefore, we propose the following hypotheses:

**H2b: The response action visibility of the CEO has a positive effect on cumulative satisfaction.**

Affected customers must receive comprehensible data breach notifications. Studies show that difficult to understand notifications are not perceived positive, but rather lead to frustration (Razek and Cone, 1981; Velez and Ashworth, 2007). This suggests that high readability leads to a more positive perception of a message. Thus, we derive the following hypothesis:

**H3a: The response action high readability has a positive effect on transactional satisfaction.**

Moreover, it has been indicated that a rise in customer satisfaction can be observed from increased transparency and thereby also influences the relationship between a company and its customers (Waddock, 2004; Eskildsen and Kristensen, 2007; Kang and Hustvedt, 2014). This relationship is reflected both in trust in the company and in long-term behavioural intentions (Gainey and Klass, 2003; Liu et al., 2015). Kim and Kim (2016) could support this in their study. As stated previously, for this study, transparency and clarity can be considered as readability (Goel and Chengalur-Smith, 2010b; Schnackenberg and Tomlinson, 2016; Holland, Krause, Provencher and Seltzer, 2018). This leads to the following hypotheses:

**H3b: The response action high readability has a positive effect on cumulative satisfaction.**

## 4 Research Design

We tested the defined hypotheses with an online experiment. A 2x2x2 full factorial design for the independent variables apology, CEO visibility and readability was used. The questionnaire was conducted among German participants. The participants were asked to imagine a fictitious data breach of a digital banking service. This example was considered because it contains highly sensible PII like a personal name, place of residence, financial situation or indicators of purchase history which can be
misused in malicious ways, e.g., to do unintended transactions on behalf of the victim (Capital One, 2017).

4.1 Data-Collection Procedure and Sample

Participants were recruited through mailing lists, public announcements posted in the university community, and social media posts. The participants were asked to imagine that they are a customer of the “Smart-Bank.” They were informed what data was collected by the bank. After this introduction about the offered services of the bank and the gathered data, the participants were informed that the bank has suffered a data breach and the participant belong to the affected participant. Hence, they receive a random scenario containing the company’s response to the data breach. Following this, the participants received the same survey about the perceived independent variables, their transactional satisfaction with the company response and their cumulative satisfaction with the company. In the end, they were asked if they found this scenario realistic. We surveyed 812 participants. Answers have been removed if they are invalid or incomplete. Manipulation checks were performed by asking questions regarding the content of the scenario, which could verify whether participants had genuinely read the scenario. After removing the answers, we obtained a sample size of n=567 participants, with an average age of 25 years (M=25.38, SD = 6.84 years) and 38.98% men and 60.14% women were surveyed. In our sample, 45.68% have a college degree or higher. Furthermore, 96.65% of the participants have a high school diploma or received a degree from a vocational school. Participants stated that 29.28% experienced a data breach before. In addition, for 92.42% of the respondents the security of their data had a certain value (24.34% “quite important”, 36.16% “important”, 31.92% “very important”).

4.2 Experimental Design

The introductory scenario was the same for all participants and is depicted below:

“Smart-Bank is a direct bank that offers customers services such as setting up a free checking account. Smart-Bank also offers additional digital services, such as investing in securities and using online banking, i.e. the digital processing of payments with the account. Mobile payment systems such as Apple Pay and Google Pay are also supported, allowing users to make payments using their mobile devices. These options allow customers to access their data at any time and from anywhere. You have registered at Smart-Bank some time ago because of good pricing conditions and the excellent service they receive. Smart-Bank has collected the following data for the registration and in order to be able to offer the before mentioned services: Name, login credentials, payment history, phone number, geodata, information about the employer.”

The factorial design consists of the three dimensions apology, CEO visibility and readability, each with two variations regarding the response action of the company. The information about the data breach of the bank and the company response to it was delivered by a letter in the mail.

In order to separate the different, changed variables from each other, they are in different positions in the notification. Firstly, for the independent variable apology, we varied the scenario text in the beginning. Based on Veltsos (2012) and real data breach notifications, we created elements of an apology. For the “no apology” scenario no apology was given to the customer, contrary to the “apology” scenario, an apology was given to the customer. As in a data breach notification by EasyJet, an apology has been divided into two sentences, explaining that an incident has occurred, followed by a separate sentence with an apology (EasyJet, 2020). For the independent variable CEO visibility, the signer of the data breach was exchanged. For the “visible CEO” scenario, the signer of the data breach notification was the CEO, on the contrary for the “no visible CEO” scenario the customer support was chosen. Based on real data breaches, the CEO also addresses the customer in a personal form (Toyota Financial Services, 2016; EasyJet, 2020). In the following, we describe the procedure of the data collection and the experimental design.

In order to create two measurably different messages, a formula has to be selected that can quantify the readability of a text. There are various formulas to calculate readability. An approach to measure readability is the formula of the Flesch Index created by Rudolf Flesch (1948). Because of the
prevalence in academics, the easily assessable score from 0 to 100, and the primary focus on adult reading materials instead of relation to school grade levels, we used the Flesch Index formula (Chall, 1958; Klare, 1963). A value of less than 30 means that a text is considered very difficult and is aimed at people with a university degree, while a value of over 50 to 60 is aimed at high school students (R. Flesch, 1949; DuBay, 2004). A score of 100 represents the equivalent of a primary school student and is considered as very easy. Since our survey was conducted in Germany and the participants, therefore, speak German as their native language, we use the Flesch Index translated for the German language, resulting in the following formula (Amstad, 1978):

Flesch Reading Ease Score Index = \( 180 - \frac{\text{Total Words}}{\text{Total Sentences}} - (58.5 \times \frac{\text{Total Syllables}}{\text{Total Words}}) \)

For the low readability scenario, we used a Flesch Index score below 30, for the high readability scenario we used a Flesch Index score of about 50 to ensure that we have significantly higher readability and simultaneously can convey all details of the data breach similarly and appropriately. Table 4 shows the scenario texts that were used.

<table>
<thead>
<tr>
<th>Response Strategy</th>
<th>Dimension</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apology</td>
<td>Apology</td>
<td>“We regret to inform you that there has been an incident regarding your personal and financial information. We sincerely apologize to you for this.”</td>
</tr>
<tr>
<td></td>
<td>No Apology</td>
<td>“We take information security very seriously and want to inform you about an incident concerning your personal and financial information.”</td>
</tr>
<tr>
<td>CEO visibility</td>
<td>“From: <a href="mailto:Frank.Schneider@smart-bank.de">Frank.Schneider@smart-bank.de</a>”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“I would like to inform you personally about the following”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“With kind regards. Frank Schneider, CEO Smart-Bank.”</td>
<td></td>
</tr>
<tr>
<td>CEO not visibility</td>
<td>“From: <a href="mailto:customerservice@smart-bank.de">customerservice@smart-bank.de</a>”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“With kind regards. Your Smart-Bank customer service”</td>
<td></td>
</tr>
<tr>
<td>High Readability</td>
<td>“On 01.08.2020 we became victims of a hacker attack, in which the attackers bypassed the protective measures by using a virus. During this attack various data was stolen and offered for sale in forums. Among them are also your account data.”</td>
<td></td>
</tr>
<tr>
<td>Low Readability</td>
<td>“On 01.08.2020 we became victim of an IT security attack in which unauthorized customer information, including yours, was compromised by means of a Trojan. The attackers bypassed RSA encryption by reading our private key from the database. This compromised data was then offered for sale in Internet forums.”</td>
<td></td>
</tr>
</tbody>
</table>

Table 4. Experimental Scenarios

Furthermore, each participant was assigned to one of eight different scenarios. The group size was approximately equally distributed (see Table 5).

<table>
<thead>
<tr>
<th>Apology</th>
<th>CEO visibility</th>
<th>Readability</th>
<th>Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apology</td>
<td>CEO visible</td>
<td>High</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>CEO not visible</td>
<td>Low</td>
<td>71</td>
</tr>
<tr>
<td>No Apology</td>
<td>CEO visible</td>
<td>High</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>CEO not visible</td>
<td>Low</td>
<td>72</td>
</tr>
</tbody>
</table>

Table 5. Scenario Distribution

5 Data Analysis and Results

To evaluate our data, we used the structural equation modelling (SEM) method. SEM is a statistical approach for testing hypothesis about relations among independent and dependent variables (Hoyle, 1995). It enables one to simultaneously test multiple relationships between constructs (Sarstedt et al., 2014). In line with current information systems and management research (Fombelle, Bone and Lemon, 2016; Trenz, Veit and Tan, 2020) we chose the partial least squares SEM over the covariance-
based SEM and other methods because it enables us to predict complex models with fewer observations while considering measurement errors and constructs with multi-dimensional structures (Jöreskog, K. G.; Wold, 1982; Bagozzi and Yi, 1988; Dijkstra, 2010; Rigdon, 2012; Sarstedt et al., 2014). Furthermore, due to the minor restrictive assumptions (Fombelle et al., 2016; Trenz et al., 2020), the model supports the experimental investigation of companies’ actual response actions. To calculate our model, we used SmartPLS3 software.

5.1 Measurement of Constructs

Except for CEO visibility, all items were derived by the literature and were adapted to our scenario context. The items for the construct CEO visibility were created based on the definition by (Turk et al. (2012). All items were carefully translated into German and used a 7-point Likert scale. For our control variables, we also used other scales, e.g., prior data breach experience was measured by a checkbox (“yes”? “no”) and age by a textbox. The latent measurement scales, the construct and item names and the corresponding loadings are listed in Table 6.

<table>
<thead>
<tr>
<th>Constructs and Items</th>
<th>Loadings</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO visibility (self-created, based on Turk et al., 2012; Sen Gupta et al., 2018)</td>
<td>0.928, 0.892</td>
</tr>
<tr>
<td>The author of the message holds a high position at Smart-Bank.</td>
<td>0.928</td>
</tr>
<tr>
<td>The CEO is the author of the message.</td>
<td>0.892</td>
</tr>
<tr>
<td>Apology (Liao, 2007)</td>
<td>0.853, 0.865, 0.754</td>
</tr>
<tr>
<td>Smart-Bank has apologized for what had happened.</td>
<td>0.853</td>
</tr>
<tr>
<td>Smart-Bank has apologized for the inconvenience the problem had brought.</td>
<td>0.865</td>
</tr>
<tr>
<td>Smart-Bank expressed regret for the mistake the company had made.</td>
<td>0.754</td>
</tr>
<tr>
<td>Readability (Goe and Chengalar-Smith, 2010)</td>
<td>0.832, 0.912, 0.689</td>
</tr>
<tr>
<td>The text is easy to understand.</td>
<td>0.832</td>
</tr>
<tr>
<td>The text presented the information clearly.</td>
<td>0.912</td>
</tr>
<tr>
<td>The text contains few or no IT security specific words.* (dropped due to low factor loading)</td>
<td>n.a.</td>
</tr>
<tr>
<td>No high technical understanding is necessary to understand the text.</td>
<td>0.689</td>
</tr>
<tr>
<td>Satisfaction (Goodwin and Ross, 1992; Kantsperger and Kunz, 2010; Park and Park, 2016)</td>
<td>0.927, 0.939, 0.930</td>
</tr>
<tr>
<td>I was satisfied with the way that this company has handled complaints and problems</td>
<td>0.927</td>
</tr>
<tr>
<td>Overall, I am satisfied with Smart-Bank’s reaction to the security incident.</td>
<td>0.939</td>
</tr>
<tr>
<td>I had good experiences with Smart-Bank’s reaction.</td>
<td>0.859</td>
</tr>
<tr>
<td>I was pleased with the way Smart-Bank reacted to problems.</td>
<td>0.930</td>
</tr>
<tr>
<td>Long-term Satisfaction (Kuo and Wu, 2012; Goode et al. 2017)</td>
<td>0.961, 0.957, 0.930</td>
</tr>
<tr>
<td>I intend to continue using Smart-Bank’s services in the future.</td>
<td>0.961</td>
</tr>
<tr>
<td>I plan to continue using the services of Smart-Bank.</td>
<td>0.957</td>
</tr>
<tr>
<td>Chances are high that I will use the services of Smart-Bank.</td>
<td>0.930</td>
</tr>
</tbody>
</table>

Table 6. Operationalization of Constructs (Items are Translated from German)

5.2 Measurement Validation

In order to assess our reliability and convergence validity, individual-item reliability (IIR), composite reliability (CR) and average variance extracted (AVE) are evaluated (Hildebrandt and Homburg, 1998). After removing one item from the readability scale, all items sufficiently load on their respective construct. In sum, we observe a sufficient level of IIR. The requirements of the AVE are met if the constructs exceed a value higher than or equal to 0.5 (Hair et al., 2011). Furthermore, if constructs are above a value higher than 0.7, the requirements of the CR are met (Bagozzi and Yi, 1988). In Table 7, our model illustrates that both the CR and the AVE exceed the required minimum limits. An approach to assess the discrimination validity is to apply the Fornell/Larcker criterion (Fornell and Larcker, 1981; Hair et al. 2011). Using the approach, the square root of the AVE of each construct is compared with the correlations between the construct with other constructs (Fornell and Larcker, 1981). It can be shown that all square roots of the AVE of the constructs are higher than the correlations of the constructs.
Overall, a reliable estimation of our model can be assumed. The constructs could be measured for validity and reliability using AVE and CR and showed in each case that our model meets the criteria.

5.3 Hypotheses Testing

To assess the significance of the paths in the SEM, Hair et al. (2011) recommended using the bootstrapping method with at least 5000 samples. The results of this both calculations are shown in Figure 2.

![Structural Model with path coefficients](image)

Unless H3b (readability on cumulative satisfaction) which was significant at .01 with a path coefficient by .078, all other hypotheses were significant at least at .05. In detail CEO visibility has a significant positive effect on transactional satisfaction (.148; p < .01) and cumulative satisfaction (.122; p < .05). Furthermore, apology has a significant positive effect on transactional satisfaction (.358; p < .01) and cumulative satisfaction (.155; p < .01). In addition, readability has a significant positive effect on transactional satisfaction (.213; p < .01).

Among the control variables we used age, gender, education, work experience and data breach experience, we found no significant effect on transactional satisfaction or cumulative satisfaction. Common Method variance was analysed using three markers. No significant effect on the constructs could be identified. Thus, it can be stated that all hypotheses can be supported.

6 Discussion and Implications

This paper examines the effect of apology, CEO visibility, and readability as response actions for data breaches. Especially the positive impact of these response actions on the transactional and cumulative satisfaction was examined. The effect strength can be measured using the path coefficients and the significance tests (Suhr, 2006). It is shown that the different response messages have different effects on short-term, i.e., transactional, satisfaction and long-term, cumulative satisfaction. Overall, the apology has a large effect on both transactional and cumulative satisfaction. The visibility of the CIO also has a strongly significant effect on transactional satisfaction and a moderately significant effect on cumulative satisfaction. Likewise, it is with the readability, this has a large effect on transactional satisfaction, has a small long-term effect, however. Nevertheless, apology, CEO visibility and readability have positive impacts on transactional and cumulative satisfaction. In the context of data breaches, little research has been conducted on the impact of justice theory and SCCT response
strategies on data breaches. Hence, this paper provides theoretical and practical implications. However, there are also some limitations and opportunities for further research.

6.1 Contributions to Literature

This paper offers a theoretical contribution. First, while there are conflicting views in the service literature as to whether satisfaction should be assessed by two different concepts of transactional and cumulative satisfaction (Tax et al., 1998; Gelbrich and Roschk, 2011), we were able to show that differentiation of these certainly merits consideration in the context of data breaches. Substantial deviations in the influence of response strategies on transactional and cumulative satisfaction can be observed, which leads to an implicit assumption about the heterogeneity of these satisfactions’ levels. Our research paves a way for the literature to address these satisfactions in other response actions domains. Furthermore, our research allows for a more nuanced view of customer satisfaction in the context of data breach response actions. It can be investigated to what extent the transactional different to the cumulative satisfaction impacts on customers and on the business capability of the affected company. An examination of these, in turn, might have implications for the recommendations of specific response actions that companies should apply to achieve desired results.

Second, the results allow a better understanding of the impact of traditional crisis response strategies such as the SCCT in the context of data breaches. In particular, the effect of transparency and clarity, which was reflected as readability in this study, has not yet been explored in the field of data breaches and can therefore complement the SCCT by this aspect. In addition, it can be shown that the combination of a visible CEO and low reading complexity leads to a positive attitude towards the company. Therefore, our study also contributes to the existing literature in impression management, which shows that a conscious increase in readability is also an adequate response strategy in the context of data breaches and can lead to positive reactions. By successfully examining the concepts from the crisis management literature, we continue to open the way for future researchers to explore what specific differences and similarities exist between this and the data breaches research stream.

6.2 Practical Implications

In addition to the theoretical contribution, the present study also provides practical implications. The results can help companies to optimize the strategies for their future communication after a data breach and help them to achieve the best possible outcome in case of a data breach. The results can support companies in developing communication strategies in the event of a data breach and positively influence long-term customer relationships. A properly designed response strategy is crucial. It can have a positive effect on the perception of the company’s communication strategy and overall satisfaction. It can be shown that the content of the response strategy has a direct influence on the impact of the communication strategy. As previously discussed, companies’ data breach response strategies, which can already be found in reality, always contain three basic building blocks: 1. the company’s behaviour, which is determined by whether the company acknowledges the data breach and takes responsibility by apologizing to its affected customers; 2. the intention of the company to make the data breach and its consequences understandable to the customer, which is determined by whether the message is readable and clearly formulated for the general public; 3. the expression of the importance of the data breach, which is determined by who addresses the customer in the response message. Thus, it is of relevance in the run-up to a data breach to consider how a company wants to design these three components. The results of the present study show that it is sensible for companies to act in the interests of their customers and therefore be open and apologize to them, explain the data breach in simple terms and assign it a high level of importance by sending the response from, e.g., the CEO. It can be shown that even in events of serious data breaches, such as in this case a data breach in banking, open communication with an emphasis on the importance of the incident has a positive effect on the short-term and long-term relationship of the company. It also shows that the actions of the strategy have different strong effects on customer behaviour. In the short-term context (transactional satisfaction), it is therefore highly positive for companies to show constructive behaviour with good
intentions and high importance. However, if one looks at the long-term customer relationship (cumulative satisfaction), it can be shown that especially an apology from the company also has a long-term positive correlation with satisfaction. It must also be mentioned that the emphasis on importance by the CEO results in positive long-term effects that should not be neglected. While the comprehensibility of the message has a positive effect in the short term, its positive impact on long-term satisfaction is weak. That’s why companies should decide individually based on the data breach whether it makes sense to explain it understandably or whether a complex, difficult to read message has more advantages for them.

6.3 Limitations and Opportunities for Future Research

Our study has some limitations that need to be considered when interpreting the results and providing future research opportunities. Even if the participants of the experiment were familiar with online banking and could put themselves in the situation, the experiment was based on a fictitious data breach situation. Therefore, future studies should also include a comprehensive validation of measurements where participants are affected by a data breach of a digital banking app. In addition, participants in the study were given different scenarios containing the elements apology, CEO visibility and readability in low or high form. It cannot be ruled out that a different choice of wording would have had a different effect on transactional and cumulative satisfaction. Particularly in the construct of readability, there is the additional difficulty that readability could only be reduced significantly with difficulty. Even a readability score of 50 is comparatively low (requires a high school diploma). The main problem was to create a text with lower readability but with the same content and length to exclude other factors. In terms of length, another factor could be a positive visual effect of shorter texts on satisfaction. Therefore, generally different lengths and formulations of readability, as well as apology and visibility, should be tested. For example, visibility could be tested in addition to other personalities in the company, such as the CIO or Chief Privacy Officer. In addition to transactional and cumulative satisfaction, which was studied exclusively as directly dependent variables, and although differences between the two satisfaction concepts were found, future researchers should explore the effects of their mediation on variables of loyalty, WOM or trust in order to achieve a discriminating delineation between them. An identification of varying effects could then, in turn, lead to a better assessment of response strategies. While the focus of this paper was primarily on the basic structures of a response strategy, it has already been shown that these are far more multifaceted (Bansal and Zahedi, 2015; Goode et al., 2017; Breach et al., 2020). For example, other response strategies of the SCCT, such as denial, scapegoat, justification, admonition, and sacrifice (Coombs, 2007), could be examined. A thorough investigation could provide a more comprehensive insight into the response strategies to data loss and their impact on consumers.

7 Conclusion

This study examines the impact of the response actions apology, readability, and CEO visibility after a data breach on transactional and cumulative satisfaction. 567 participants were surveyed on a data breach and the bank’s response strategy using a 2x2x2 vignette design. A structural equation model was used to identify the effects. The results of this study provide important insights into the effects of strategies and their action components on the satisfaction after a data breach, both in the long and short-term. It could be shown that an apology, as well as the visibility of the CEO and high readability of the strategy, have a strong positive effect on the satisfaction with the strategy. In addition, positive effects on the long-term satisfaction with the company were found in all response actions, although only the apology has a strong positive effect. In summary, it can therefore be concluded that the results of the study add new insights to the existing literature, as they complement aspects on the effect of response actions on the satisfaction dimensions and thus offer an opportunity for practical application.
Openness Always Pays Off

References


Openness Always Pays Off


*Twenty-Ninth European Conference on Information Systems (ECIS 2021), [Marrakesh, Morocco]*
22(3), 419–445.