

A User-centric View on Data Breach Response Expectations

Felix Hillmann¹, Tim Klauenberg², Lennart Schroeder² and Till Ole Diesterhöft³

¹ University of Paderborn, Warburger Str. 100, Paderborn, 33098, Germany

² University of Göttingen, Platz der Göttinger Sieben 5, Göttingen, 37073, Germany

³ University of Göttingen, Humboldtallee 3, Göttingen, 37073, Germany

Abstract

Due to the growing prevalence of data breaches and the associated negative outcomes, data breaches pose a serious problem for companies. Since universal response strategies may not fully address diverse customer expectations, their effectiveness could be limited. As a result, understanding customer expectations serves as the cornerstone of a successful response strategy. By integrating prior data breach research with expectation confirmation theory, we examine individual customer expectations across a wide range of situations and business environments. Therefore, we conducted twelve qualitative interviews. Our findings enrich the body of research on data breaches by highlighting the individualized nature of customer expectations regarding data breach responses, which are shaped by numerous factors. We also discuss our contributions to the literature and the implications for managing data breach responses more effectively.

Keywords

Data breach response, customer expectations, expectation confirmation theory

1. Introduction

According to the Ponemon Institute [21] for 83% of the companies it is not a question of if, but when a data breach will happen. Companies that store large amounts of personal data face a high risk of data breaches [10, 14], which can have various negative effects. Companies affected by breaches must inform affected customers and regulatory authorities [23]. Therefore, the importance of a cost-effective communication and response strategy that meets customer expectations is increasing [16]. Such a strategy aims to minimize damage to the company [36] and mitigate the negative impact caused by disgruntled customers [18, 27]. Various response strategies have been analyzed in the literature as recovery actions. Compensation and apology have been identified as common practices in addressing data breaches [16, 18]. Although Goode et al. [16] and Hoehle et al. [18] have shown that the success of the company's response strategy strongly depends on customer expectations. Consequently, companies need to ascertain customer expectations and incorporate them into their respective response strategy to minimize the negative impacts of a data breach [16, 36]. However, current literature has yet to explore the diversity of customer expectations in a proactive and qualitative approach. The Expectation Confirmation Theory (ECT), proposed by Oliver [38], supports an understanding of the importance of aligning the response strategy with individual customer expectations, impacting overall satisfaction and trust in the company. Given this background, our study aims to answer the following research question (RQ):


RQ: What are customers' expectations of a company's response to a data breach?

CIISR 2023: 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research, co-located with the 18th International Conference on Wirtschaftsinformatik (WI 2023), September 18, 2023, Paderborn, Germany

✉ felixhi@campus.uni-paderborn.de (F. Hillmann); tim.klauenberg@stud.uni-goettingen.de (T. Klauenberg); lennart.schroeder02@stud.uni-goettingen.de (L. Schroeder); tillole.diesterhoeft@uni-goettingen.de (T. O. Diesterhöft)

ORCID: 0009-0006-0129-2000 (F. Hillmann); 0009-0007-0376-5374 (T. Klauenberg); 0009-0003-2315-2525 (L. Schroeder); 0000-0002-4141-3261 (T. O. Diesterhöft)

© 2023 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

Drawing on previous research in data breach response expectations and ECT, we examine the alignment between companies' response strategies and individual customer expectations [16, 18, 36].

To answer the RQ, we conducted twelve qualitative interviews with affected or potentially impacted customers. These interviews explored various customer expectations that have not been previously studied. The identified expectations can be further examined for their effectiveness in response to data breaches. Additionally, these findings have practical implications as companies can optimize their data breach response strategy based on individual customer expectations. Thus, this study specifically targets company security management.

2. Research Background

2.1. Data Breaches

A data breach refers to the unauthorized use, storage, processing, or disclosure of personal data in violation of data protection laws, which can cause harm to individuals, companies, or governments [37, 39]. Breaches can occur through various means, such as data loss or theft, hacking, unauthorized access, accidental disclosure, lack of security measures, or abuse of personal data [4, 24, 32, 52].

Data breaches have become a common and serious threat due to increased reliance on digital technology and the internet [35, 40]. Despite increased cybersecurity awareness and investment, companies continue to struggle with securing their networks and data, resulting in rising costs of data breaches [22]. No company is immune to attacks or breaches, whether intentional or due to human error [16, 49].

Data breaches pose significant threats to privacy and security, particularly when sensitive personal information is involved [31]. Laws and regulations have been enacted in many countries to protect personal data and hold companies accountable for breaches [23]. The impact of data breaches on affected customers can include identity theft and financial losses [43]. Customers may lose trust in the company that experienced the breach, leading to a decline in customer loyalty and a loss of business for the company [5, 34, 36]. Companies may face financial losses, legal penalties, reputation damage, and decline in sales [25, 47]. Recovering from a breach requires significant investments in IT infrastructure, employee training, and preventive measures [7, 13, 22]. Overall, the consequences of a data breach can be far-reaching and affect not only the company but also its customers.

2.2. Review of Data Breach Response Strategies Research

To prevent data subjects from being harmed due to improper data disclosure [31], laws are being enacted that require companies to notify affected customers in the event of a data breach [23]. In this context, it has been shown that the challenge is to adapt the company's response strategy to the affected customer expectations [16]. The majority of companies strategically employ apologies and compensation, which previous research on data breach response has found to have a positive impact on perceived service quality, customer loyalty, and repurchase intent, thus minimizing the damage done [16, 18]. Regardless, companies often experience a significant rate of customer attrition due to the discrepancy between their response strategy and customers' expectations [16, 18]. Additionally, many companies opt to initiate external disclosure of a data breach only after they have gained a sufficient understanding of the breach and conducted a thorough investigation [28]. Regrettably, delays caused by a lack of response plans can result in ineffective and prolonged communication with customers, leading to decreased customer satisfaction [48]. Although companies may provide financial compensation, such as free products or services, discounts, or credit monitoring, to customers affected by a data breach, as well as communicate with them about the incident, offer an apology, and provide details on the breach and how to protect oneself [17], there is uncertainty about how to properly align compensation

levels with customer expectations [15]. Determining the appropriate level of compensation is a challenging and costly process [18]. Any deviation from customer expectations, whether exceeding or falling short, may result in reduced satisfaction and repurchase intentions [16]. Moreover, the severity of a data breach can vary [35, 42], affecting customer reactions and expectations differently, which necessitates a careful balance between compensation and severity to meet customer expectations without overcompensating. In conclusion, managers must strive to match compensation with customer expectations to ensure future customer retention in the event of a data breach [16, 36]. Consequently, there is a growing need to expand research aimed at meeting customer expectations. Focusing on these issues can help companies mitigate the negative impact of data breaches and strengthen their relationships with customers.

2.3. Expectation Confirmation Theory

The expectation confirmation theory (ECT) is a widely studied theoretical model in the field of consumer behavior and was originally proposed by Oliver [38] to explore the concept of customer satisfaction. Based on this theory, individuals pre-establish their expectations regarding a product or service before engaging with it, and subsequently assess their level of satisfaction based on the degree to which the product or service meets or surpasses those initial expectations [1, 38]. If a product or service satisfies or surpasses predetermined expectations, the individual experiences confirmation, resulting in positive satisfaction. Conversely, if the product or service fails to meet predetermined expectations, the individual experiences disappointment, leading to negative satisfaction [3]. Furthermore, the theory posits that post-consumption behavior is influenced by cognitive dissonance, a psychological state of mental discomfort that arises when individuals hold conflicting beliefs or values. A significant discrepancy between an individual's expectations and their actual experience with a product or service is likely to result in cognitive dissonance [38]. Research has demonstrated that ECT can be applied to multiple domains, including product repurchase [44], healthcare [8] and e-commerce [33]. Given the demonstrated predictive power of ECT in the various domains, we believe it is appropriate to use ECT to examine customer behavior on a company's data breach response strategy. In the course of a data breach, preserving customer loyalty is a crucial factor in a company's long-term costs [36], making it essential for companies to meet consumer expectations regarding their response to the breach. Nonetheless, there remains a paucity of research regarding the customer's viewpoint of response strategies and their expectations in this regard. According to ECT, companies should conduct a thorough exploration of customer expectations to align their response strategy and meet customer expectations following a data breach. This proactive approach can provide a useful way for companies to gain detailed insights into customer expectations, enabling them to adjust their response strategies and mitigate potential negative impacts on customer satisfaction, retention, and churn [16, 36]. Furthermore, this approach can assist companies in adapting their response strategies according to the diverse levels of severity inherent in various data breaches, as well as in gaining a comprehensive understanding of customers' distinctive expectations associated with each type of breach. To identify and gain an overview of these diverse and individual expectations regarding response strategies, we are conducting a qualitative study.

3. Research Methodology

Qualitative research places a significant emphasis on the lifeworld of individuals, aiming to comprehend specific perspectives [12]. This approach focuses on the subjective experiences of those involved [2]. Qualitative research describes social phenomena in detail and depth, allowing for a more nuanced understanding of human experience and behavior [26]. Since this research focuses on a user-centered view of data breach response expectations, qualitative research is appropriate for conducting this project. Therefore, the framework of Kuckartz & Rädiker [29] will be used in this thesis as it focuses on conducting a qualitative content analysis based on interviews. Fundamentally, it is about subjectivity, as Flick [11] points out, and the related

elicitation of the experiences and perceptions of those affected [2]. This can be achieved through qualitative social research.

3.1. Data Collection

In order to capture the user-centered view of expectations in response to data breaches, the problem-centered interview according to Witzel [50] was chosen. The problem-centered interview is a semi-structured open questioning method that focuses on a problem yet still allows the interviewees to express their personal viewpoints relatively freely [19]. The problem-centered interview is well-suited to the project of this study, which focuses on a user-centered view of expectations in response to data breaches. This topic represents a significant social problem of the modern age that affects both customers and companies. As previously noted, current measures such as compensation and apology often fail to meet customers' expectations of an appropriate response strategy and are insufficient in terms of recovery compared to service failures. Consequently, these measures cannot be fully applied in response to data breaches, and they do not necessarily provide full compensation for any damage incurred [9, 18]. Thus, it is crucial to identify a suitable response strategy that better meets customer expectations and strengthens the relationship between company and customer. Given the complexity of this topic, guiding the interviewer through targeted and follow-up questions during the problem-centered interview can yield the most nuanced and comprehensive data possible. For these reasons, the problem-centered interview was chosen. First, a short questionnaire was created using Qualtrics software to capture the socioeconomic background of the respondents, as suggested by Witzel [50]. This information also serves to enable the interviewer to prepare appropriately for the interview. Participants are asked about the frequency and companies involved in any past data breaches they have experienced, in order to address these cases specifically during the interview. If participants have not experienced a data breach, they were asked to provide the social media platforms they use and the health insurance company they are insured with, so that a representative fictional scenario can be presented to them. Furthermore, an interview guide was developed to serve as a frame of reference, incorporating pre-written questions that cover various topics [50]. The questions are designed to assess customer expectations following a data breach and are thus tailored to answer the research question. If the participants have not experienced a data breach, the guide includes a personalized scenario based on the information provided in the questionnaire. This approach is intended to ensure that all participants can best empathize with the case that they are affected by a data breach. On the other hand, if the participants have already been affected by a data breach, actual cases are addressed during the interview. This reference to real cases should allow to obtain valuable information about the expectations and the actual reaction of the companies. A total of twelve participants were recruited for the interviews. The demographics of the participants (age, gender, education level) were considered to ensure a diverse sample. The questionnaire revealed that four participants had experienced a data breach, five were unaware, and three had not yet encountered such an incident. The interviews lasted an average of 25 minutes, ranging from 14 to 39 minutes and were conducted between January and February 2023. The data collection process was concluded when it was determined that no new significant information was being revealed, thus achieving theoretical saturation, and ensuring that no additional properties or dimensions would emerge during the analysis [45]. All interviews were recorded and transcribed, following the transcription guidelines set forth by Kuckartz & Rädiker [29]. The transcription process resulted in a total of 99 pages of material.

3.2. Data Analysis

Since the content-structuring qualitative content analysis according to Kuckartz & Rädiker [29] is used in this work, the following explanations should make transparent how the results of this study were obtained.

Phase 1 - Initiating text work, memos, case summaries: The text was reviewed for components essential to answering the research question, and comments and notes were added.

Phase 2 - Develop main categories: The focus in this phase is on developing the main categories. During this phase, "Customer Expectations of the Company's Respond" could be identified as the first central main category.

Phase 3 - Coding data of the main categories (1st coding process): Any text passages with expectations were assigned the main category "Customer Expectations of the Company's Response" accordingly. If new main categories could be identified, they were included in addition to this one. It should be noted that text passages or individual sentences need not be assigned to a single category exclusively. A passage can pertain to several categories if multiple topics are addressed. The data were coded by two researchers. To ensure consistency, the coding results were reviewed and discussed together after every three interviews analyzed.

Phase 4 - Forming inductive subcategories: The next phase in the content analysis process is the differentiation of main categories into more specific subcategories. In this step, the expectations and thus the main category "Expectation of the company" were transferred into the concrete expectations.

Phase 5 - Coding data with subcategories (2nd coding process): In a second coding process, all text passages previously identified only as an expectation were coded with the appropriate subcategory and thus with the specific expectation. Analogous to the procedure in phase 3, further subcategories were included if they were identified.

Phase 6 - Simple and complex analyses: The sixth phase of this process involves preparing the presentation of the research results. Thus, all categories were examined, and interrelationships were explored in order to answer the research question and, beyond that, to possibly arrive at further findings.

Phase 7 - Writing down results and documenting procedures: This step reflects the elaboration of the present study.

4. Findings

4.1. Customer Expectations of the Company's Response

In terms of the RQ, customers' expectations of company response form the main category of this research. Table 1 illustrates how respondents' statements were assigned to each subcategory. This includes the various expectations that respondents have expressed regarding the company response because of the data breach (see Appendix, Table 4). To ensure anonymization of respondents, ID's B1 through B12 are used in the following.

Table 1
Categories of customers' expectations of the company's response

Category	Category definition	Example	Coding Rule
Compensation N = 10	The category compensation includes all customer expectations of compensation from the company as a result of a data breach.	"With the negligence one, there definitely, I do expect compensation at the end."	Applies if respondents expect compensation, even if it is not explicitly stated in what form this compensation is expected.
Notification N = 12	Includes all statements in which customers want to be informed about the incident.	"[I] would also want to know how it came about now."	Applies in the case that the respondents should be informed about the data breach.

Table 2
Categories of customers' expectations of the company's response (continued)

Category	Category definition	Example	Coding Rule
Follow-up Notification N = 5	Contains all statements in which further funding was expected from the company beyond initial information.	"I would always like to be informed about the next steps and that we might be able to talk a bit about this."	Applies when respondents want to be kept informed and want to know what happened with the data breach. Also, if this is mentioned in a different context.
Fast reaction of the company N = 6	Includes all statements that expect the company to respond quickly as a result of a data breach.	"Act as fast as possible, certainly, and contact affected parties and get it fixed as soon as possible."	Applies when respondents' statements call for or expect the company to respond quickly.
Transparency N = 5	Includes all statements in which companies are expected to be transparent in their dealings with data subjects.	"The more sensitive the data becomes, the more important it is (...) that companies are transparent (...)"	Applies if in the statements of the respondents a transparent handling of the data breach of the companies with the customers is expected.
Apology N = 9	The apology category includes all statements in which an apology was expected or requested.	"A company can also apologize here only I think in writing personally to one."	Applies when respondents expect an apology from the company.
Empathy N = 5	Includes all statements in which respondents expected empathy in communicating, apologizing, or communicating with the company.	"As long as (...) an empathic apology comes for it."	Applies when respondents expect empathy from the company.
Measures N = 12	Includes all statements in which respondents expected the company to take measures as a result of the data breach.	"That they'll make sure it never happens again."	Applies if the statements contain concrete suggestions for improving safety or refer to the fact that the problem will be remedied, and this will no longer occur.
Support N = 8	Includes all statements in which assistance is expected to be provided to affected individuals in dealing with a data breach.	"What consequences, what I could have to fear, how you would advise me, how I should best proceed regarding my data breaches."	Applies when the company is expected to take a collaborative approach to assist in dealing with the incident and to provide information about possible consequences and risks following a data breach.

Table 3
Categories of customers' expectations of the company's response (continued)

Category	Category definition	Example	Coding Rule
Participation in the decision-making process N = 6	Includes all statements where affected individuals want to be involved in the company's response process.	"I would like to find a way to satisfy both parties (...) [and] would like to participate in the decision-making process."	Applies when respondents want to be involved in the solution and decision-making process and can actively contribute their opinions.

Compensation: Ten out of twelve respondents expressed the expectation of compensation. The interviewees have different expectations and demands regarding the format and amount of compensation. In addition, it was also mentioned that there are different factors that influence the expectation of compensation as a response. In addition, two central subcategories of compensation were identified: Financial compensation and free/discounted services. Interviewee B3 stated that companies are only expected to pay compensation if the data breach has caused damage to the customer. If no harm has occurred, compensation is not necessarily expected, but is still perceived as positive. Furthermore, B5 has additionally mentioned that compensation is explicitly expected if the company has acted negligently. Connecting to this, B10 said that high compensation is expected in particular if sensitive data has been published. If the Severity of the data breach is less, compensation is also expected to be less. In addition to the general expectation of compensation, the expectation of financial compensation was also identified during the interviews. This category is defined by the explicit expectation of financial compensation expressed by the interviewees. In total, the expectation of financial compensation was expressed by eight interviewees. Within the financial compensation, this reveals that the expectation of financial compensation is influenced by the severity of the data breach. To this, it was also expressed by B4 that financial compensation is expected when damage has occurred to the respondents. In addition to the severity of the damage, B3 said that the type of data is a factor influencing the expectation of financial compensation, especially when sensitive data is involved. One further subcategory of compensation is the expectation of free/discounted services. This subcategory includes paragraphs in which the expectation of free or discounted services was mentioned. Free/discounted services were expressed by two interviewees. It was mentioned by B1 that the service should be suitable for the company and a service offered should be free or at a reduced price.

Notification: Interviewee B11 primarily expect to be notified about the breach and receive an explanation of how it happened and its potential causes. In addition, Respondent B5 and B8 suggested providing regular updates on the investigation's status, which should include information on the cause, scope, and impact of the breach, as well as which data was stolen and the extent of individual impact.

Follow-up Notification: Five out of twelve participants expressed a desire for follow-up notifications in addition to the initial notification. They seek information on the details of the data breach, the measures being taken, and preventive measures for future incidents. For example, B10 would like to be informed about the outcome of the data breach.

Fast Reaction of the Company: Half of the interviewees mentioned that they expect prompt action from the company in response to a data breach. This expectation is addressed on the one hand to the notification of this incident, and on the other hand to the measures that should be made in consequence, as B1 noted. Respondent B4 also expressed this expectation in the event of a data breach being reported through the media before being acknowledged by the company. In addition, B6 expressed that timely notification is expected especially when sensitive data is involved (see Type of data).

Transparency: Transparency describes the extent to which information is visible and accessible [51]. Five respondents expect companies to be transparent in their dealings with customers. In the case of sensitive data, respondent B3 expects increased transparency regarding

the whereabouts of the data and the company's-initiated measures. Furthermore, B5 expected continuous updates from companies during longer investigations, which should include the status of the investigations and future measures or precautions to be taken, as well as final results or findings. In addition, B5 mentioned the reduction of uncertainties and fears as a possible consequence of increased transparency.

Apology: Within the interviews, nine out of twelve interviewees expressed the expectation of an apology. In this context, different conditions were expressed when an apology is expected. For instance, Respondent B4 stated that an apology is only expected if the company is responsible for causing the data breach (see Company fault). Additionally, negative reactions may occur if the company does not apologize and does not meet expectations, as B7 stated in this context. B5, in turn, expects an apology regardless of whether the company is to blame for the data breach. However, in addition to the terms of when compensation is expected, there are also different expectations in which manner the apology should be delivered. In this context B1, expressed that a written apology was expected.

Empathy: The category of empathy is characterized by respondents' expectation of empathy in communication with the company as a result of a data breach. During the interviews, five interviewees said the expectation of empathy when communicating, apologizing, or communicating with the company. Thus, B7 expressed that empathy in the communication increases customer's forbearance as long as an empathetic apology is provided. Furthermore, it was added that the increased use of empathy is perceived positively and increases the customer's comprehension. Complementing this, B7 additionally specified that an empathic apology is expected.

Measures: All interviewees expected the company to perform measures in consequence of the data breach. In this context, this refers to all statements that contain specific suggestions for improving security or refer to the fact that the problem will be remedied. As several participants, including B4, noted, the measures should ensure that data breaches do not recur (see). A wide variety of possibilities are mentioned for companies to avoid such incidents as well as to minimize the damage afterwards. Specific ways to realize this expectation and avoid incidents of this nature were explained by B2 and B4. B8 additionally states that depending on the type of data, a higher level of data protection is expected.

Support: B10 expects support in dealing with a data breach and that the company will take a collaborative approach and provide information about possible consequences and risks following a data breach. Furthermore, the respondents also mentioned that they would like to receive preventive and protective measures or a possible guide on what to do or recommendations for action as noted by B4. This is supported by B8 and B9.

Participation in the Decision-making Process: When involving affected individuals in the company's response process to data breaches, half of the respondents expect to be included in the decision-making and solution-finding processes of the company's response. This is exemplified by B1's statement. Furthermore, B4 suggested that companies should offer different compensation options. Nevertheless, the opinion and input of affected individuals should be given room to maneuver, as B2 pointed out.

4.2. Influencing Factors of Customer Expectation

In addition to customer expectations, the interviews also identified various factors that influence customer expectations. Table 2 illustrates how respondents' statements were assigned to each subcategory. Although these have already been mentioned in the category of expectations, they are presented in their entirety in the following category (see Appendix, Table 5).

Table 2
Categories of influencing factors of customer expectation

Category	Category definition	Example	Coding Rule
Severity of the data breach N = 12	Includes all statements in which the severity of the data breach had an impact on the expectation.	"(...) and depending on the severity, of course, you would have to see whether financial compensation or compensation in kind would come into question."	Applies if the expectations regarding the severity of the data breach change. The same applies if they do not change and this factor is explicitly mentioned in this context.
Type of company N = 9	The type of company as a subcategory describes the influence of the type of company on the customer's expectation of the company's response as a consequence of a data breach.	"Because of the size of the company, I would definitely expect them to be more transparent about it, to follow up when a data breach happens."	Applies when the type of company had an impact on expectations
Type of Data N = 12	This category is characterized by respondents having different expectations for different types of data.	"Yes, if more sensitive data is affected, I expect fast notification."	Applies when the type of data has an impact on expectations.
Personal responsibility of the customer N = 4	This influencing factor affects expectations when customers themselves are responsible for what data and information they share.	"If it's kind of your own fault that something like that happens, that you change passwords more often or email addresses or something."	Applies when personal responsibility has had an impact on expectations.
Company fault N = 4	This category is defined by the fact that fault by the company affects expectations.	"Yes, so if I clicked on some phishing email and then my data was stolen, then of course I don't expect compensation from the company. (...) So if it's clear that the company has nothing to do with it, then I don't expect an apology."	Applies when expectations change, when the company is at fault or the not at fault.

Severity of the Data Breach: The respondents stated that the severity of the abuse, especially due to the type of data (see Type of data) and potential consequences, has an impact on their expectations of the company and customer reactions. B1 and B10 consider categorizing sensitive data as more severe and leaving an company in the event of far-reaching consequences. Furthermore, B3 mentioned that with increasing severity of the data breach, higher transparency, and more information from the company regarding the violation are expected.

Type of Company: The type of company describes the influence of the type of company on the customer's expectation of the company's response as a consequence of a data breach. In this context, nine of the twelve respondents expressed that the type of company had an influence on their expectations. In this regard, expectations are higher for companies that collect sensitive data than for companies with less sensitive data, as B7 said in this regard. In addition, interviewees B4 described that they have higher expectations regarding transparency and notification for data breach response at larger companies. It is also described that at smaller companies there is a higher level of understanding when a data breach occurs, as also noted by B4.

Type of Data: All respondents expressed that the type of data has an influence on their expectations towards the company. Firstly, it was expressed by B11 that the breach of sensitive data, especially health data is perceived as more significant. Furthermore, interviewees stated an expectation of compensation, in particular for sensitive data (see Compensation). In addition to compensation, more transparency in the handling of data breach was expected, especially for sensitive data (see Transparency). In addition, B6 expected rapid notification and response from the company. In addition, it was expressed by B11 that there is a higher expectation of protective measures by the company for sensitive data. On the other hand, B2 and B3 mentioned that for less sensitive data, compensation in the same way is sufficient regardless of the severity of the data breach (see Severity of data breach), as long as no personal or irreversible damage occurs.

Personal Responsibility of the Customer: In the context of this research, personal responsibility of the customers could be identified as an influencing factor. For four participants, this category influences expectations as a result of a data breach. It affects expectations if customers themselves are responsible for what data and information they share, as B7 notes. In addition to lower expectations to the company, the customer reaction is also influenced. This is changed by customers taking personal responsibility to protect themselves by taking measures, B4 commented.

Company Fault: The company fault is another factor influencing expectations. It was said by B4 that no compensation or apology is expected if the company is not at fault. If the company is at fault, then the company is expected to approach the customer with an optimal solution and participation in the decision-making process is therefore rejected, as B5 noted. As B5 also said, expectations are higher when the company is at fault, and in that case expects notification, information about what measures will be taken, an apology, and compensation. In addition, financial compensation in this context is seen as positive by B2.

4.3. Meeting the Customer Expectations

In connection with the expectations, we were able to identify various statements in the interviews that provide information about the reaction to meeting or not meeting the customer expectations. This category therefore shows, the perception of the customers, the impact on their attitude towards the company and what steps they would adopt in these cases. Table 3 illustrates how respondents' statements were assigned to this category. All respondents in this category indicated that not meeting expectations has negative consequences for the customer- company relationship (see Appendix, Table 6).

Table 3
Meeting the customer expectation

Category	Category definition	Example	Coding Rule
Meeting the customer expectation N = 7	The category contains all statements about what happens if expectations are met or not met.	“Because you're disappointed, simply. You had expectations, they are not fulfilled or just destroyed. And yes, then I am sad and that is normal.”	Applies when respondents gave their assessments of meeting and not meeting expectations.

B6 expressed disappointment in this regard. If expectations are not met, the majority of respondents indicate that they would leave the company or potentially switch to another one, such as B2 stated. If expectations are met, however, respondents indicate that their opinion and intention to enter into a business relationship with the company is reinforced, as B2 also stated. In addition, B8 stated that meeting expectations can strengthen the relationship and trust with the company. Respondents did not indicate whether they would also consider failure to meet expectations, in the sense of exceeding expectations, to be negative.

5. Discussion

Based on literature-based knowledge, twelve qualitative interviews were conducted under consideration of the ECT to gain an overview of the strongly individualized expectations [18, 36] and needs of customers in different situational and company contexts. The interviews conducted in this study enabled the interviewees to express their expectations of companies' response strategies in the event of a data breach.

5.1. Contribution to Literature

Our study contributes to the literature on data breaches and service failure in multiple ways, advancing existing research. This study employs a proactive and qualitative methodology to gather and analyze data on customer expectations and influencing factors before the occurrence of a data breach. We present valuable insights into individualized expectations of different demographic groups and contribute to the security literature by presenting unique data and theoretical perspectives, enabling companies to develop adjustments and novel approaches to meet customer expectations following a data breach. In doing so, our findings support and extend the current research of Goode et al. [16] and Hoehle et al. [18], which emphasize that companies should align their actions with customer expectations. Consistent with previous findings from the literature and research on the expectation of apology [6, 36] and compensation [16, 18, 30], respondents in our interviews also expressed this expectation. Additionally, they expressed a desire for companies to involve affected parties in the response process, which supports the earlier research findings of Diesterhöft et al. [9]. In addition to corroborating expectations derived from existing literature, this study yielded novel findings. These include new expectations as well as associated influencing factors. While our findings confirm previous research indicating that customer trust and loyalty are significantly impacted by a data breach, we found that a well-tailored response strategy that meets customer expectations can mitigate the loss of trust and loyalty. Moreover, the results of the interviews indicate that those affected expect greater empathy, transparency, and follow-up notifications from the company. These findings are consistent with crisis management research, which advocates open and continuous communication for companies [20, 46]. Another aspect of our study encompasses the identification of diverse factors influencing customer expectations pertaining to a company's response strategy in the context of data breaches. These factors include the type of data affected, the company's characteristics, the extent of the customer's culpability, the degree of the company's responsibility, and the severity or scope of the data breach incident. Our study partially contradicts existing literature and shows that affected individuals expect communicative interactions, such as follow-up notifications regarding the current status or updates, in order to stay informed. This insight introduces a novel approach wherein active, continuous communication in data breach response should be considered more as an ongoing process. This perspective carries implications for prior experiments and research designs, potentially leading to a reevaluation of response strategy effects on customers, subsequently altering their responses and perceptions.

5.2. Implications for the Management of Data Breach Responses

In addition to the theoretical implications, the results of this work also provide practical implications for companies to potentially improve the management of data breach responses. First, we were able to identify various customer expectations that concern how companies communicate with customers. These can be implemented as part of the legal notification of the data breach to optimize it in terms of customer expectations [23]. Specifically, when sensitive data is breached, respondents expect the company to communicate as soon as possible, as well as transparency in communication and handling of the data breach. In this context, interviewees also expect the company to keep the customer informed of the further progress of the data breach by means of follow-up notifications. In addition, our research provides new insights for the practical implementation of apology, which have not been previously considered in the literature [16, 18]. Our research suggests that apologies are particularly expected when the company is definitely at fault for the occurrence of the data breach. Moreover, in the context of communicating the data breach, it was also expressed that empathy is expected. This insight can be adopted by companies in the context of apology and notification in order to increase customer satisfaction and reduce the negative consequences of a data breach. Second, our research extends the outcomes-based approach of compensation [16]. Our research suggests that there are different expectations regarding the sensitivity of data and the severity of individual consequences related to compensation. For these cases, the majority of respondents indicated higher expectations for the level of compensation. Therefore, companies must manage data breach response in a situation-specific manner, considering the individual customer's expectations. Third, the interviews indicate several actions that respondents expect to take as a result of a data breach to address the problem. In particular, companies that hold sensitive data are expected to take preventive measures to minimize the likelihood of data breaches so that the company is better protected in the future.

5.3. Limitations and Future Research Directions

It is important to acknowledge that the findings of our study are subject to certain limitations stemming from the reliance on information and insights derived from the participants' experiences, opinions, and attitudes. Consequently, generalization of the results may not be feasible. First, it must be considered that only four of the twelve interviewees had previously been affected by a data breach. Thus, the expectations were only expressed in the context of a fictional scenario. As a result, it may not always match the actual response and expectations of a real data breach [16]. Second, the interviewees who were already affected by a data breach did not express their expectations immediately after the incident of the breach, but rather after the breach had occurred. Thus, their expectations could be biased by the time gap. Conducting interviews with affected parties immediately after the incidence of a data breach can increase representativeness. Third, it is crucial to examine the limitations associated with the experiment, particularly concerning the sample size and representativeness of the participants. In cases where the sample size is small, the results may lack generalizability and make it difficult to detect general trends or patterns in the results. Therefore, in future research also the sample size should be increased to achieve higher representativeness. Notwithstanding these limitations, qualitative research employing interviews can prove to be an invaluable method for delving into the experiences, opinions, and attitudes of the participants. It is of utmost importance to acknowledge the limitations, while appropriately interpreting and presenting the results to ensure the credibility and reliability of the study's conclusions. To strengthen our findings, future research could use a quantitative methodology. In the context of influencing factors, prospective research could be conducted. This would allow an analysis of customer expectations regarding the level of compensation and avoid the associated uncertainty as to how these can be reconciled [15].

6. Conclusion

Building upon prior research on data breaches and ECT, this study aims to investigate the expectations customers hold regarding a company's response to a data breach. We conducted problem-centric interviews within a qualitative study (n=12) to obtain an overview of individual customer expectations. Our research implies that customer expectations are highly personalized and influenced by various factors. In this regard, we lay the groundwork for future research to quantitatively examine additional expectations and consider influencing factors in the study design. Consequently, our research offers novel insights that should be taken into consideration when designing future research experiments. Moreover, we contribute valuable knowledge to practitioners by emphasizing the importance for companies to understand and be aware of customer expectations. Companies should tailor their data breach response to the specific situation, taking into account the expectations of individual customers. This highlights that the research area possesses additional gaps that warrant exploration in future studies. By examining the diverse and individual expectations of affected parties concerning the response strategies employed by companies during a data breach, the findings of this study have already made a substantial contribution in addressing these gaps.

References

- [1] Anderson, E.W. & Sullivan, M.W. (1993), 'The Antecedents and Consequences of Customer Satisfaction for Firms', *Marketing Science*, 12(2), pp. 125–143.
- [2] Blumer, H. (1980), 'Der methodologische Standort des symbolischen Interaktionsismus', in Arbeitsgruppe Bielefelder Soziologen (ed.) *Alltagswissen, Interaktion und Gesellschaftliche Wirklichkeit*. [Online]. Wiesbaden: VS Verlag für Sozialwissenschaften. pp. 80–146.
- [3] Bolton, R.N. & Drew, J.H. (1991), 'A Multistage Model of Customers' Assessments of Service Quality and Value', *Journal of Consumer Research*, 17(4), pp. 375–384.
- [4] Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. & Boss, R.W. (2009), 'If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security', *European Journal of Information Systems*, 18(2), pp. 151–164.
- [5] 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), pp. 70–104.
- [6] Chan, E.Y. & Palmeira, M. (2021), 'Political ideology moderates consumer response to brand crisis apologies for data breaches', *Computers in Human Behavior*, 121p. 106801.
- [7] Cheng, L., Liu, F. & Yao, D.D. (2017), 'Enterprise data breach: causes, challenges, prevention, and future directions: Enterprise data breach', *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5), pp. 1–14.
- [8] Chou, H.-K., Lin, I.-C., Woung, L.-C. & Tsai, M.-T. (2012), 'Engagement in E-Learning Opportunities: An Empirical Study on Patient Education using Expectation Confirmation Theory', *Journal of Medical Systems*, 36(3), pp. 1697–1706.
- [9] Diesterhöft, T.O., Schweneker, S.I., Masuch, K., Aslan, A. & Braun, M. (2022), 'The Role of Uncertainty in Data Breach Response Processes - A Reactance Theory Perspective', in 'Forty-Third International Conference on Information Systems', pp. 1–17.
- [10] Edwards, B., Hofmeyr, S. & Forrest, S. (2016), 'Hype and heavy tails: A closer look at data breaches', *Journal of Cybersecurity*, 2(1), pp. 3–14.
- [11] Flick, U. (2010), 'Gütekriterien qualitativer Forschung', in Günter Mey & Katja Mruck (eds.) *Handbuch qualitative Forschung in der Psychologie*. 1. Aufl [Online]. Wiesbaden: VS Verlag für Sozialwissenschaften. pp. 395–407.
- [12] Flick, U., Kardorff, E. von & Steinke, I. (2015), in *Qualitative Forschung. Ein Handbuch*. 11th edition. Rowohlt Taschenbuch.

- [13] Forbes R2_11 (2014), 'NVIDIA Corporate Network Breached', Forbes Media LLC., <https://www.forbes.com/sites/davelewis/2014/12/29/nvidia-corporate-networkbreached/?sh=489544a36241>. Accessed 18.03.2023.
- [14] Gatzlaff, K.M. & McCullough, K.A. (2010), 'The Effect of Data Breaches on Shareholder Wealth', *Risk Management and Insurance Review*, 13(1), pp. 61–83.
- [15] Gelbrich, K. (2010), 'Anger, frustration, and helplessness after service failure: coping strategies and effective informational support', *Journal of the Academy of Marketing Science*, 38(5), pp. 567–585.
- [16] 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*, 41(3), pp. 703–727.
- [17] HHS (2013), 'Breach Notification Rule', U.S. Department of Health & Human Services, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>. Accessed: 18.03.2023.
- [18] Hoehle, H., Venkatesh, V., Brown, S., Tepper, B. & Kude, T. (2022), 'Impact of Customer Compensation Strategies on Outcomes and the Mediating Role of Justice Perceptions: A Longitudinal Study of Target's Data Breach', *MIS Quarterly*, 46(1), pp. 299–340.
- [19] Hölzl, E. (1994) 'Qualitatives Interview', in Arbeitskreis Qualitative Sozialforschung & Otmar Chorherr (eds.) *Verführung zum Qualitativen Forschen: Eine Methodenauswahl*. [Online]. Wien: . pp. 61–68.
- [20] Huang, Y.-H. & Su, S.-H. (2009), 'Determinants of consistent, timely, and active responses in corporate crises', *Public Relations Review*, 35(1), pp. 7–17.
- [21] IBM & Ponemon Institute (2022), 'Cost of a data breach 2022 - A million-dollar race to detect and respond', <https://www.ibm.com/reports/data-breach>. Accessed 18.03.2023.
- [22] IBM & Ponemon Institute (2020), 'Cost of a Data Breach Report 2020',
- [23] Identity Theft Resource Center (2020), 'Data Breach Report in 2018', <https://www.idtheftcenter.org/post/identity-theft-resource-centers-annual-end-of->, Accessed: 18.03.2023.
- [24] Johnston, A.C., Warkentin, M., McBride, M. & Carter, L. (2016), 'Dispositional and situational factors: influences on information security policy violations', *European Journal of Information Systems*, 25(3), pp. 231–251.
- [25] Kaspersky (2022), *Cybersicherheit in der Supply Chain Deutschlands - Aktuelle Kaspersky-Studie legt Status Quo der IT-Sicherheit in deutschen Unternehmen offen*. (https://go.kaspersky.com/supply-chain-report-de.html?utm_medium=PR. Accessed: 18.03.2023.
- [26] Kergel, D. (2018) *Qualitative Bildungsforschung: Ein integrativer Ansatz*. Wiesbaden: Springer Fachmedien Wiesbaden.
- [27] Kim, S.H. & Kwon, J. (2019), 'How Do EHRs and a Meaningful Use Initiative Affect Breaches of Patient Information?', *Information Systems Research*,
- [28] Knight, R. & Nurse, J.R.C. (2020), 'A framework for effective corporate communication after cyber security incidents', *Computers & Security*, 99pp. 1–18.
- [29] Kuckartz, U. & Rädiker, S. (2022), in *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung: Grundlagentexte Methoden*. Grundlagentexte Methoden. 5. Auflage. Weinheim Basel: Beltz Juventa.
- [30] 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 & Production Management*, 37(1), pp. 56–74.
- [31] Kulynych, J. & Korn, D. (2002), 'The Effect of the New Federal Medical-Privacy Rule on Research', *New England Journal of Medicine*, 346(3), pp. 201–204.
- [32] Kwon, J. & Johnson, M.E. (2015), 'Protecting Patient Data-The Economic Perspective of Healthcare Security', *IEEE Security & Privacy*, 13(5), pp. 90–95.
- [33] Lu, K. & Liao, H. (2023), 'Dynamic preference elicitation of customer behaviours in e-commerce from online reviews based on expectation confirmation theory', *Economic Research-Ekonomska Istraživanja*, 36(1), pp. 2915–2938.

- [34] Malhotra, A. & Kubowicz Malhotra, C. (2011), 'Evaluating Customer Information Breaches as Service Failures: An Event Study Approach', *Journal of Service Research*, 14(1), pp. 44–59.
- [35] Martin, K.D., Borah, A. & Palmatier, R.W. (2017), 'Data Privacy: Effects on Customer and Firm Performance', *Journal of Marketing*, 81(1), pp. 36–58.
- [36] Masuch, K., Greve, M. & Trang, S. (2021), 'What to do after a data breach? Examining apology and compensation as response strategies for health service providers', *Electronic Markets*, 31(4), pp. 829–848.
- [37] Odusote, A. (2021), 'Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a More Robust and More Effective Legislation', *Beijing Law Review*, 12(04), pp. 1284–1298.
- [38] Oliver, R.L. (1980), 'A Cognitive Model of the Antecedents and Consequences of Satisfaction Decisions', *Journal of Marketing Research*, 17(4), pp. 460–469.
- [39] Ong, R. & Sabapathy, S. (2021), 'Hong Kong's data breach notification scheme: From the stakeholders' perspectives', *Computer Law & Security Review*, 42pp. 1–16.
- [40] Otto, P.N., Anton, A.I. & Baumer, D.L. (2007), 'The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information', *IEEE Security & Privacy Magazine*, 5(5), pp. 15–23.
- [41] Ponemon Institute (2022), Bericht über die Kosten einer Datenschutzverletzung 2022, IBM Security, <https://www.ibm.com/reports/data-breach>. Accessed: 18.03.2023.
- [42] Posey, C., Raja, U., Crossler, R.E. & Burns, A.J. (2017), 'Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA', *European Journal of Information Systems*, 26(6), pp. 585–604.
- [43] Roberds, W. & Schreft, S.L. (2009), 'Data breaches and identity theft', *Journal of Monetary Economics*, 56(7), pp. 918–929.
- [44] Spreng, R.A., MacKenzie, S.B. & Olshavsky, R.W. (1996), 'A Reexamination of the Determinants of Consumer Satisfaction', *Journal of Marketing*, 60(3), pp. 15–32.
- [45] Strauss, A.L. & Corbin, J.M. (1998), *Basics of qualitative research: techniques and procedures for developing grounded theory*, in 2nd ed. Thousand Oaks: Sage Publications.
- [46] Strong, K.C., Ringer, R.C. & Taylor, S.A. (2001), 'THE* Rules of Stakeholder Satisfaction (* Timeliness, Honesty, Empathy)', *Journal of Business Ethics*, 32pp. 219–230.
- [47] Tanimura, J.K. & Wehrly, E.W. (2009), *The Market Value and Reputational Effects from Lost Confidential Information*.
- [48] Whitler, K.A. & Farris, P.W. (2017), 'The Impact of Cyber Attacks On Brand Image: Why Proactive Marketing Expertise Is Needed for Managing Data Breaches', *Journal of Advertising Research*, 57(1), pp. 3–9.
- [49] Widup, S., Rudis, B., Hylender, D., Spitler, M., Thompson, K., Baker, W., Bassett, G., Karambelkar, B., Brannon, S., Kennedy, D. & Jacobs, J. (2015), *2015 Verizon Data Breach Investigations Report*.
- [50] Witzel, A. (2000), 'Das problemzentrierte Interview', in *Qualitative Social Research. Sozialforschung*, p. 13.
- [51] Zhu, K. (2002), 'Information Transparency in Electronic Marketplaces: Why Data Transparency May Hinder the Adoption of B2B Exchanges', *Electronic Markets*, 12(2), pp. 92–99.
- [52] Zviran, M. & Haga, W.J. (1999), 'Password Security: An Empirical Study', *Journal of Management Information Systems*, 15(4), pp. 161–185.

Appendix

Table 4
Statements of customers' expectations of the company's response

Category	Respondent	Statement
Compensation	B3	"If something had really happened, that someone had debited money from my account, then yes. But if I don't have any other obvious damage, then I don't think they have to give me anything back. That would be nice, but I don't think it's that important."
	B5	"With the negligence one, there definitely, I do expect compensation at the end."
	B10	"I expect a high level of compensation if personal data is published that is problematic or has far-reaching consequences for my working life. That means, for example, if I explain my relationships with some colleagues or bosses or whatever, and this is published, and as a result I have restrictions within my job: I am somehow removed because they have read how I think about some things or things like that, then I definitely expect a high level of compensation. But if it just comes out where I'm going to spend the next summer vacation, the compensation can definitely be lower."
	B4	"If I had suffered any financial loss, I would have definitely expected something like [a compensation]"
	B3	"It is much more sensitive data, my expectations are then already higher and also compensation"
	B1	"There is the possibility of the health insurance to receive services that are beneficial to your health, such as in the form of fitness programs, cures or much more, which must be taken over by each health insurance patient or each patient with to some extent, which they could then perhaps provide free of charge."
Notification	B11	"[I] would also want to know how it came about now."
	B5	"If the investigation drags on, [I] expect to receive updates on its progress."
	B8	"I would like to know exactly what data was misused and to what extent."
Follow-up Notification	B10	"I would always like to be informed about the next steps and that we might be able to talk a bit about this."
Fast Reaction of the Company	B1	"Act as fast as possible, certainly, and contact affected parties and get it fixed as soon as possible."
	B4	"By the time it comes out through the media, it's actually too late."
	B6	"If more sensitive data is involved, I expect to be notified in a timely manner."
Transparency	B3	"The more sensitive the data becomes, the more important it is (...) that companies are transparent (...)"
	B5	"If it drags on for a long time, I definitely also expect to be told in between how it looks and definitely at the end the result, the conclusion (...)."
		"[Transparency] is simply much more important. That you really get the feeling that you are not so much in danger."

Table 4
Statements of customers' expectations of the company's response (continued)

Category	Respondent	Statement
Apology	B4	"If it is obvious that the company has nothing to do with it, then I don't expect an apology."
	B7	"I would actually also consider whether I change the health insurance company then."
	B5	"I expect on both points that they contact me, give me info on how they want to proceed and apologize that it happened. So that's what I expect in both cases, even though it's not their fault."
	B1	"A company can also apologize here only I think in writing personally to one."
Empathy	B7	"The more empathetic at this point, the better. If you come back to it in the mail or letter and say, we've tried our best, we've implemented the possible security standards, and the attacker still succeeded, I think I have a little more understanding."
	B7	"As long as (...) an empathic apology comes for it."
Measures	B4	"That they'll make sure it never happens again."
	B2	"A general information or such a preventive screening to (...) check the passwords that were used (...), check them against such a database of public passwords."
	B4	"There's also two-factor authentication or something like that, but Zalando doesn't have that, which makes it a bit more secure somehow (...)."
	B8	"That it is ensured that this will definitely no longer occur in the future, because this is already very sensitive data, where I would also like to see a higher level of data protection than is currently the case with Instagram, for example."
Support	B10	"What consequences, what I could have to fear, how you would advise me, how I should best proceed regarding my data breaches."
	B4	"That they may also give me advice on how I could improve the security."
	B8	"How one is informed preventively."
	B9	"Support from the company (...), how I can proceed further and what I can do against it, and what the possibilities are for me."
Participation in the Decision-making Process	B1	"I would like to find a way to satisfy both parties (...) [and] would like to participate in the decision-making process."
	B4	"In the decision-making process, they could provide me with more options (...) [such as] the option to receive a voucher, a special membership, or free shipping."
	B2	"[And offer] some flexibility and work with you to find a solution that suits you."

Table 5
Statements on the factors influencing customer expectations

Category	Respondent	Statement
Severity of the Data Breach	B1	"Depending on the severity, [I would] (...) switch my health insurance company."
	B10	"If it has far-reaching consequences, I would really consider ending my relationship with the company."
	B3	"In the difficult case [I want to] get even more information about what was done to restore everything. So, in this case, I consider all the information even more important."
Type of Company	B7	"Because this is already very sensitive data, where I would also like to see a higher level of data protection than now, for example, with Instagram. Exactly. So, my expectations of health insurance are significantly higher."
	B4	"Because of the size of the company, I would definitely expect them to deal with it in a transparent way, that they keep following up on the data breach."
	B4	"But if it's not such a large company (...) and if you compare it with a small or medium-sized company, then you might be a bit more understanding for such a data breach."
Type of Data	B11	"Such data is of course very sensitive data and especially in relation to future employers, etc. It is of course difficult when such data is used. Of course, it is difficult when such data is made public."
	B6	"Yes, if more sensitive data is affected, I expect fast notification."
	B11	"Yes, because it is health data with which you can do a lot. And as I said, for example, that the employer might not consider you, I think that's definitely data where you should take very strong precautions and protective measures so that it doesn't get out to the public."
	B2	"If I don't have any other obvious damage, then they don't have to give me anything back. It would be nice, but I don't think it's that important [and] (...) if money should really be withdrawn, then (...) [I also want] the same amount of money back."
	B3	"The password was probably stolen and leaked at some point, but there was no intrusion by any third party trying to gain access to the account. That's why I wouldn't expect anything more based on my experience."
Personal Responsibility of the Customer	B7	"And I also assume that it will be the case at some point. But since I myself am also to a certain extent to blame for the information and data that I share and that can also become public, and I also believe that Instagram itself can do little about it, I actually don't expect that much at all."
	B4	"If it's kind of your own fault that something like that happens, that you change passwords more often or email addresses or something."
Company Fault	B4	"Yes, so if I clicked on some phishing email and then my data was stolen, then of course I don't expect compensation from the company. (...) So if it's clear that the company has nothing to do with it, then I don't expect an apology."

Table 5
Statements on the factors influencing customer expectations (continued)

Category	Respondent	Statement
Company Fault	B5	“For example, I think I would prefer they already have a solution. I think that if there is a problem that was perhaps caused by them because they had a security gap, then I think they must also come up with the optimum solution for me afterwards. And that's where I tend not to want to be involved in the decision-making process because I don't want to be involved that much.”
	B5	“So definitely, I would have much higher expectations if the company was negligent. So much higher. If I expect (...) that they contact me, give me information on how they want to proceed and apologize that it happened. (...) and with the negligence, there in any case, I already expect compensation in the end.”
	B2	“So, I wouldn't expect it, I wouldn't take it for granted. I would definitely appreciate it. Especially if we don't necessarily take Coinbase as an example now, but any data breakdowns where it was really the fault of the company itself in the past, because someone screwed up.”

Table 6
Statements on meeting the customer expectation

Category	Respondent	Statement
Meeting the Customer Expectations	B6	“Because you're disappointed, simply. You had expectations, they are not fulfilled or just destroyed. And yes, then I am sad and that is normal.”
	B2	“Then you go to the competition. Simple as that,”
	B2	“That would confirm me or at least confirm my opinion that I made the decision to become a customer of this company at the time.”
	B8	“Then I would definitely be satisfied (...). My trust (...) would be greater than before. (...) [I] would not worry that something like this will happen again or look for alternatives.”