Electronic Markets (2021) 31:829–848
https://doi.org/10.1007/s12525-021-00490-3

RESEARCH PAPER

What to do after a data breach? Examining apology and compensation as response strategies for health service providers

Kristin Masuch[1] · Maike Greve[2] · Simon Trang[1]

Received: 31 July 2020 / Accepted: 5 July 2021 / Published online: 17 November 2021

Abstract

Innovative IT-enabled health services promise tremendous benefits for customers and service providers alike. Simultaneously, health services by nature process sensitive customer information, and data breaches have become an everyday phenomenon. The challenge that health service providers face is to find effective recovery strategies after data breaches to retain customer trust and loyalty. We theorize and investigate how two widely applied recovery actions (namely apology and compensation) affect customer reactions after a data breach in the specific context of fitness trackers. Drawing on expectation confirmation theory, we argue that the recovery actions derived from practice, apology, and compensation address the assimilation-contrast model's tolerance range and, thus, always lead to satisfaction with the recovery strategy, which positively influences customers' behavior. We employ an experimental investigation and collect data from fitness tracker users during a running event. In the end, we found substantial support for our research model. Health service providers should determine specific customer expectations and align their data breach recovery strategies accordingly.

Keywords Health data breach recovery action · Data breach response strategies · Compensation · Apology · Expectation confirmation theory · Assimilation-contrast model

JEL classification I12

Introduction

Internet-enabled innovations and applications have opened up new opportunities to expand and improve market potential in all industries (Cavusoglu et al., 2004). The healthcare industry also has experienced this trend, which supports its tasks primarily through digital applications, including the use of mobile devices to track personal activity levels. Professional athletes and normal people (Kim & Kwon, 2019; Piwek et al., 2016) use this technology to achieve personal self-optimization, such as improved physical performance and positive habits (Piwek et al., 2016), as well as to monitor personal health status and prevent or control diseases (Greve et al., 2020). Such goals can be achieved by tracking personal data, including number of steps taken, geolocation, or heart rate (Chuah et al., 2016).

However, to enjoy the many uses and benefits of intelligent technology, consumers need to share their personal data with service providers. This technology enables necessary intermodal connectivity and pocket-size functionalities that previously required multiple devices.

Responsible Editor: Ulrich Reimer.

This article is part of the Topical Collection on Digital Healthcare Services

✉ Kristin Masuch
kristin.masuch@uni-goettingen.de

Maike Greve
maike.greve@uni-goettingen.de

Simon Trang
strang@uni-goettingen.de

[1] Chair of Information Security and Compliance, University of Goettingen, Platz der Göttinger Sieben 5, 37073 Göttingen, Germany

[2] Chair of Information Management, Digital Health Research Group, University of Goettingen, Humboldtallee 3, 37073 Göttingen, Germany

As a result, it has become a common practice to use such devices (Piwek et al., 2016), and this trend's popularity can be seen in the market demand for fitness trackers and smartwatches, among other such technology (Chuah et al., 2016). However, this technology's many benefits come with a high risk of cyber-attacks on systems. It has been shown that, especially in mobile digital health gadgets, incidents of information security breaches rising sharply and breaches are observed almost daily (Cavusoglu et al., 2004; Liu & Sun, 2016; McLeod & Dolezel, 2018).

Particularly in the health industry and explicitly with fitness trackers, data breaches represent a high risk (Liu & Sun, 2016; Mousavizadeh et al., 2016). This is based on two aspects. First, fitness trackers are particularly vulnerable due to their interconnectivity and mobile data transfers (Piccoli et al., 2018). Second, fitness trackers collect highly sensitive personal health data that include medical data, though they do not officially belong to the category of medical apps that must follow legal regulations for medical devices. Therefore, they are not subject to strict security guidelines (Behne & Teuteberg, 2020), making them a perfect target for attacks.

The healthcare industry has acknowledged this high risk of data breaches, being the industry with the largest financial losses following data breaches, exceeding US$7 million (Digital Guardian, 2018). Investigated data breaches negatively impact the affected company's market value (Cavusoglu et al., 2004) and can damage customers' trust and the company's reputation (Goel & Shawky, 2009). Such data breaches have affected the entire industry adversely (Cavusoglu et al., 2004).

In addition to this phenomenon's increasing urgency, characteristics that influence the negative consequences' severity have been identified. For example, effects on a company's market value can differ depending on the data breach's severity (Morse et al., 2011). Furthermore, it was found that the data breach's characteristics and how the affected company reacts impact market value, e.g., a significantly negative impact on market value could occur if the company apologizes for a data breach.

However, costs incurred after a data breach do not all involve loss of market value, but instead entail business losses caused by the decrease in customer trust and loyalty after a data breach. These costs can be felt years after the initial incident (Ponemon Institute LLC, 2018) and are indirect, including brand damage and negative customer sentiment (Sherr & Wingfield, 2011), which lead to customers terminating their relationship with the company. Some companies have reported customer losses of up to 40% after a data breach (Ponemon Institute LLC, 2013). Few studies have addressed strategies that companies can employ in the wake of such breaches to manage their effects and minimize them.

Recent research has made significant advances in understanding data breach response strategies by applying insights from service failure literature to data breaches, creating a link between marketing communications literature and crisis response literature (Goode et al., 2017; Malhotra & Kubowicz Malhotra, 2011). The basic idea behind this is that data breaches can occur in the form of an electronically transmitted service failure, which the customer experiences as a disruption in core service provision. Therefore, the notion of how a service provider can recover after a service failure and restore its reputation (McColl-Kennedy & Sparks, 2003; Patterson et al., 2006) can be applied to the data breach context. For example, Goode et al. (2017) examined compensation as a recovery action after a data breach, drawing on the perspective of Mattila and Cranage (2005), who found that compensation (and apology) positively influence perceptions of fairness, which are related positively to satisfaction. In addition to this basic construct, customer expectations also have been identified as important antecedents in influencing user satisfaction with privacy breach responses (Berezina et al., 2012). It becomes clear that although efforts have been made to transfer literature on service failures to the context of data breaches. However, a research gap remains as a lack of a deeper understanding of the effectiveness of various responses to customer behavior following a data breach.

In examining typical recovery actions after a data breach, one finds that the compensation suggested by Goode et al. (2017) was a unique recovery action that was not adopted as a common response among companies after a data breach. It elicits disconfirmation from customers and is, therefore, outside the assimilation-contrast model's tolerance range, which is positive in this case. However, the literature lacks deeper insights into how different recovery actions function in real-world settings following a data breach and thereby allowing companies to reassure customers after a data breach as efficiently as possible. In addition, the question arises as to whether it is desirable to address the tolerance range of assimilation-contrast model. After all, it is not clear whether a reaction that causes customers to fall within the assimilation-contrast model's tolerance range actually exerts a positive long-term effect on customer behavior and, thus, on negative indirect costs, such as lost trust, loyalty and word of mouth.

To determine which recovery actions are applied commonly in the context of data breaches and should be studied, we examined real-world data breaches at publicly traded U.S. companies from 2007 onward using the Privacy Rights Clearinghouse and identified and coded related response strategies. Based on a database of 72 healthcare data breaches with response strategies, two strategies—compensation and apology—were identified as relevant common practices in the context of health data breaches. Since when considering recovery actions after data breaches designed to address and engage the customer directly, apologies and compensation are the most commonly used recovery actions used by companies affected by a confirmed data breach.

Therefore, it is crucial to investigate the actual impact from a typical compensation and apology in context. Furthermore, it is important to determine how a successful recovery action can influence customer perceptions. For this purpose, in addition to actual recovery actions and the influence from existing expectations, this research examines the following research question:

RQ How do typical compensation and apology as recovery actions by a health service provider influence customers' reaction to a data breach?

We address this question using a fitness tracker company's recovery actions after a data breach. For this purpose, a survey was conducted on 507 users of fitness trackers at a local sports event based on a data breach scenario. For this purpose, it was ensured that the fitness tracker users accepted that the device would collect their health data, which includes tracking GPS data from running tracks, monitoring heart rate, and displaying calories burned. Also, personal information such as gender, age, and name is collected the first time the device is used.

Our study contributes to healthcare and security literature, providing insights explicitly into security issues in digital health. First, we put the assimilation-contrast model into a general theoretical context with data breaches and further showed a positive correlation to other dependent variables (trust, loyalty, word of mouth) from the tolerance range of the model. Second, we extended the literature on data breach recovery actions to include other actions used in practice and their impact on customer behavior after a data breach. Third, our study adds to the existing literature on healthcare security by illustrating how customer responses can be explained, mainly to help healthcare providers determine recovery actions for their customers in response to data breaches. Fourth, we were able to show that the context of service failure is also applicable to health data breaches.

In addition to theoretical contributions, several practical implications from our study provide essential insights into customer responses at an individual level, as the perceived recovery actions influences customer behavior after recovery. Our results can help companies and managers determine their customers' expectations after a data breach and find suitable strategies for expectations. They also enable companies to repair damaged relationships with their customers.

Practical background and related research

Review of data breach response strategies research

Few studies in extant literature have examined how companies should respond after a data breach. Consequently, it can be assumed that companies are likely to rely on findings from general crisis management literature when responding to a data breach (Gwebu et al., 2018). However, providing an appropriate response to a data breach poses a significant challenge, especially given that there is often some uncertainty about what has happened, and legal requirements necessitate disclosing data breaches quickly (Masuch et al., 2020). Although companies have been responding to data breaches for years, little research has been done on how these data breach responses, derived from crisis response strategies, work in context.

A few existing studies have examined actual data breach responses and their effects on stock prices. For instance, Gwebu et al. (2018) examined the effects from response strategies after a data breach as to whether a company has a good reputation. Based on 221 data breaches, the strategies in responding to breaches were categorized into defensive, accommodative, moderate, and image renewal. Based on the companies' reputations, the impact on their stock prices was examined. For companies with solid reputations, the response strategies to a data breach did not affect their market value, while the opposite occurred for companies with poor reputations.

Here, differences in market value after a data breach can be identified based on the response strategy. The moderate (ingratiation or justification) and image renewal (correction commitment, stakeholder, or value commitment) strategies appeared to affect the company's market value positively, an effect that could be confirmed. Simultaneously, the defensive (denial or excuse) and accommodative (apology or remedial action) strategies appeared to exert a negative impact on stock price, an effect that could not be confirmed with statistical significance.

Masuch et al. (2021) expanded on this research by categorizing response strategies differently, considering the underlying response and recovery actions in response strategies and considering whether it makes a difference whom the data breach affects. Thus, a distinction is made between response and recovery actions. Companies' response actions in the present study's context focus on whitewashing data breaches, in which, similar to Gwebu et al. (2018), such incidents are denied or downplayed, or responsibility is not accepted. In contrast, recovery actions involve the company directly addressing the customer, apologizing, and showing remorse. The research indicated that data breach responses only impact the context of customer-related data breaches, and that the whitewashing response action did not elicit a negative impact on the company's market value, whereas the apology recovery action elicited a negative impact.

On the other side of data breach research, instead of direct financial losses due to the negative impact on stock price, the immense financial losses from the loss of the company-customer relationship are considered.

After all, the responses to a data breach are not intended to address shareholders exclusively and, thus, the company's stock value, but often serve as a means to respond to those affected directly from the breach. Thus, response strategies often are used to appease customers after an incident and make them feel like they have been compensated for any losses (Grönroos, 1988). In addition to providing information about the incident, as discussed earlier, responses can include recovery actions designed to reassure those affected and stabilize their relationship with the company (Goode et al., 2017).

In this area, little research has addressed such actions' impact on customer behavior after a data breach and has attempted to find positive influencing factors. For example, some companies offer customers compensation for their losses in the form of a monetary compensation or a non-monetary equivalent (Goode et al., 2017). Extant research has demonstrated that compensation positively impacts customer attitudes, thereby averting negative impacts (e.g., Goode et al., 2017; Kude et al., 2017).

For the present study, the literature has examined existing response strategies with response actions and recovery strategies to data breaches. Response actions try to defend the company, whereas recovery actions try to address the damaged customer and repair the relationship. Actual recovery actions have been studied in terms of effects on stock price, while other research has examined recovery actions' impact on the company's relationship with customers. Thus, extant research is lacking on how actual recovery actions used after a data breach affect the company-customer relationship and whether they influence it positively.

Practical review of data breach recovery actions in healthcare

As mentioned earlier, the healthcare industry is a branch of particular importance with unique challenges. It involves managing highly sensitive personal health data and experiences public and political pressure to adopt new technological practices, particularly when surrounding infrastructure is not secure (Angst et al., 2017). Regulation and public concerns underline this industry's sensitivity and pressure healthcare providers to secure patient data and comply with regulations (Kwon & Johnson, 2015).

However, existing research indicates that the healthcare industry lags in security strength (Kruse et al., 2017) and experiences security incidents, such as data breaches, daily (McLeod & Dolezel, 2018). Although this area is relevant to study, little research has focused on the consequences from such incidents. However, considering that data breaches in particular are unavoidable and always become public knowledge due to mandatory disclosure requirements, it is imperative to address cost-effective ways to mitigate harm.

To identify how companies in the healthcare industry have attempted to address the consequences of data breaches so far, we examined data breaches in the healthcare industry since 2007 and coded the response strategies (please see Appendix 1 for details).

We identified 72 data breaches at publicly traded U.S. companies in the healthcare industry between 2007 and 2019, all of which were required to communicate their data breaches to those affected due to legal regulations.

The responses observed here follow the typical spectrum of crisis response strategies that are possible under the legal requirements. Thus, none of the companies denied that the data breaches occurred.

In 57 of the 72 companies' responses, they tried to defend themselves by downplaying, or trying to justify the data breach. It already has been demonstrated that this type of strategy positively affects a company's stock price and, therefore, often is used to protect the company (e.g. Masuch et al., 2020). Nevertheless, it must be noted that this type of strategy focuses more on addressing losses in stock value and less on losses in reputation and customers (Masuch et al., 2020).

However, in the context of data breaches, it already has been demonstrated that the main, long-term cost is the loss of reputation and company-customer relationships. In addition, a wide range of other companies is involved, from health insurers to fitness trackers, i.e., customers changing companies is quite realistic. Therefore, companies' remaining response strategies include recovery actions and demonstrate a more understanding, customer-oriented approach that attempts to stabilize the company-customer relationship (Ponemon Institute LLC, 2018). Overall, 38 of the 72 companies offered their customers compensation or apologized to them. Table 1 provides a short outline of selected data breaches in the health sector, demonstrating how companies use these two recovery strategies: apology and compensation.

In 2013, DaVita Inc.—which provides kidney dialysis services through a network of 2753 outpatient dialysis centers in the U.S., serving 206,900 patients, and 259 outpatient dialysis centers in 10 other countries, serving 28,700 patients (DaVita Inc., 2020)—experienced a data breach when an employee's laptop was stolen. The stolen information included names; health information such as diagnoses, insurance benefits, and dialysis treatment information; and Social Security numbers. The company offered a year of free credit monitoring as compensation for its affected customers (DaVita Inc., 2013).

UnitedHealth, a healthcare company that offers healthcare products and insurance services, discovered that one of its employees was suspected of participating in identity theft activities in 2007. Sensitive personal information on 127 customers was found in the suspect's possession, including Social Security numbers, names, addresses, and dates of birth. Considering their obligation to protect all customers, the company offered a 1-year subscription to Equifax Credit Watch Gold (which provides daily credit file monitoring, identity theft insurance, and copies of credit reports) to all members whose data could have been accessed by the employee in the past 2.5 years (United-Healthcare, 2007).

Table 1 Apology and compensation in recent health data breaches

Instantiation	Examples	Response Strategy
Compensation Material or immaterial payments that a customer receives in exchange for losses from a data breach	DaVita Inc On 09.07.2013, an employee's laptop was stolen, resulting in personal health data—including diagnoses, etc., from 11,500 patients—being breached (DaVita Inc., 2013)	Free credit monitoring was offered as a compensation strategy
	UnitedHealth Group Inc On 07.25.2007, personal information on 127 customers was found in a suspect's possession. This personal information included names, addresses, dates of birth, and Social Security numbers (UnitedHealthcare, 2007)	As a compensation strategy, a one-year subscription to Equifax Credit Watch Gold was offered
Apology A sympathetic way to announce that a data breach has occurred	Medtronic On 10.11.2018, unauthorized access occurred in connection with protected health and other personal information on 12 New Hampshire residents (Medtronic, 2018)	The company explained the incident and apologized for it
	Quest diagnostics On 11.17.2017, personal information on employees was breached via mail (Quest Diagnostics, 2015)	The company explained and apologized for the incident

In 2018, Medtronic, an Irish medical device company that generates most of its sales from the U.S. healthcare system, discovered that employees misused customer information. The company apologized publicly to the affected customers (Medtronic, 2018).

In 2014, at Quest Diagnostics, a U.S. clinical laboratory, an employee sent out a report that contained employee data via mail to business partners outside the company. The data—including names, addresses, Social Security numbers, dates of birth, employee IDs, and mail addresses—were misused. The company apologized publicly for the incident (Quest Diagnostics, 2015).

For this study's purposes, the practically studied data breaches in the healthcare industry indicate that companies followed crisis response theory regarding their response strategies to data breaches. In the area of recovery actions for customers, compensation and apology were used. In addition, no research in this context has been conducted regarding the actual impact from responses transferred from the crisis response. Thus, research is lacking on how compensation and apology, as recovery actions, affect the company-customer relationship in the healthcare industry.

Theoretical framework

Building on the practical background and drawing on the related research, we created a theoretical framework and derived hypotheses based on expectation confirmation theory.

Expectation confirmation theory as a theoretical lens

Expectation confirmation theory has existed for several decades and first appeared in psychology and marketing literature (Oliver, 1977, 1980). It has been researched in other disciplines over time, including information systems (IS) (Bhattacherjee, 2001; Brown et al., 2014; Venkatesh & Goyal, 2010).

The theory attempts to explain and predict a customer's repurchase intention and satisfaction levels by comparing their expectations with perceived performance (Oliver, 1977). This comparison leads to confirmation or disconfirmation, and ultimately to customer satisfaction or dissatisfaction. This final (dis)satisfaction level has been found to be a determinant of repurchase intention (Oliver, 1980). This relationship between satisfaction and purchase intention has been extended in recent literature to include other dependent variables. The IS literature shows, for example, that the resulting satisfaction, from the confirmation in expectations and experiences, has a positive effect on the continuance intention in IT (Bhattacherjee, 2001; Islam et al., 2017). Furthermore, this satisfaction also has a positive correlation in loyalty or trust when using websites (Flavián et al., 2006; Valvi & West, 2013) or also a positive word of mouth in the context of service convenience (Dai et al., 2008).

However, recent literature on information systems now examines this basic theory using four competing models:

generalized negativity; assimilation; contrast; and assimilation-contrast (Brown et al., 2014; Goode et al., 2017).

The generalized negativity model, developed from the fulfilled expectations hypothesis, asserts that positive or negative disconfirmation negatively affects resulting outcome evaluations (Irving & Meyer, 1994; Wanous et al., 1992). The resulting effect from any discrepancy in expectations, whether positive or negative, results in negative consequences, as demonstrated by Venkatesh and Goyal (2010) in the IS context during technology use.

The assimilation model is based on the rationale that disconfirmation is avoided to some extent by adjusting outcome evaluations to reduce cognitive dissonance (Sherif & Sherif, 1965). For example, it has been evaluated by Szajna and Scamell (1993) in the context of satisfaction with a system. They demonstrated that users' satisfaction level with the same system was higher when expectations were set high than when expectations were set low.

Unlike the assimilation model, the contrast model's underlying idea involves understanding outcome ratings as a function with the size and direction of the gap between expectations and experiences in a robust potential disconfirmation (Churchill & Surprenant, 1982; Patterson et al., 1996). Compared with the assimilation model, it is not the cognitive dissonance, but the difference between expectation and evaluation that is crucial. If the difference here is positive, it elicits positive effects and vice versa. The model also is anchored in IS research, e.g., Staples et al. (2002) found support for the contrast model in the context of system satisfaction and effectiveness.

The assimilation-contrast model combines the main ideas from the assimilation and contrast models. It assumes that when a small difference exists between expectations and experiences, the evaluation will adjust. Thus, the assimilation model follows the divergence of expectations and experiences within a certain tolerance range. However, if the difference turns out to be too large, the model follows the contrast model's idea, with positive differences eliciting positive effects and negative differences eliciting negative effects (e.g., Becker et al., 1992; Johnston, 1995; Klein, 1999). The assimilation-contrast model has been demonstrated and developed several times in IS research, e.g., Brown et al. (2012) found support for the model in software use. It was demonstrated that smaller disconfirmations between expectations and experiences led to the assimilation of expectations and positively affected software use. Large positive disconfirmations exerted the same effect. By comparison, large negative disconfirmations led to less software use (Brown et al., 2012).

In doing so, Brown et al. (2012) also introduced the modified assimilation-contrast model, which also builds on prospect theory and suggests that negative disconfirmation exerts a more substantial impact than positive disconfirmation. Brown et al.'s (2012) modified model also was validated across several dependent variables (intention, usage, and satisfaction) and also applied to Goode et al.'s (2017) data breach context.

In transferring the assimilation-contrast model, Goode et al. (2017) pointed out that it already is used increasingly in service failure literature to adjust customer expectations regarding compensation after a service failure. Their study investigated a Sony PlayStation network breach using the modified assimilation-contrast model and the generalized negativity model. They examined hypotheses concerning compensation's impact on key customer outcomes after a major data breach and the resulting efforts to restore service. Expectations and experiences with compensation as a recovery action were examined as precursors to the perception of service quality, intention to continue, and intention to purchase.

It could be demonstrated that the modified assimilation-contrast model is applicable for the service quality and continuance intention, and that the tolerance range, as well as the positive and negative effects from large disconfirmation in the data breach context, can be proven. The generalized negativity model again can explain repurchase intention in a data breach with the corresponding effects. Overall, the study demonstrated that expectation confirmation theory explains the perception of service quality and intention to continue and repurchase.

In summary expectation confirmation research indicates that in IS research there are limited competing model of expectation confirmation theory examined. Nevertheless, it should be noted that the assimilation-contrast model holds particular prominence, particularly in recent research, as it already has been applied to the context of data breaches relevant to the present study and has demonstrated that the effect's mechanism is applicable.

However, it leaves open the question of how more typical response strategies that follow the usual pattern of data breach recovery actions interact, what influence those strategies exert on satisfaction with the response, and the long-term effects on the company-customer relationship, particularly in the healthcare industry.

In contrast to Goode et al. (2017), the present study is not intended to measure how differences in expectation (dis)conformation affect direct effects on customer behavior. Instead, it aims to investigate how expectations and (dis)confirmation of expectations affect satisfaction with commonly used recovery actions after a healthcare-related data breach and how they affect customer behavior.

Hypotheses derivation and theoretical framework development

For this study's purposes, our research model considers expectations of a recovery actions after a data breach and the actual perceived experience (recovery actions) to explain satisfaction with it, as well as long-term customer behavior—as measured by word of mouth, loyalty, and trust—through satisfaction with the recovery action (see Fig. 1).

In addition to basic ideas from expectation confirmation theory, the results from Bhattacherjee (2001), Brown et al., (2012, 2014) and Goode et al. (2017) in particular are used to derive hypotheses and develop the research model.

To identify the effect from expectations, it is essential to build on Goode et al.'s (2017) results, in which an offer of compensation is a unique, unprecedented, and practically rarely used type of recovery action. Thus, it suits the underlying assumptions to follow the effects from the modified assimilation-contrast model.

It is based on the idea that small discrepancies between expectations and experiences are treated differently than larger discrepancies (Brown et al., 2014). Thus, it suggests that a slightly high, accurate, or slightly low expectation is preferable to an excessively high/low one (Brown et al., 2014), considering that the smaller the discrepancy between expectations and experience, the smaller the negative influence from experience. An explanation for this can be found when the difference between the experience rating and expectation is small, and expectations can be assumed to be inertial, causing the experience to be assimilated toward the outcome rating (e.g., Johnston, 1995). In contrast, when differences are large, contrast is weighted more heavily, and disconfirmation prevails (e.g., Klein, 1999).

Thus, considering only the relationship between expectations and experiences, we note that experiences always are measured against expectations. Unless complete confirmation occurs, the evaluation process always is negative, considering that a discrepancy, whether positive or negative, indicates a non-confirmation effect.

Thus, it can be assumed that these effects mainly are due to the surprise effect on affected individuals, considering that they are not aware of any comparable recovery actions in response to a data breach from their experience. Unlike Goode et al. (2017), we build on typical, commonly used recovery actions derived from actual responses by companies that have experienced a data breach. Thus, we can assume that a comparable recovery action causes only minor disconfirmations. Therefore, we hypothesized the following:

H1 Users' expectation of a data breach recovery action is associated negatively with a confirmation.

As defined in the previous hypothesis, we examined typical, commonly used recovery actions after a data breach in the healthcare industry. From the practical derivation of recovery actions in the healthcare industry, it was found that the two most commonly used recovery actions are apology and compensation. Considering that data breaches have become an everyday occurrence, and that companies must disclose data breaches and often resort to apology, compensation, or a combination of the two (Masuch et al., 2021), it can be assumed that customers who are offered such a recovery action with wording similar in practice are less surprised. Thus, this effect follows the assimilation-contrast model in the tolerance range, i.e., an offered and expected recovery action positively affects the confirmation between expectation and experience. This resulted in the following two hypotheses:

H2a After a data breach, a typical compensation is associated positively with confirmation.

H2b After a data breach, a typical apology is associated positively with confirmation.

Thus, it can be assumed that expectations are a determinant of satisfaction with recovery action. This effect is based on the fact that expectations can be viewed as a kind of reference level for the customer toward the experience (Brown

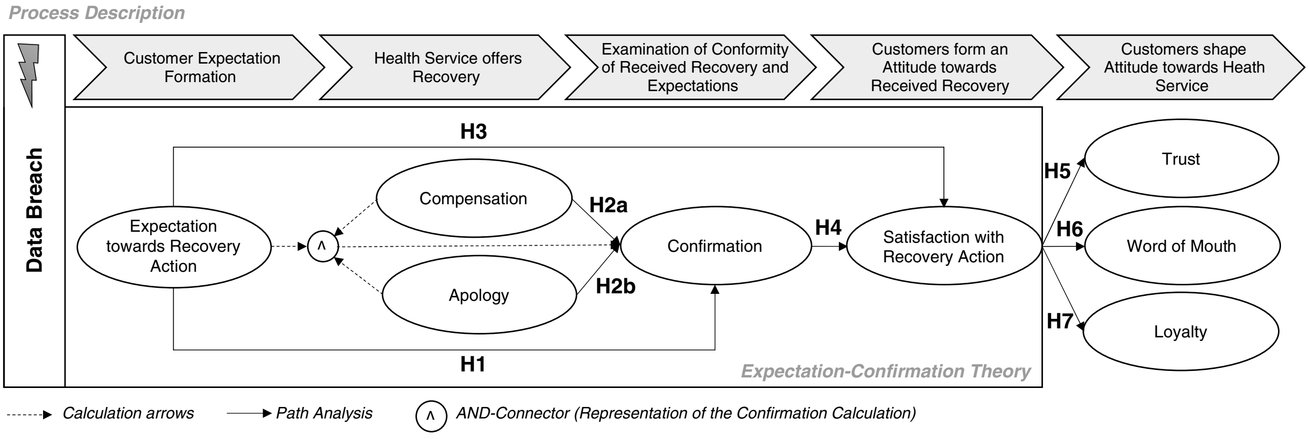
Process Description
Customer Expectation Formation
Health Service offers Recovery
Examination of Conformity of Received Recovery and Expectations
Customers form an Attitude towards Received Recovery
Customers shape Attitude towards Heath Service
Data Breach
H3
Compensation
H2a
Expectation towards Recovery Action
∧
Confirmation
H4
Satisfaction with Recovery Action
Apology
H2b
H1
Expectation-Confirmation Theory
H5
Trust
H6
Word of Mouth
H7
Loyalty
Calculation arrows
Path Analysis
∧
AND-Connector (Representation of the Confirmation Calculation)

Fig. 1 Research model

et al., 2014). Therefore, high expectations tend to increase satisfaction, while low expectations tend to decrease satisfaction (Bhattacherjee, 2001).

However, this relationship ignores the adjustment in expectations after the experience. If one examines the assimilation-contrast model, it states that expectations are adjusted to experience within a certain tolerance range; thus, low disconfirmation continues to lead to satisfaction (Brown et al., 2014). If one lies outside this tolerance range, expectations are no longer adjusted to experience and lead to negative or positive effects, depending on the disconfirmation direction.

According to Oliver (1977), overly high expectations lead to negative disconfirmation, but would exert a fundamentally positive affect on satisfaction, and vice versa, in the case of low expectations. With agreement or low disconfirmation, i.e., with (almost) correct expectations, these would be neither significantly negative nor significantly positive (Goode et al., 2017). Since in the case of a data breach recovery action, customers have a comparative value from previous incidents, they will have expectations regarding the company's response in any case. These expectations can be expected to be either equal to or higher than the comparison value.

Thus, based on the fundamental idea of expectation confirmation theory, we assume that this form of expectation exerts a positive effect on satisfaction with the recovery action, leading to the following hypothesis:

H3 Users' expectations of a data breach recovery action are associated positively with their satisfaction with the actual data breach recovery action.

Considering that we intended to demonstrate that a typical recovery action in healthcare always lies within the assimilation-contrast model's tolerance range, it can be assumed that experiences are close to expectations. Thus, outcome ratings always would be aligned with expectations, i.e., the customer always would be in a range in which the service received is deemed appropriate (Kettinger & Lee, 2005).

In the present study's context, this would imply that the level of compensation disappointment lies within the customer's tolerance range; thus, the response to the data breach is viewed as satisfactory. This means that even if the customer expected an apology/compensation, but did not receive one, the expectation of disappointment would be low enough that expectations would be adjusted according to the experience. Thus, in the studied scenario, the post hoc expectations always would be equal to the experience and positively affect the customer's satisfaction.

Therefore, we assume that this effect can be demonstrated not only in overall satisfaction, but also in satisfaction with the recovery action, consequently yielding the following hypothesis:

H4 Users' extent of confirmation is associated positively with their satisfaction with the actual data breach recovery action.

Satisfaction is viewed as the key to building and retaining a long-term customer base (Anderson & Sullivan, 1993; Anderson et al., 2011). The interest at this point is whether the satisfaction generated in the tolerance range also has a positive long-term effect on actual customer behavior and can thus avert the negative long-term consequences.

Therefore, we also examined components that exert a long-term impact on customer behavior and corporate reputation. For this purpose, we first identified trust as a principal measure of customers long-term behavior after the data breach recovery strategy. This is due to the fact that trust is seen, particularly in marketing literature, as an indicator that distinguishes long-lasting and profitable relationships with a company and could therefore indicate that customers will not leave the company after a data breach (Flavián et al., 2006).

Overall, trust is defined primarily by three components, honesty, benevolence, and the company's competence (Coulter & Coulter, 2002; Gundlach & Murphy, 1993; Larzelere & Huston, 1980). Experience allows the customer to create expectations about these three components and to create expectations about events that may occur in the future, and therefore to decide whether to continue the relationship. Consequently, trust is generated as a result of knowledge accumulation. Trust is often not set as a pure result of experiences and expectations, but much more related to satisfaction with the experiences. Thus, trust should be greater if the satisfaction that the company or product gives to the consumer is greater (Flavián et al., 2006). In this case, when a satisfaction with the recovery action occurs. Therefore, we hypothesize the following:

H5 Users' level of satisfaction with the data breach recovery action is associated positively with users' trust in the company.

Since in the case of data breaches, in addition to the lost trust, it is in particular the termination of customer loyalty that leads to high costs, we set loyalty as the second main measure of customers' long-term behavior after the data breach recovery strategy for this purpose.

Loyalty is defined as a deep-rooted commitment to buy a product again in the future or to prefer a company even though situational influences, in this case the data breach, might cause switching behavior. Loyal customers are thus willing to buy products again or remain loyal to companies even though there are competitive alternatives to switch to. A customer will be loyal if he believes that the company will fulfill the agreed conditions. At the same time, the alternatives in the market will be less attractive (Li & Green, 2011).

Since data breaches are a common phenomenon and are known to affect all companies, we postulate that the fulfillment of expectations in the response after a data breach and thus the satisfaction with the recovery action will lead to the customer's continued loyalty with the company. The significant positive relationship between customer satisfaction and customer loyalty has already been confirmed by several studies (e.g.Chang et al., 2009; Cronin et al., 2000; Oliver & Burke, 1999).

However, we hypothesize that not only customer satisfaction but also satisfaction with recovery action has a positive impact on customer loyalty:

H6 Users' level of satisfaction with the data breach recovery action is associated positively with users' loyalty.

An essential ingredient and outcome of successful long-term relationships has been identified as word of mouth. This involves existing customers spreading good word about the company and its products and services (Anderson, 1988; Richins, 1983).

Word of mouth is particularly important in the case of negative news, such as data breaches, as it can either join the negative news, fall silent, or in the best case, be positive about the situation. Anderson (1988) can identify that there is a clear relationship between word of mouth and customer satisfaction. He showed that more extreme levels of satisfaction (positive or negative) lead to more extreme word of mouth and yet was able to show that satisfaction leads to word of mouth.

Thus, it can be assumed that satisfaction with the recovery action leads to positive word of mouth:

H7 Users' level of satisfaction with the data breach recovery action is associated positively with users' word of mouth.

Based on the theoretical and practical derivations, we established a research model based on expectation confirmation theory, with the assumption that the confirmation follows the (modified) assimilation-contrast model.

Research design

Study's setting and data collection

For data collection, the live *Altstadtlauf Göttingen* sports event was chosen, as it would reach a large number of people using fitness trackers. The run attracts several thousand people annually. In 2019, 4000 people registered.

Runners and bystanders were considered as potential candidates for the survey. Care was taken to ensure that the participants used a fitness tracker to increase external validity and ensure that they could imagine the fictitious data breach situation. Participants were selected and sampled individually or in groups as follows Fig. 2.

The survey was conducted anonymously, thereby excluding the possibility of contacting the participants afterward. Subsequently, each participant received the same questionnaire with manipulation control. The participants needed about 10 min per person to complete the questionnaire.

Experimental design and sampling

To test our research model, a scenario experiment was implemented. A scenario including a fictitious data breach of a

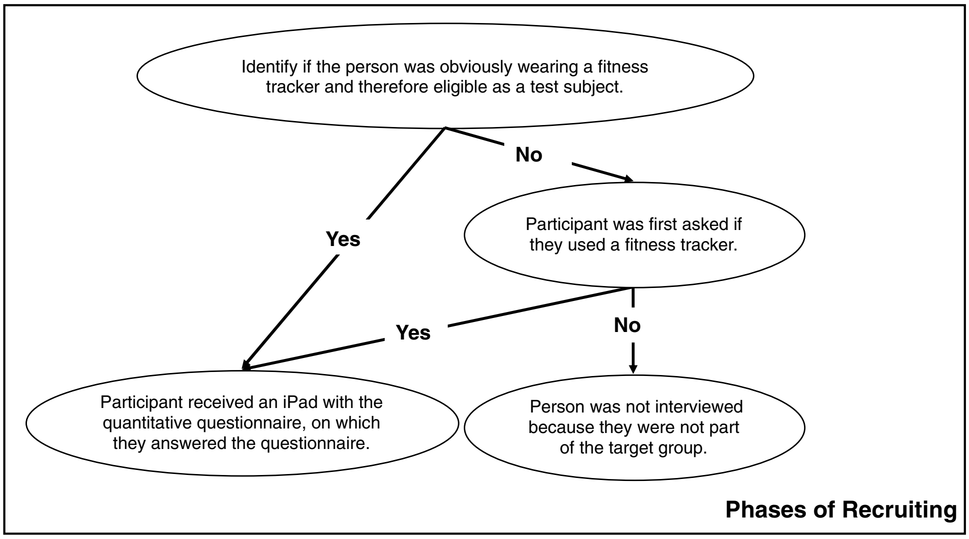
Identify if the person was obviously wearing a fitness tracker and therefore eligible as a test subject.
No
Yes
Participant was first asked if they used a fitness tracker.
Yes
No
Participant received an iPad with the quantitative questionnaire, on which they answered the questionnaire.
Person was not interviewed because they were not part of the target group.
Phases of Recruiting

Fig. 2 Recruiting phases

fitness tracker was developed. During the survey, participants needed to imagine that they had a fitness tracker they regularly used for running. It was explained that this could be an app on their mobile phone or a portable device, like a smartwatch.

In the first paragraph of the message, the data breach's severity was mentioned. For this purpose, it is explained that the user (participant) gave the fitness tracker personal information—such as email address, date of birth, height, weight, etc.—once, and the tracker collects live GPS data on each run to evaluate mileage. The participant was presented with the situation that he would like to start a new run, but that a message from the fitness tracker's provider appears shortly before the run begins, stating that an unauthorized third party violated some of his data. To ensure comparability, all participants received the same introductory information:

> Please imagine that you have a fitness tracker that you regularly use for jogging. This could be an activity tracker app (Runtastic, Nike Run Club, Strava, ...) or a fitness watch (Fitbit, Apple Watch, Samsung Galaxy Fit, ...). The fitness tracker needs personal data from you once, such as email address, date of birth, height, weight, running behavior, etc. Also, every time you use the fitness tracker for jogging, the running route is tracked using GPS data to receive an evaluation after the run. You now want to go running and receive the following message: "Dear user, we discovered a security incident in your fitness tracker account on June 25, 2019. Some of your personal data have been stolen by an unauthorized third party."

After this introduction, the participants received another message that contained the health care provider's response to the data breach by randomization, which was implemented using the Qualtrics questionnaire tool's functionality. Thus, it was possible to ensure that the randomization was distributed equally. In this step, a vignette design was chosen to query the independent variables (apology and compensation) through scenario-based experimental manipulation. Four scenarios (neutral × neutral, neutral × apology, neutral × compensation, and apology × compensation) were assigned randomly to the participants through an intermediate design (Atzmüller & Steiner, 2010) to test the two countermeasures' effectiveness.

First, the apology contains the values "no apology received" or "apology received," and the compensation is expressed as "no compensation received" or "compensation received".

If the customers received the apology as a supplier reaction, it was added to the second paragraph. Thus, they received a message that included an apology from the provider, in which the company expresses regret over the incident and promises to work on the problem to prevent it from recurring.

If the customer received a compensation offer, it was in the third paragraph of the message. The vendor offered the customer the opportunity to use the premium version free of charge for 3 months. (There were no further obligations, and the account automatically was reset to the standard version after 3 months). The concrete reactions used in the scenario are provided in Table 2 with their respective characteristics.

Across the different treatment groups, we collected 507 valid answers. Invalid responses were identified by uncompleted questionnaires, a manipulation check, and an attention check. The participants' average age was 28.52 years (SD = 9.14 years), and the sample comprised 54.83% men and 44.38% women. These respondents stated that they train or engage in other sports activities 3.15 times a week and run 1.47 times a week on average. In addition, 59.4% of respondents stated that they "occasionally" or "more frequently" (29.6% always) use a fitness tracker for sports. To validate random assignment, we checked the variation in control variables among the four treatments via variance analysis, which did not indicate any significant effects and, thus, did not indicate any sign of randomness validation. Please see the Appendix 2 for details.

Table 2 Scenarios

		Compensation	
		Neutral	*Compensation*
Apology	*Neutral*	“If you have any questions, please contact us.”	“As compensation, we offer you use of our premium version free of charge for three months. (There are no further obligations. Your account then automatically will be switched back to the standard version.) If you have any questions, please contact us."
	Apology	“We deeply regret the incident and are striving to address it to ensure that such an inconvenience does not recur. We apologize for the inconvenience. If you have any questions, please contact us."	“We deeply regret the incident and are striving to address it to ensure that such an inconvenience does not recur. We apologize for the inconvenience. As compensation, we offer you use of our premium version free of charge for three months. (There are no further obligations. Your account then automatically will be switched back to the standard version.) If you have any questions, please contact us."

Measurement of constructs

All research constructs were adapted from the literature. The items were selected for consistency with the construct definition in this research context and the measurement quality. All items were reworded carefully to fit the research context and measured using a seven-point Likert scale, ranging from 1 ("fully disagree") to 7 ("fully agree"). Other scales were used partly for the control variables, e.g., age was measured using a metric scale. The latent measurement scales—including construct names, elements, and related referents—are listed in Table 3.

A potential problem in this study is common method bias, so Harman's single-factor test was performed to test for a common factor (Podsakoff & Organ, 1986). All measurement items used in the investigation were subjected to exploratory factor analysis. In doing so, it can be stated that no method bias was found in the data, as the total variance extracted by one factor is 42%, which is less than the recommended threshold of 50%. Thus, as no single factor emerged from the analysis, it can be concluded that the study was free of common method bias.

Table 3 Operationalization of constructs

Constructs and items	Loadings
Expectation–compensation (Goode et al., 2017)	
I expect compensation (monetary or non-monetary) when personal data are stolen	.671
I assume that the provider provides me with, in the event of a data breach, free usable content	.805
I find that compensation, such as three months of free premium membership, represents reasonable compensation if a third party misuses my fitness tracker data	.681
Expectation–apology (Goode et al., 2017)	
I expect an apology from the provider when personal data are stolen	.810
I assume that the provider would show remorse to its customers after a data breach	.738
I find that an apology is a reasonable response from the provider if a third party misuses my fitness tracker data	.724
Confirmation (Bhattacherjee, 2001)	
My experience with the fitness tracker provider's recovery action after the data breach was better than expected	.902
The fitness tracker provider's recovery actions after the data breach were better than expected	.917
Overall, most of my expectations regarding the fitness tracker provider's recovery actions after the data breach were confirmed	.688
Satisfaction with recovery action (Kantsperger & Kunz, 2010)	
Overall, I am satisfied with the fitness tracker provider's response to the incident	.895
The fitness tracker provider's response fully meets my expectations	.893
Looking back, I perceive the fitness tracker provider's response as a good experience	.855
Looking back, the decision to use this fitness tracker was the right one	.725
The fitness tracker provider's response corresponds with my expectations	.871
Trust in fitness tracker (Choi & Ji, 2015)	
I think the fitness tracker is safe	.930
I find the fitness tracker trustworthy	.957
All in all, I trust the fitness tracker	.958
I find the fitness tracker reliable	.884
Word of mouth with fitness tracker (Kim & Son, 2009)	
I will tell others about the fitness tracker's positive aspects	.935
I will recommend the fitness tracker to anyone who seeks my advice	.958
I will advise my friends and acquaintances to use this fitness tracker	.962
Loyalty with fitness tracker (Kau & Loh, 2006)	
I will continue to use this fitness tracker	.885
I will not change my fitness tracker provider after the incident	.870
In the near future, I intend to consider the fitness tracker provider's new product offers	.840
I consider myself to be a loyal customer of this fitness tracker provider	.877

Data analysis and results

We tested our hypotheses using a partial least squares (PLS) structural equation modeling (SEM) approach, which is consistent with other experimental IS and management research studies (Fombelle et al., 2016; Trenz et al., 2020).

In experimental research designs with latent variables, SEM is preferable to other methods because it can account for measurement errors and theoretical constructs' multidimensional structures (Bagozzi & Yi, 1988). As the PLS estimator offers advantages in fewer restrictive assumptions, it finds broad application in experimental research designs (Fombelle et al., 2016; Trenz et al., 2020).

In addition, the PLS estimator fits our primary goal of predicting the effects from recovery strategies, rather than testing the theory. We dummy-coded the experimentally manipulated recovery strategies (apology and compensation) into two variables for the structural model setup. Furthermore, the higher-order constructs were modeled using the two-step approach (Hair et al., 2012). SmartPLS 3.0 software was used to perform the analysis, and R (Version 4.0.3) was used to perform other calculations.

Measurement validation

Our model included the three independent variables compensation, apology, and expectation. The expectation variable was formed with a higher-order construct of the factors expectation compensation (M = 4.70, SD = 2.00) and expectation apology (M = 5.87, SD = 1.70).

It was found that all reflection-modeled constructs' element loads and internal consistencies were above the 0.7 limit. The only exceptions were the first and third items of the expectation confirmation construct, but they were not removed, as they were very close to the 0.7 limit.

Table 4 provides composite reliability (CR) and average variance extracted (AVE) data used to assess the construct's reliability and validity. Both requirements were met when all constructs evaluated CR values higher than 0.7, with AVE and Cronbach's alpha values higher than 0.5 (Bagozzi & Yi, 1988). In our model, all CR values clearly were above the 0.7 limit. All AVE values also reached the limit. To assess discriminant validity, Fornell and Larcker offer an approach in which the square root of the AVE is compared with the correlations between the constructs. The comparison indicated that all constructs retained a higher value for the square root of the AVE (bold diagonal numbers) than for the correlation with other constructs (Fornell & Larcker, 1981). We concluded that our data indicate acceptable measurement properties for further analyses.

Hypotheses testing

We used the PLS method to estimate the theoretical structural model described above. The bootstrapping re-sampling method with 5000 samples was used to assess the paths' significance. The results from the calculations are provided in Fig. 3.

It can be stated that the results support our research model's structure. The R^2 of the dependent variable satisfaction was 52.1%, trust was 52.2%, variable loyalty was 63.8% and word of mouth was 67.8%.

It was found that expectation (.077; significant at .05) and confirmation (.688; significant at .01) exerted a significant positive effect on satisfaction. Compensation (.136; significant at .05) and apology (.168; significant at .01) exerted a significant positive effect on confirmation. Furthermore, a significant positive influence from satisfaction on trust (.522; significant for .01), loyalty (.638 significant for .01), and word of mouth (.678; significant for .01) could be observed.

Table 4 Construct validation

	Cronbach's alpha	AVE	CR	Exp Comp	Exp Apo1	Comp	Apo1	Conf	Satisf	Trust	Loy	WoM
ExpComp	.534	.764	.521	**.874**								
ExpApo1	.629	.802	.575	.282	**.896**							
Comp	n/a	n/a	n/a	.033	.020	**n/a**						
Apo1	n/a	n/a	n/a	.002	.003	.030	**n/a**					
Conf	.792	.878	.709	.055	− .073	.140	.172	**.937**				
Satisf	.902	.928	.723	.130	.002	.171	.168	.706	**.963**			
Trust	.950	.964	.870	.084	.003	.036	.045	.551	.522	**.982**		
Loy	.891	.924	.754	.091	.013	.011	.067	.586	.638	.711	**.961**	
WoM	.948	.967	.906	.142	− .027	.031	.054	.581	.678	.710	.753	**.983**

ExpComp expectation compensation, *ExpApol* ExpectationApology, *Comp* compensation, *Apol* apology, *Conf* confirmation, *Satisf* satisfaction, *Loy* loyalty, *WoM* word of mouth

Bold Diagonal Numbers = Square Root of AVE

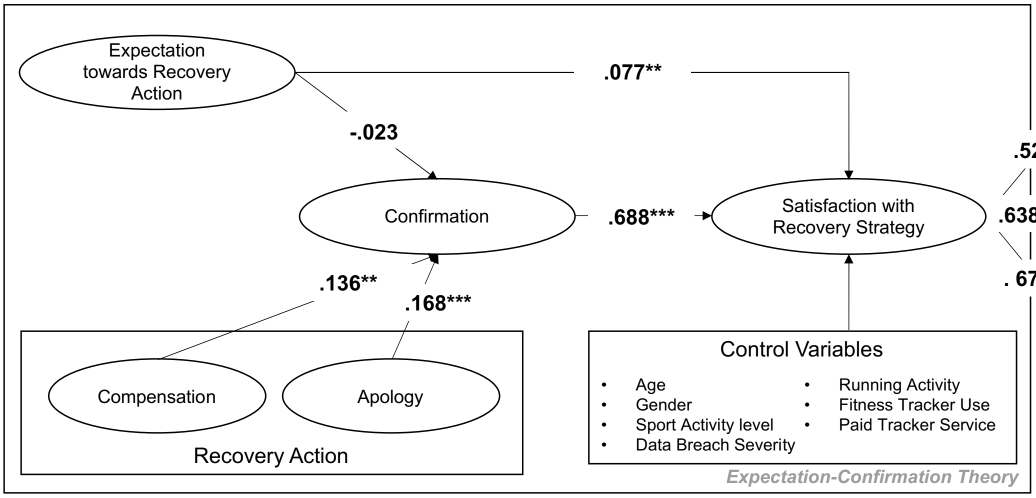

Fig. 3 Structural model with path coefficients (***significant at .01, **significant at .05)

The negative effect observed from expectations on confirmation was insignificant (−.023 not significant).

Furthermore, the following control variables were used: age; gender; sports activity level; data breach severity; running activity; use of a paid fitness tracker app; and use of the fitness tracker. Except for data breach severity (−.056 significant at .1), the control variables exerted no significant effect on satisfaction. Table 5 enables a further overview of all hypotheses and results.

As an additional post hoc analysis, we conducted a factorial variance analysis, with the research model's latent variables used as dependent variables. We found significant main effects from compensation [F(1,503) = 15.89, p < .001] and apology [F(1,503) = 14.288, p < .001], and a significant interaction effect between compensation and apology on satisfaction with recovery action. We also found significant main effects from compensation [F(1,503) = 8.552, p = .004] and apology [F(1,503) = 14.95, p < .001] on confirmation. The results with means are reported in the Appendix 2.

Discussion and implications

Summary of findings

This study examined satisfaction with recovery actions and how they affect customers' behaviors after a data breach using typical real-world compensation and apology

Table 5 Support for hypotheses; Note: (***significant at .01, **significant at .05)

Hypotheses	Support for hypothesis	
H1: Users' expectations of a data breach recovery action are associated negatively with confirmation	Not supported, with a negative influence on confirmation	−.023
H2a: After a data breach, a typical compensation is associated positively with confirmation	Supported with a positive influence on confirmation	.136**
H2b: After a data breach, a typical apology is associated positively with confirmation	Supported with a positive influence on confirmation	.168***
H3: Users' expectations of a data breach recovery action are associated positively with their satisfaction with the actual data breach recovery action	Supported with a positive influence on satisfaction	.077**
H4: Users' extent of confirmation is associated positively with their satisfaction with the actual data breach recovery action	Supported with a positive influence on satisfaction	.688***
H5: Users' level of satisfaction with the data breach recovery action is associated positively with users' trust in the company	Supported with a positive influence on trust	.522***
H6: Users' level of satisfaction with the data breach recovery action is associated positively with users' loyalty	Supported with a positive influence on loyalty	.638***
H7: Users' level of satisfaction with the data breach recovery action is associated positively with *users' word of mouth*	Supported with a positive influence on word of mouth	.678***

as healthcare providers' recovery actions. Specifically, healthcare data breaches provide an understanding of how strategic recovery actions can impact satisfaction levels with recovery actions positively and overcome damage to customer trust, while positively influencing behavior. To sum up, both compensation and apology used in practice exert a positive impact on confirmation.

In this context, it can be stated that customers expect both after a data breach, but particularly an apology. This expectation, which is formed before the actual recovery action occurs, negatively affects confirmation. However, this influence is insignificant, considering that disconfirmation between expectation and confirmation lies within the assimilation-contrast model's tolerance range due to the use of typical recovery actions. Therefore, as shown in Goode et al. (2017), expectations should be adjusted to reflect experience afterward.

Based on the post hoc variance analysis, it can be inferred that disconfirmation between expectations and experiences is highest when customers do not experience an apology or compensation. Considering that customers are more likely to expect an apology than compensation, the mean values indicate that disconfirmation between expected apology and not experienced is second-highest, followed by disconfirmation in the case of expected compensation not being received.

Also, positive disconfirmation can be observed, although this also lies within the tolerance range and, thus, does not exert a significantly positive effect if either an apology or compensation is expected, and the customer receives both.

Thus, confirmation's strongly significant influence on satisfaction with recovery action can be explained, ultimately impacting trust, word of mouth, and customer loyalty positively.

Although this is a ubiquitous and topical issue, the recovery actions used here are used almost routinely in practice and, thus, have strong practical relevance. Little research has been done on different data breach recovery actions' influence in practice, particularly in the healthcare sector. Therefore, this paper provides both theoretical and practical implications. Nonetheless, this work is not without limitations and provides opportunities for future research.

Theoretical implications

This research offers several theoretical contributions to the literature.

First, we built on assimilation-contrast model literature in the context of crises. It now is clear that in the case of crises that must be addressed publicly and occur regularly, by providing a comparative benchmark for companies' responses, it is possible to stick to past strategies because satisfaction with the response is elicited. This is because the response, if unsurprising, lies within the assimilation contrast model's tolerance range; thus, the expectation is adjusted to the experience.

Furthermore, research on the assimilation-contrast model can be extended to indicate that a response to a data breach in the tolerance range leads not only to satisfaction based on fulfilled expectations, but also positive long-term behavior among customers as far as trust, loyalty, and positive word of mouth. We also demonstrated that these variables, which already have been resolved in the underlying expectation confirmation theory for fulfilled expectations, also apply to the assimilation-contrast model's tolerance area. Thus, our research adds more dependent variables to the literature on the assimilation-contrast model domain.

Second, we helped ground the literature on data breach recovery actions used in practice. We complemented the literature by introducing another form of recovery action, the apology, by coding data breach response strategies, thereby complementing Goode et al.'s (2017) response strategy.

We expanded on Goode et al.'s (2017) research, demonstrating how recovery actions after a data breach that are applied in practice act in the theoretical framework of the (modified) assimilation-contrast model. Here, we demonstrated that these recovery actions build on Goode et al.'s (2017) explanation in the tolerance range and that both positive and negative disconfirmations exist, but are assimilated due to the tolerance range.

Third, we can build on existing literature on data breach recovery actions after healthcare breaches by investigating various data recovery actions after a data breach through experimental research, thereby complementing existing security literature.

This can illustrate how further research can explain customer responses to help health service providers determine recovery actions, such as compensation and apology, in response to a data breach. Although research to date has focused on how companies can prevent data breaches and how security policies are managed (Romanosky et al., 2014), researchers and companies, particularly health service providers, need to understand and apply recovery actions. It is also essential that research and practice address the problem, as data breaches are inevitable and unplanned. Both health service providers and customers also incur unplanned costs after data breaches (Gatzlaff & McCullough, 2010).

Fourth, we demonstrated that the service failure literature has applicability and, thus, transferability to health data breaches (Goode et al., 2017). Therefore, our paper also can contribute to service recovery literature by investigating recovery actions' impact on customer behavior after a health data breach and, conversely, by drawing new conclusions for service recovery literature.

Practical implications

In addition to theoretical contributions, our results can help health service providers optimize their strategies for their future company communications after a data breach and adapt them in such a way that the best possible results are achieved, even after a data breach.

Based on the identified results, health service providers can derive communication strategies in advance of a data breach to minimize the breach of trust and its consequences in case of a similar data breach, as well as restore customer satisfaction, loyalty, and trust in a best-case scenario.

It can be demonstrated that customer expectations strongly influence later consequences from a data breach. Therefore, it would be useful for health service providers to know their customers' expectations in the run-up to a data breach, or else find a way to determine them.

It could be demonstrated that these expectations can be derived from the company's previous recovery actions after earlier data breaches or otherwise be based on other companies' recovery actions in the industry. As previously mentioned, data breaches are inevitable, particularly in the specific case of fitness trackers, and should be prepared for as thoroughly as possible. In addition to expectations, recovery actions exert influence and can lead to more positive customer behavior. If no experiential data exist, it would be reasonable and positive for a healthcare provider, after a similar data breach, to offer both compensation and an apology, and to match, or slightly exceed, expectations, which are known in the best-case scenario. If the healthcare service provider chooses this route and offers its customers the recovery action that they expect, the company can compensate for the data breach's consequences cost-effectively.

Furthermore, the healthcare service provider can make a distinction between the two recovery actions. For example, our study's results suggest that an apology after an incident is the most cost-effective and recommended route, leading to satisfaction with the recovery action, and customers expect less compensation with an apology. However, it generally is the case that matching expectations with the actual recovery action received is most important for positive customer behavior and for bridging the breach of trust.

In addition, one important aspect, particularly for health service providers, was identified: the significant influence from the data breach's severity. For health service providers, this means that if only minor important data are stolen—which, for example, do not reveal the person's health status—then customer satisfaction, trust, and loyalty can be regained more easily, and word of mouth incurs less damage. Conversely, the theft of health-related data leads to higher expectations of recovery action from the health service provider, which should not go unfulfilled.

To sum up, health service providers would be well-advised to assume that they will be victims of a data breach at least once during their business years, so they should determine their customers' expectations to strike the right balance between apology and compensation and, thus, achieve the ultimate recovery effect.

Limitations and opportunities for future research

Our study has some limitations that need to be considered when interpreting the results and suggesting future research directions.

Primary, even if the experiment's participants owned fitness trackers, the experiment was based on a fictitious health data breach situation in which the participants had to empathize with the given situation. In the ideal case, future studies should provide a comprehensive validation of the measurements in which participants are affected by a data breach from a digital health app.

Furthermore, only two recovery actions were applied in the present work. Although two independent researchers conducted the development of the two categories for recovery strategies, it cannot be guaranteed that no other important aspects could belong to a different category and that all aspects were captured during the coding process. Future researchers can refine the coding of recovery actions and find other possible categorization levels.

As mentioned above, the injured parties in the study received either fixed compensation and/or a defined apology from the health service provider. It also should be noted that different formulations could have elicited different effects on satisfaction with recovery action, i.e., different formulations of apologies and compensation forms and levels should be tested to determine future satisfaction levels.

Furthermore, the control variable severity exerted significant influence on satisfaction with recovery action. This suggests that when severe data breaches cause low satisfaction levels, recovery actions are crucial.

It also should be considered whether it makes a difference when a recovery action is executed in terms of how long after the breach.

In addition, future studies could use other variables to measure satisfaction with recovery actions, such as whether class action lawsuits are pursued against providers.

Finally, it should be noted that future studies with real health data breach scenarios should consider that expectations change over time (Bhattacherjee & Premkumar, 2004). Thus, expectations before consumption might deviate from expectations "during" and "after" consumption (Oliver & Burke, 1999), considering that firsthand experiences often "color" consumer expectations. Therefore, scientists have argued that expectations after consumption (perceived utility) are more realistic and should be considered (Bhattacherjee, 2001).

Conclusion

Given that fitness trackers belong to the category of health applications subject to a low level of security, this study examined typical recovery actions' impact on bridging the loss of customer trust caused by a data breach. We theorized and investigated how two widely used recovery actions affect customer reactions after a data breach in the specific context of fitness trackers.

Based on expectation confirmation theory, through the assimilation-contrast model, we argued that a combination of response strategy characteristics and individual customer expectations influences satisfaction with recovery actions and, thus, customer behavior. In particular, we investigated the effects from compensation and apology on customers' satisfaction with the received recovery action. How these recovery actions affect customers' attitudes toward the health service provider also was investigated, measured through trust, loyalty, and word of mouth.

A scenario-based experiment with two independent variables was conducted with 507 participants at a community running event. Our study's results provide valuable insights into how recovery actions used by healthcare providers following a data breach in practice affect customer satisfaction with recovery actions and the resulting impact on customer trust, loyalty, and word of mouth. It was demonstrated that different practiced recovery actions positively impact customer satisfaction and behavior, and are within the assimilation-contrast model's tolerance range; therefore, any disconfirmation between expectations and experiences is assimilated.

This can complement the growing knowledge base on how to recover after a health data breach based on the health service provider's strategic management. It also will allow healthcare providers to understand how to derive their customers' expectations for recovery action if they already have experience with data breach recovery strategies. Otherwise, it allows them to identify and derive initial strategies to mitigate a data breach's consequences. Therefore, this study's results provide practical applications for health service providers, and the research can be expanded further through future studies on health data breach recovery actions.

Appendix 1

Data collection procedure and sample selection for a practical review of data breach recovery actions in healthcare

The data collected are secondary data related to 72 announcements of data breaches by public U.S. companies. In addition, the sample referred only to companies listed on public stock exchanges (i.e., NYSE, AMEX, or NASDAQ).

To identify company-specific data breach announcements with defined characteristics, we used the nonprofit online Privacy Rights Clearinghouse database (Gatzlaff & McCullough, 2010; Rosati et al., 2017, 2019), which has been collecting all notifications of privacy breaches since 2005.

This analysis only uses data breaches since 2007. This topic was chosen because the costs of security breaches doubled from 2006 to 2007, i.e., higher relevance can be determined from 2007 onward (Richardson, 2008). Altogether, 8376 reported data breaches were found in the database between January 2007 and October 2019 (Privacy Rights Clearinghouse, 2019).

Of these reported incidents, 348 data breaches occurred at publicly traded companies, i.e., listed on stock exchanges, at the time of the incidents. Each company also had to be listed during the estimated period, usually in the range of [130, 1] from the date of the event. Also, each security breach was investigated to determine whether it violated data confidentiality to consider only breaches that comprised an actual data breach (Campbell et al., 2003; Ko et al., 2009).

Altogether, 321 data sets from the 348 breaches were revealed. Of these data breaches, each company's responses on the day of disclosure were researched. For 18 companies, no further information on the announcements of data breaches could be found (see Fig. 4).

The additional information on the data breach events that needed to be collected included the company's official announcement or, if not available, news reports on the event that cited the official response and additional information on the breach's severity.

The company's announcements can be found by searching each company's official website for press releases or through U.S.-American public prosecutor offices' databases. In several states, such as New Hampshire and New Jersey, laws (Digital Guardian, 2018) require public companies to disclose any data breach that entails customer and/or employee information. These announcements, as well as the information made available to those concerned, are publicly available in relevant offices' databases.

If the announcement was not found on the company's website or in the public prosecutor's office database, news reports were used to find the necessary information. These news reports cited official announcements and were found using the Lexis-Nexis database and information from the Privacy Rights Clearinghouse database.

Whenever the incident report was no longer publicly available online, the Wayback Machine web archive was used. This archive contains a collection of all websites that have ever been available publicly online. If not all required information was included in the announcement, additional news reports were collected (data collection period: 11-01-2019 to 11-25-2019).

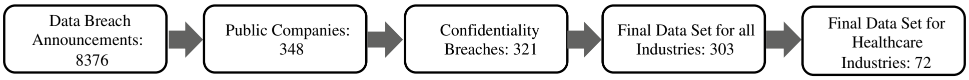
Data Breach Announcements: 8376
Public Companies: 348
Confidentiality Breaches: 321
Final Data Set for all Industries: 303
Final Data Set for Healthcare Industries: 72

Fig. 4 Data collection process

After the announcements of the data breaches for each incident were collected, two independent researchers coded them. The inter-rater reliability in the coding of the categories for the whitewash and apology, calculated using Cohen's Kappa, had an agreement of 0.6. To make the data set usable for this paper, the companies in the sample all are within the healthcare industry. In the end, 72 data breaches remained, which were considered for the chapter "Practical Review of Data Breach Recovery Actions in Healthcare."

Appendix 2

Variance analysis

We conducted a two-way ANOVA for further analysis. The binary variable compensation (Comp) and apology (Apol) are the independent variables. For all latent variables, we calculated the average item measures and used them, as well as the control variables, as dependent measures. See Table 6.

Table 6 Two-way variance analysis and descriptive statistics on dependent variables

Dependent variable	All		Treatment				ANOVA
	N = 507		Control N = 133	Comp N = 126	Apol N = 120	Comp + Apol N = 128	
Expectation compensation	Mean	4.70	4.63	4.77	4.69	4.72	Comp: F(1,503) = 0.443, n.s Apol: F(1,503) = 0.004, n.s Comp*Apol: F(1,503) = 0.164,n.s
	SD	1.44	1.58	1.48	1,49	1.21	
Expectation apology	Mean	5.87	5.78	5.96	5.92	5.83	Comp: F(1,503) = 0.139, n.s Apol: F(1,503) = 0.001, n.s Comp*Apol: F(1,503) = 1,391,n.s
	SD	1.26	1.29	1.19	1.22	1.32	
Confirmation	Mean	3.26	2.93	3.10	3.24	3.78	Comp: F(1,503) = 8.552, p = .004** Apol: F(1,503) = 14.95, p < .001*** Comp*Apol: F(1,503) = 2.184, n.s
	SD	1.45	1.36	1.52	1.42	1.39	
Satisfaction	Mean	3.51	2.98	3.57	3.55	3.99	Comp: F(1,503) = 15.89, p < .001*** Apol: F(1,503) = 14.288, p < .001*** Comp*Apol: F(1,503) = 0.354,n.s
	SD	1.53	1.39	1.63	1.43	1.51	
Word of Mouth	Mean	3.01	2.78	3.08	3.15	3.06	Comp: F(1,503) = 0.480, n.s Apol: F(1,503) = 1,418, n.s Comp*Apol: F(1,503) = 1.685,n.s
	SD	1.70	1.54	1.69	1.74	1.82	
Loyalty	Mean	3.38	3.13	3.42	3.61	3.37	Comp: F(1,503) = 0.102, n.s Apol: F(1,503) = 2.338, n.s Comp*Apol: F(1,503) = 3.420,n.s
	SD	1.61	1.51	1.72	1.60	1.61	
Trust	Mean	2.93	2.72	3.01	3.04	2.97	Comp: F(1,503) = 0.630, n.s Apol: F(1,503) = 1.034, n.s Comp*Apol: F(1,503) = 1.644,n.s
	SD	1.60	1.56	1.64	1.57	1.62	
Age	Mean	30.5	31.1	29.4	31.1	30.6	Comp: F(1,503) = 0.525, n.s Apol: F(1,503) = 1.928, n.s Comp*Apol: F(1,503) = 0.534,n.s
	SD	9.14	9.22	7.63	9.93	9.63	
Sport activity	Mean	3.15	2.85	3.25	3.33	3.18	Comp: F(1,503) = 0.803, n.s Apol: F(1,503) = 2.190, n.s Comp*Apol: F(1,503) = 3.711,n.s
	SD	1.62	1.64	1.47	1.76	1.59	
Running activity	Mean	1.43	1.26	1.49	1.52	1.46	Comp: F(1,503) = 0.559, n.s Apol: F(1,503) = 0.889, n.s Comp*Apol: F(1,503) = 1.349,n.s
	SD	1.40	1.14	1.29	1.31	1.42	
Tracker use	Mean	2.90	3.22	2.82	2.82	2.73	Comp: F(1,503) = 1.276, n.s Apol: F(1,503) = 1.315, n.s Comp*Apol: F(1,503) = 0.469,n.s
	SD	2.48	2.54	2.48	2.45	2.45	

SD standard deviation, *p* p-value; significance level: *0.05; **0.01; ***0.001; *n.s.* not significant

Funding Open Access funding enabled and organized by Projekt DEAL.

References

Anderson, C. L., Agarwal, R., & Anderson, C. L. (2011). The digitization of healthcare: Boundary risks, emotion, information. *Information Systems Research, 22*(3), 469–490.

Anderson, E. W. (1988). Customer satisfaction and word of mouth. *Journal of Service Research, 1*(1), 5–17.

Anderson, E. W., & Sullivan, M. W. (1993). The antecedents and consequences of customer satisfaction for firms. *Marketing Science, 12*(2), 125–143. https://doi.org/10.1287/mksc.12.2.125

Angst, C. M., Block, E. S., Arcy, J. D., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*(3), 893–916. https://doi.org/10.25300/MISQ/2017/41.3.10

Atzmüller, C., & Steiner, P. M. (2010). Experimental vignette studies in survey research. *Methodology, 6*(3), 128–138. https://doi.org/10.1027/1614-2241/a000014

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74–94. https://doi.org/10.1007/BF02723327

Becker, B. W., Berry, L. L., & Parasuraman, A. (1992). Marketing services: Competing through quality. *Journal of Marketing, 56*(2), 132. https://doi.org/10.2307/1252050

Behne, A., & Teuteberg, F. (2020). A healthy lifestyle and the adverse impact of its digitalization: The dark side of using eHealth technologies. *Proceedings of the Internationale Tagung Wirtschaftsinformatik, Potsdam.*

Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions, and word of mouth. *International Journal of Contemporary Hospitality Management, 24*(7), 991–1010. https://doi.org/10.1108/09596111211258883

Bhattacherjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly, 25*(3), 351–370.

Bhattacherjee, A., & Premkumar, G. (2004). Understanding changes in belief and attitude toward information technology usage. *MIS Quarterly, 28*(2), 229–254. https://doi.org/10.2307/25148634

Brown, S. A., Venkatesh, V., & Goyal, S. (2012). Expectation confirmation in technology use. *Information Systems Research, 23*(2), 287–598. https://doi.org/10.1287/isre.1110.0357

Brown, S. A., Venkatesh, V., & Goyal, S. (2014). Expectation confirmation in information systems research: A test of six competing models. *MIS Quarterly, 38*(3), 729–756.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448. https://doi.org/10.3233/JCS-2003-11308

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Chang, H. H., Wang, Y.-H., & Yang, W.-Y. (2009). The impact of e-service quality, customer satisfaction and loyalty on e-marketing: Moderating effect of perceived value. *Total Quality Management & Business Excellence, 20*(4), 423–443. https://doi.org/10.1080/14783360902781923

Choi, J. K., & Ji, Y. G. (2015). Investigating the importance of trust on adopting an autonomous vehicle. *International Journal of Human-Computer Interaction, 31*(10), 692–702. https://doi.org/10.1080/10447318.2015.1070549

Chuah, S. H. W., Rauschnabel, P. A., Krey, N., Nguyen, B., Ramayah, T., & Lade, S. (2016). Wearable technologies: The role of usefulness and visibility in smartwatch adoption. *Computers in Human Behavior, 65*, 276–284. https://doi.org/10.1016/j.chb.2016.07.047

Churchill, G. A., & Surprenant, C. (1982). An investigation into the determinants of customer satisfaction. *Journal of Marketing Research, 19*(4), 491–504. https://doi.org/10.1177/002224378201900410

Coulter, K. S., & Coulter, R. A. (2002). Determinants of trust in a service provider: The moderating role of length of relationship. *Journal of Services Marketing, 16*(1), 35–50. https://doi.org/10.1108/08876040210419406

Cronin, J. J., Brady, M. K., & Hult, G. T. M. (2000). Assessing the effects of quality, value, and customer satisfaction on consumer behavioral intentions in service environments. *Journal of Retailing, 76*(2), 193–218. https://doi.org/10.1016/S0022-4359(00)00028-2

Dai H., Salam A.F., & King R. (2008). Service convenience and relational exchange in electronic mediated environment: An empirical investigation. *Proceedings of the International Conference on Information Systems (ICIS), Paris*

DaVita Inc. (2013). *DaVita—Recommended steps to help protect your identity*. Retrieved October 25, 2020, from https://oag.ca.gov/system/files/Samples Notices_0.pdf

DaVita Inc. (2020). *Kidney disease and dialysis information—DaVita*. Retrieved October 25, 2020, from https://www.davita.com/

Digital Guardian. (2018). *The definitive guide to U.S. state data breach laws.* Retrieved October 25, 2020, from https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf

Flavián, C., Guinalíu, M., & Gurrea, R. (2006). The role played by perceived usability, satisfaction, and consumer trust on website loyalty. *Information and Management, 43*(1), 1–14. https://doi.org/10.1016/j.im.2005.01.002

Fombelle, P. W., Bone, S. A., & Lemon, K. N. (2016). Responding to the 98%: Face-enhancing strategies for dealing with rejected customer ideas. *Journal of the Academy of Marketing Science, 44*(6), 685–706. https://doi.org/10.1007/s11747-015-0469-y

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error: A comment. *Journal of Marketing Research, 18*(1), 39–50.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and*

Insurance Review, 13(1), 61–83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404–410. https://doi.org/10.1016/j.im.2009.06.005

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

Greve, M., Lembcke, T.-B., Diederich, S., Brendel, A. B., & Kolbe, L. M. (2020). Healthy by app—Toward a taxonomy of mobile health applications. In *Proceedings of the Pacific Asia conference on information systems (PACIS), Dubai, UAE.*

Grönroos, C. (1988). New competition in the service economy: The five rules of service. *International Journal of Operations & Production Management, 8*(3), 9–19. https://doi.org/10.1108/eb054821

Gundlach, G. T., & Murphy, P. E. (1993). Ethical and legal foundations of relational marketing exchanges. *Journal of Marketing, 57*(4), 35. https://doi.org/10.2307/1252217

Gwebu, K. L., Wang, J., & Wang, L. (2018). the role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems, 35*(2), 683–714. https://doi.org/10.1080/07421222.2018.1451962

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science, 40*(3), 414–433. https://doi.org/10.1007/s11747-011-0261-6

Irving, P. G., & Meyer, J. P. (1994). Reexamination of the met-expectations hypothesis: A longitudinal analysis. *Journal of Applied Psychology, 79*(6), 937–949. https://doi.org/10.1037/0021-9010.79.6.937

Islam, A. K. M. N., Mäntymäki, M., & Bhattacherjee, A. (2017). Towards a decomposed expectation-confirmation model of IT continuance: The role of usability. *Communications of the Association for Information Systems, 40*(1), 502–523. https://doi.org/10.17705/1CAIS.04023

Johnston, R. (1995). The zone of tolerance: Exploring the relationship between service transactions and satisfaction with the overall service. *International Journal of Service Industry Management., 6*(2), 46–61. https://doi.org/10.1108/09564239510084941

Kantsperger, R., & Kunz, W. H. (2010). Consumer trust in service companies: A multiple mediating analysis. *Managing Service Quality: An International Journal, 20*(1), 4–25. https://doi.org/10.1108/09604521011011603

Kau, A. K., & Loh, E. W. Y. (2006). The effects of service recovery on consumer satisfaction: A comparison between complainants and non-complainants. *Journal of Services Marketing, 20*(2), 101–111. https://doi.org/10.1108/08876040610657039

Kettinger, W. J., & Lee, C. C. (2005). Zones of tolerance: Alternative scales for measuring information systems service quality. *MIS Quarterly: Management Information Systems, 29*(4), 607–623. https://doi.org/10.2307/25148702

Kim, S. H., & Kwon, J. (2019). How do EHRs and a meaningful use initiative affect breaches of patient information? *Information Systems Research, 30*(4), 1184. https://doi.org/10.1287/isre.2019.0858

Kim, S. S., & Son, J.-Y. (2009). Out of dedication or constraint? A dual model of post-adoption phenomena and its empirical test in the context of online services. *MIS Quarterly, 33*(1), 49–70.

Klein, J. G. (1999). Developing negatives: Expectancy assimilation and contrast in product judgments. *Advances in Consumer Research, 26*, 463.

Ko, M., Osei-Bryson, K. M., & Dorantes, C. (2009). Investigating the impact of publicly announced information security breaches on three performance indicators of the breached firms. *Information Resources Management Journal, 22*(2), 1–21. https://doi.org/10.4018/irmj.2009040101

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25*(1), 1–10. https://doi.org/10.3233/THC-161263

Kude, T., Hoehle, H., & 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 and Production Management, 37*(1), 56–74. https://doi.org/10.1108/IJOPM-03-2015-0156

Kwon, J., & Johnson, M. E. (2015). Protecting patient data—The economic perspective of healthcare security. *IEEE Security and Privacy, 13*(5), 90–95. https://doi.org/10.1109/MSP.2015.113

Larzelere, R. E., & Huston, T. L. (1980). The dyadic trust scale: Toward understanding interpersonal trust in close relationships. *Journal of Marriage and the Family, 42*(3), 595. https://doi.org/10.2307/351903

Li, M., & Green, R. D. (2011). A mediating influence on customer loyalty: The role of perceived value. *Journal of Management and Marketing Research*, 1–12. http://www.aabri.com/manuscripts/10627.pdf. Last access on August 10 2020

Liu, J., & Sun, W. (2016). Smart attacks against intelligent wearables in people-centric internet of things. *IEEE Communications Magazine, 54*(12), 44–49.

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

Masuch, K., Greve, M., & Trang, S. (2020). Please be silent? Examining the impact of data breach response strategies on the stock value. *Proceedings of the International Conference on Information Systems (ICIS), Hyderabad, India* (pp. 1–16)

Masuch, K., Greve, M., & Trang, S. (2021). Apologize or Justify? *Examining the Impact of Data Breach Response Actions on Stock Value of Affected Companies, Computers & Security, 112*(2022), 102502. https://doi.org/10.1016/j.cose.2021.102502

Mattila, A. S., & Cranage, D. (2005). The impact of choice on fairness in the context of service recovery. *Journal of Services Marketing, 19*(5), 271–279. https://doi.org/10.1108/08876040510609899

McColl-Kennedy, J. R., & Sparks, B. A. (2003). Application of fairness theory to service failures and service recovery. *Journal of Service Research, 5*(3), 251–266. https://doi.org/10.1177/1094670502238918

McLeod, A., & Dolezel, D. (2018). Understanding healthcare data breaches: Crafting security profiles. *24th Americas Conference on Information Systems (AMCIS), New Orleans*

Medtronic. (2018). Security Breach Notification. https://www.doj.nh.gov/consumer/security-breaches/documents/medtronic-minimed-20181126.pdf. Last access on August 10, 2020

Morse, E. A., Raval, V., & Wingender, J. R. (2011). Market price effects of data security breaches. *Information Security Journal, 20*(6), 263–273. https://doi.org/10.1080/19393555.2011.611860

Mousavizadeh, M., Kim, D. J., & Chen, R. (2016). Effects of assurance mechanisms and consumer concerns on online purchase decisions: An empirical study. *Decision Support Systems, 92*, 79–90. https://doi.org/10.1016/j.dss.2016.09.011

Oliver, R. L. (1977). Effect of expectation and disconfirmation on postexposure product evaluations: An alternative interpretation. *Journal of Applied Psychology, 62*(4), 480–486.

Oliver, R. L. (1980). A cognitive model of the antecedents and consequences of satisfaction decisions. *Journal of Marketing Research, 17*(4), 460–469.

Oliver, R. L., & Burke, R. R. (1999). Expectation processes in satisfaction formation. *Journal of Service Research, 1*(3), 196–214.

Patterson, P. G., Cowley, E., & Prasongsukarn, K. (2006). Service failure recovery: The moderating impact of individual-level cultural value orientation on perceptions of justice. *International Journal of Research in Marketing, 23*(3), 263–277. https://doi.org/10.1016/j.ijresmar.2006.02.004

Patterson, P. G., Johnson, L. W., & Spreng, R. A. (1996). Modeling the determinants of customer satisfaction for business-to-business professional services. *Journal of the Academy of Marketing Science, 25*(1), 4–17. https://doi.org/10.1177/0092070397251002

Piccoli, G., Rodriguez, J., Palese, B., & Bartosiak, M. (2018). The dark side of digital transformation: The case of information systems education. *Proceedings of the International Conference on Information Systems (ICIS), Louisiana*

Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The rise of consumer health wearables: Promises and barriers. *PLoS Medicine, 13*(2), e1001953.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management, 12*(4), 531. https://doi.org/10.1177/014920638601200408

Ponemon Institute LLC. (2013). *2013 cost of data breach study: Global analysis.* Retrieved November 30, 2020, from https://www.ponemon.org/local/upload/file/2013ReportGLOBALCODBFINAL5-2.pdf

Ponemon Institute LLC. (2018). *2018 cost of data breach study: Impact of business continuity management.* Retrieved November 30, 2020, from https://www.ibm.com/downloads/cas/AEJYBPWA

Privacy Rights Clearinghouse. (2019). *Privacy rights clearinghouse*. Retrieved September 30, 2020, from https://privacyrights.org/data-breaches

Quest Diagnostics. (2015). *Security breach information*. Retrieved November 30, 2020, from https://oag.ca.gov/system/files/Quest attachment to CA online submission_0.pdf?

Richardson, R. (2008). *CSI computer crime and security survey*. Computer security institute. Retrieved October 25, 2020, from http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall10/CSIsurvey2008.pdf

Richins, M. L. (1983). Negative word-consumers: Pilot study. *Journal of Consumer Research, 47*(1), 68–78.

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies, 11*(1), 74–104. https://doi.org/10.1111/jels.12035

Rosati, P., Cummins, M., Deeney, P., Gogolin, F., van der Werff, L., & Lynn, T. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis, 49*, 146–154. https://doi.org/10.1016/j.irfa.2017.01.001

Rosati, P., Deeney, P., Cummins, M., van der Werff, L., & Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from U.S. listed companies. *Research in International Business and Finance, 47*, 458–469. https://doi.org/10.1016/j.ribaf.2018.09.007

Sherif, M., & Sherif, C. (1965). Attitudes as the individual's own categories: The social-judgment approach to attitude and attitude change. In C. Sherif & M. Sherif (Eds.), *Attitude, ego-involvement, and change* (pp. 105–139). Wiley Publishing

Sherr, I., & Wingfield, N. (2011). *Play by play: Sony's struggles on breach*. Wall Street Journal. https://www.wsj.com/articles/SB10001424052748704810504576307322759299038. Last access on August 10, 2020

Staples, D. S., Wong, I., & Seddon, P. B. (2002). Having expectations of information systems benefits that match received benefits: Does it really matter? *Information and Management*. https://doi.org/10.1016/S0378-7206(01)00138-0

Szajna, B., & Scamell, R. W. (1993). The effects of information system user expectations on their performance and perceptions. *MIS Quarterly: Management Information Systems, 17*(4), 493–516. https://doi.org/10.2307/249589

Trenz, M., Veit, D. J., & Tan, C.-W. (2020). Disentangling the impact of omnichannel integration services on consumer behavior in integrated sales channels. *MIS Quarterly*. https://doi.org/10.25300/MISQ/2020/14121

UnitedHealthcare. (2007). *Security breach information*. Retrieved November 30, 2020, from https://www.doj.nh.gov/consumer/security-breaches/documents/united-healthcare-20070625.pdf

Valvi, A. C., & West, D. C. (2013). E-loyalty is not all about trust, price also matters: Extending expectation-confirmation theory in bookselling websites. *Journal of Electronic Commerce Research, 14*(1), 99–123.

Venkatesh, V., & Goyal, S. (2010). Expectation disconfirmation and technology adoption: Polynomial modeling and response surface analysis. *MIS Quarterly, 34*(2), 281–303.

Wanous, J. P., Poland, T. D., Premack, S. L., & Davis, K. S. (1992). The effects of met expectations on newcomer attitudes and behaviors: A review and meta-analysis. *Journal of Applied Psychology, 77*(3), 288–297. https://doi.org/10.1037/0021-9010.77.3.288