

A Quantitative Study on the Impact of Data Breaches on Customer Satisfaction

Author: Mart Tijmen Riefel
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

ABSTRACT,

The escalating prevalence of online services and the consequential storage of data, increases the potential of (online) service failures, particularly in the form of data breaches. As a result, it has become essential to investigate the impact of such failures. In this paper, the focus lies on investigating the impact of an online service failure using an exemplary Data Breach Announcement (DBA). Utilizing, the CIA Triad model, failure characteristics and vulnerability perceptions provided by literature, the effect on customer satisfaction has been examined. The findings reveal that perceived risk has a negative impact, while cognitive trust has a positive impact on customer satisfaction in the aftermath of a Data Breach Announcement (DBA). The findings also emphasise the importance of effectively managing risk and nurturing cognitive trust to mitigate the negative consequences of data breaches.

Graduation Committee members:

Dr. Agata Leszkiewicz

Dr. Letizia Alvino

Keywords

Data Breach, CIA Triad, Cognitive Trust, Perceived Risk, Customer Satisfaction

1. INTRODUCTION

The rapid expansion of data collection by service providers is a tendency for potential data breaches. Data breaches are security episodes in which vulnerable data, such as government-managed retirement numbers, driver's permit numbers, names, and birthday celebrations, is presented to unauthorized third parties (Romanosky et al., 2011).

Latitude Financial Services, an Australian personal loan provider, confirmed on the 16th of March that it had been exposed to a data breach, with the impact of two service providers. Detecting unfamiliar activities, Latitude Financial Services discovered itself being a victim of a malicious cyber-attack. The subsidiary of Deutsche Bank verified that the breach was caused by stolen employee login credentials. Accordingly, the breach impacted the data of approximately 330.000 customers. Consisting of identification documents, passport numbers, or other personal information. As Latitude Financial Services has not been successful in terminating the incident, numerous systems remain inaccessible to its customers. (Hope, 2023) Between 2005 and 2022, the Privacy Rights Clearinghouse (PRC) reported 20,030 data breaches involving 1,993,414,981 breached records only in the USA. Despite the significant emphasis on consciously working with sensitive data, training employees or numerous cyber policies, hackers continue to find the weak spots for a potential cyber-attack (*Data Breach Chronology* | *PrivacyRights.Org*, n.d.).

The potential for e-commerce is without question undeniable, yet this area is commonly threatened by service failures. Service failure involves activities resulting from customers' perception of the initial service failing below the customer's set expectations. (Zeithaml et al., 1993) In the online environment, it is common to save confidential information. For customers, it is an easy way, most important, a useful way of saving passwords, codes, or any other sensitive and confidential data in one 'cloud'. Until the service fails and the personal codes are exposed. Consequences of online service failures can be the inaccessibility of a service, a leak of data or a decline in trust.

Rui Sousa and Christopher A. (2009) conducted an empirical study in which they took a better look at the effect of service failures and recovery in e-services. Through an online survey limited to actual customers of commercial e-banking services, they investigated the behaviour of customers after an online service failure. Concluding that the customers' reaction to an online service failure does not differ much from a traditional service failure. Yet it is harder to reassure customers' loyalty after an online disruption in service (Sousa & Voss, 2009). A different paper studied customers' reactions to security breaches concerning the best approach for companies to minimize its damage. Accordingly, awareness of accountability for data breaches has had a significant impact on how individuals respond to organizations' attempts to restore trust. Also, participant personalities influenced perceptions of responsibility and trust in companies after a data breach (Carre et al., 2018).

1.1 Research Objective and Question

While there is existing research on cyber incidents and their influence on customers' loyalty and/or trust, there is a gap in understanding how customers perceive online service failures caused by cyber incidents. Afroz et al. (2013) conducted research in which they established a correlation between a customer's trust and the customer's awareness of a data breach. Another study saw that the impact of a leak in data is massive. So concluded Ariffin et al. (2019) that such incidents lead to financial loss, image damage, a decline in customer trust and

conformity issues for the firm itself. Our research objective is the need for research that explores the impact of different types of cyber incidents on customers' perceptions of service quality, such as their expectations, satisfaction, and willingness to continue using the service. Additionally, there is a need for research that investigates how customers respond to service failures caused by cyber incidents, including e.g., their likelihood to engage in negative word-of-mouth, complaints, or switching behaviours. Understanding these responses is crucial for service providers and other online platforms in developing effective strategies for managing and mitigating the impact of cyber incidents on customer satisfaction, loyalty, and retention. Ultimately, according to Schlackl et al., (2022), there is currently a lack of research on the consequences of a data breach and how it affects the customers affected. Chakraborty et al., (2016) made a connection in that perceived severity and perceived risk are both relevant drivers for post-breach shopping, but research on cognitive trust and its effect on customer satisfaction after reading a data breach announcement could be explored more. As this research is also answering to the literature's call for further research regarding data breaches combined with the non-U.S data sets (Schlackl et al., 2022).

Based on the research gap, we can identify the different variables of perceived risk, cognitive trust, and customer satisfaction. Using these variables, we can create a research question that will help address decreasing the research gap about this topic. The research question therefore will be: ***What is the impact of perceived risk and cognitive trust on customer satisfaction with online services in the aftermath of service failures caused by cyber incidents?***

In conducting this research, we will use a quantitative survey based on a sketch of a breach announcement and apply one of the aspects of the CIA framework (Confidentiality, Integrity, and Accountability). This CIA framework is a well-established model in cyber security to guide and help study the impact of information breaches. (*Confidentiality, Integrity, and Availability: The CIA Triad* | *Office of Information Security* | *Washington University in St. Louis*, n.d.). Due to the time and scope of the research, this thesis will solely focus on the confidentiality aspect of a data breach.

1.1.1 Practical Relevance

As the academic relevance has been established, it is also important to acknowledge the practical relevance of this research question, which lies in that the question addresses new insights into how service providers can better respond to and manage cyber incidents. Several researchers have established the relationship between a negative impact of a service breakdown and customer behaviour (Srinivasan et al., 2002). Understanding the impact of cyber incidents on the core variables (perceived risk, cognitive trust, and customer satisfaction), service providers can anticipate and develop approaches to mitigate the potential loss and rebuild the relationship that was harmed with its customer. In general, this research aims to improve resilience towards cyber incidents related to customers of service providers and service providers themselves.

2. LITERATURE REVIEW

2.1 CIA Triad

As mentioned in the introduction, the CIA triad model is a framework in cyber security that helps to study the impact of information breaches. The framework consists of three aspects, confidentiality, integrity, and availability. According to the European Commission, (2016), "A data breach occurs when data for which your company/organization is responsible suffers a

security incident resulting in a breach of confidentiality, availability or integrity.” The elements of the CIA triad framework thus address the effect of a data breach: confidentiality (i.e. “preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information”), integrity (i.e. “guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity”) and availability (i.e. “ensuring timely and reliable access to and use of information”) (U.S. Government Publishing Office, 2015, p. 153). Figure 1 gives a representation of the CIA Triad framework.

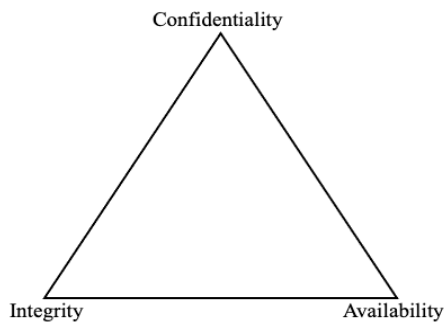


Figure 1 - CIA Triad

2.1.1 Confidentiality

The first requirement for information systems is that they should act in accordance with the confidentiality aspect. This indicates that the system should only distribute data to the authorized person. As data must be only accessible to the designated users, measures should be taken to protect and prevent data from getting exposed.

2.1.2 Integrity

A second requirement for information systems is integrity. Integrity refers to the accuracy and consistency of data and prevents unauthorized or accidental modifications to data. Failure to maintain can lead to significant consequences including loss of trust in data. Information systems therefore should ensure that the data is being protected. It is crucial to take precautions to ensure that information systems live up to the integrity requirement of the CIA triad.

2.1.3 Availability

The last aspect of the CIA triad model is availability. Another important aspect information systems should use. As stated above, the availability requirement is to ensure authorized users have timely and uninterrupted access to resources and services. Information systems should be available when needed, i.e., in critical operations to avoid disruptions. To maintain this feature, organizations should implement measures such as redundancy, or have disaster recovery backup plans.

2.2 Independent Variables

2.2.1 Cognitive Trust

Cognitive trust is derived from theoretical viewpoints of seeing trust as a rational choice, that is rooted in economic (Williamson, 1993), political (Hardin, 2002), and sociological (Coleman, 1990) theories. According to (Komiak & Benbasat, 2006) cognitive trust is defined as a ‘trustor’s rational expectations that a trustee will have the necessary attributes to be relied upon.’ As stated in the CIA Triad, a data breach occurs when the data of whom a company is responsible suffers a security incident. Therefore, the appearance of cognitive trust in

data breaches is motivated by the fact that customers trust organizations to protect their sensitive data from security incidents. If breached, this may lead to negative perceptions of trust. Martin et al., (2017) conducted a study that confirmed different types of data vulnerabilities that may affect customer’s trust. The study highlights the importance of cognitive trust in the context of data breaches.

2.2.2 Perceived Risk

In this research, we will define perceived risk as a *consumer’s faith about uncertain outcomes of an online service interruption*. Supported by (Baker, 2001, p. 233) who states that “perceived risk is associated with uncertainty and magnitudes of outcome.” Various types of risks have been identified by (Jacoby & Kaplan, 1972), i.e., financial, performance, physical, psychological, social, time and opportunity cost risks. In our study, three types of risk are most relevant. The three types of risk address different aspects that a customer may experience when a data breach occurs. First, psychological risk is related to the emotional impact of the breach, such as feelings of violation or loss of control. Financial risk is related to the possible financial impact caused by the incident. Lastly, performance risk is related to the impact of the breach on the organization’s operations.

2.3 Dependent Variable

2.3.1 Customer Satisfaction

Customer satisfaction is an important variable for a company’s performance. Therefore, it is in our interest to research. For a clear picture of this study, it is of essence to have a well-defined definition of customer satisfaction. According to (Hill et al., 2003) customer satisfaction is “a measure of how your organization’s ‘total product/service’ performs in relation to a set of customer requirements.” As a data breach result may have an impact on personal and sensitive data, the customer’s satisfaction with the organization may be decreasing as a result. The Net Promoter Score (NPS) is a widely adopted metric by service industries. The NPS was first introduced by Reichheld as a metric to predict future sales. Through time it has been beneficial too for measuring customer loyalty. Asking customers the famous ‘how likely are you to’ questions, the Net Promoter Score is an adequate metric to use to measure customer satisfaction (Baehre et al., 2022).

2.4 Hypotheses

To answer the main research question of this thesis. *What is the impact of perceived risk and cognitive trust on customer satisfaction with online services in the aftermath of service failures caused by cyber incidents?*, two questions have been formulated in the style of hypotheses.

2.4.1 Cognitive trust and customer satisfaction

The satisfaction of a customer’s experience can be an indicator of the level of trust a customer has in a company. As companies actively use online channels for collecting data, the severity of a data breach can result in a negative impact on the customer’s trust (Greve et al., 2020). The level of a consumer’s trust in a company can be a factor in the satisfaction of customers in a company. If a customer perceives a company as trustworthy, the customer is more likely to have positive feelings about the company, its products, and its services. Resulting in a potentially higher level of customer satisfaction. Nevertheless, cognitive trust can also have a negative impact on customer satisfaction. A customer with a low(er) level of trust is more likely to have negative feelings about the company and thus a lower level of

satisfaction. This has led to the formulation of the following hypothesis:

Hypothesis 1: A higher level of cognitive trust increases customer satisfaction. Therefore the level of cognitive trust while reading a data breach announcement (DBA) has a positive impact on CS.

2.4.2 Perceived risk and customer satisfaction

The fear of a customer's sensitive data being exposed to the outside is a crucial factor in a customer's satisfaction. A customer's feeling about a perceived severity of a data breach manifest itself in the possible consequences of this breach (Chakraborty et al., 2016). The emotion, and perceived risk, that a customer associates with a service failure impact the satisfaction of the customer. Accordingly, this brings us to the following hypothesis.

Hypothesis 2: A higher level of perceived risk reduces customer satisfaction. Therefore the perceived risk of a data breach announcement (DBA) has a negative impact on CS.

2.5 Conceptual Framework

Considering our independent and dependent variables, including the hypotheses that have been formulated to help investigate the impact of an online service failure on a customer, the following conceptual framework has been developed:

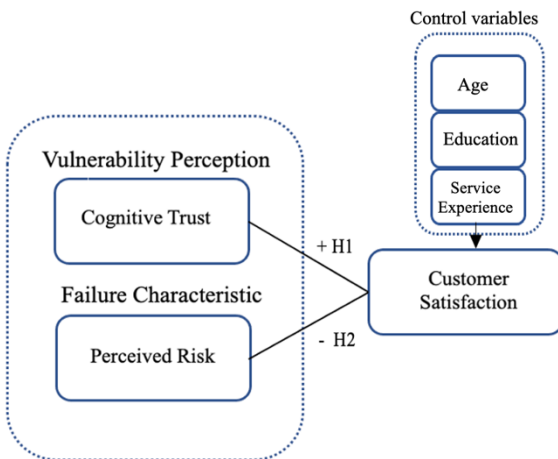


Figure 2 - Conceptual Framework

3. METHODOLOGY

3.1 Research Design

To test the formulated hypothesis, a quantitative study has been conducted. According to Saunders et al., (2019, p. 178) "A quantitative study examines relationships between variables, which are measured numerically and analyzed using a range of statistical and graphical techniques." This study will be solely based on a questionnaire, known as a mono-method quantitative study (Saunders et al., 2019).

The data of this paper is the data obtained from the survey. The approach of using surveys was chosen for several reasons, including its cost-effectiveness, convenience, and wide reach. Online surveys provide a platform for researchers to collect data from a large and diverse pool of participants, regardless of geographical location. Moreover, online surveys allow for automated data collection, reducing the likelihood of errors and minimizing the potential for data loss. The questionnaire will give an exemplary DBA, of which the sample will be asked to answer several questions using a 7-point Likert

scale (1 = strongly disagree, 7 = strongly agree). Likert Scale questions are often used in research as they allow for a "degree of opinion" or no opinion at all. It gives a better representation for individuals to express their opinion. The main advantage of Likert Scale questions is that they are not simply answered by a "yes" or "no" (Likert Scale Definition, Examples and Analysis, 2022). Therefore, the use of the Likert Scale questions offers a valuable way to gather a deeper understanding of the respondents in this study.

Surveys can be an effective tool used for research that investigates the perception of customers of an online data breach. As such, it allows researchers to collect data directly from customers who use(d) online services. Also, the survey can be conducted anonymously, which increases the likelihood that participants will provide honest and representative answers.

3.2 Control Variables

To enhance the validity of this research, control variables have been added to prevent any other factors from influencing the relationship between the dependent and independent variables. Three control variables have been implemented that may influence the outcome of this study.

Starting with the variable age. Age can have a strong role in influencing the relationship between the independent and dependent variables. People of different age groups have different experiences and perspectives in life that can influence the outcome of this study. Age as a control variable helps to mitigate effects that may arise due to age differences.

Next, education is also an important control variable to consider. Education also has a crucial role in the knowledge a person possesses. Therefore, it may influence the outcome of this study. Controlling for education helps to minimize bias due to educational differences and helps enhance the internal validity of this research.

Lastly, customers' experience with Netflix has also been included as a control variable. Controlling for service experience, we eliminate the influence of a customer's past experience with Netflix, and therefore solely focus on the impact of our exemplary DBA.

3.3 Sample

Having a good and representative sample is a crucial aspect to consider in research. It helps to make reliable and trustworthy conclusions that will support the hypothesis created. A large number of participants in a study is preferred as it will reduce the impact of random errors, increase its validity and make results more accurate. The sample for this study must be carefully considered as it is of the essence that the sample represents the study (Becker, 2008, p. 67). To conduct a study about the effect of a data breach announcement on customer satisfaction, the sample must be aware of the impact and effect of a service failure.

A total of 193 participants filled out the distributed questionnaire. This number is considered to be a representative sample and helps increase the sample's validity of the findings (Hartley, 2014).

However, due to incomplete surveys; 55 (28,5%), and participants that did not consent with the term 4 (2%), we must subtract and remove these recordings from the data analysis. To be precise, responses that were missing one or more answers in the questions related to one of the variables were considered not useful. Subtracting these responses from our sample leaves us

with only 134 responses out of 193. This is the final sample that will be used for analysis.

3.4 Questionnaire Questions

The questions that are used in the survey are carefully considered to gain insight into the effect of cognitive trust and perceived risk on customer satisfaction and are adapted from existing studies. Table 1 gives a representation of the question chosen. The questionnaire used can be found in the appendix. (Appendix, section 1)

Variable	Source	Items
Cognitive trust (IV)	(Martin et al., 2017) (Hess Jr. et al., 2003)	CT1-CT4*
Perceived risk (IV)	(Chakraborty et al., 2016)	PR1-PR3*
Customer satisfaction (DV)	-	3**
Age (CV)	(Dangelico et al., 2022)	1 - Ordinal variable
Education (CV)	(Dangelico et al., 2022)	1 - Ordinal variable
Service Experience (CV)	-	1 – “How would you rate the services from Netflix?”

**Both IV's are measured on a 7-point Likert scale.*

***DV is measured using the Net Promoter Score.*

Table 1 - Operationalization of main concepts

3.5 Data Collection

The data collection process is a crucial step in any research endeavour. Given the focus of this study on the impact of an online data breach, an online questionnaire was considered to be the most appropriate method for data collection. This choice was based on the fact that the target audience primarily utilizes the online internet platform, making an online survey a logical and also relevant way to gather information for this research.

The distribution process for this study used a wide range of channels to reach potential participants. Different social media platforms including Facebook, LinkedIn, Snapchat, WhatsApp, and Instagram were employed to distribute information about the survey and invite individuals to participate and help with this research. These platforms were selected due to their many active users and also their ability to target specific people. Additionally, personal networks and acquaintances were used as well, as they provided an opportunity to use existing connections and expand the reach of the survey. By utilizing both social media channels and personal networks, a broader and more varied amount of participants was reached, ensuring a diverse representation and enhancing the validity of the study.

All respondents in the survey participated on a voluntary basis with the possibility to stop and withdraw at any time during the survey. The survey was conducted anonymously to ensure its confidentiality.

4. RESULTS

The questionnaire is being evaluated using the coding program Rstudio. A numeric cvs file containing the responses of all participants has been used for assessing the data collected. For each of the Likert-scale questions of the independent variables and the Net Promoter Score questions of the dependent variable the mean and standard deviation have been taken to show its significance towards the hypothesis and for its descriptive statistics visualization.

The hypothesis will be evaluated as follows; first, by conducting a linear regression analysis. Secondly by using descriptive statistics. Moreover, correlations between the different variables are investigated as well. A detailed overview of the regression analysis can be found in the Appendix (Appendix – section 2)

Variable	Mean	Standard Deviation (SD)
Customer Satisfaction (DV)	6.443	1.255
Perceived Risk (IV)	4.190	1.036
Cognitive Trust (IV)	5.027	0.892
Age (CV)	2.984	1.392
Education (CV)	3.806	0.791
Service Experience (CV)	4.566	0.883

Table 2 - Descriptive Statistics

4.1 Analysis of the dependent variable

4.1.1 Customer Satisfaction

To assess the dependent variable customer satisfaction the Net Promoter Score was used as a measurement tool. These 'how likely are you' questions were asked to participants on a scale of 0 to 10. Divided into three categories: detractor (0 till 6), passive (7 and 8) and promoter (9 and 10). Based on the NPS scale, the mean was calculated to be 6.44 with a standard deviation of 1.25.

The NPS serves as a valuable metric to use for measuring customer satisfaction. Not only does it measure overall satisfaction, but it also focuses on the likelihood of customers recommending a product, service or company to others. On average, with a mean of 6.44, participants express a level of dissatisfaction based on the NPS score. As 6.44 equals a detractor. Yet, the standard deviation (1.25) indicates variability in the responses. Suggesting that the satisfaction level among participants varies.

Therefore it is important to address the underlying factors that lead to a lower or higher level of customer satisfaction. This motivates us to study the different factors that influence customer satisfaction, our independent variables.

4.2 Analysis of the independent variables

4.2.1 Perceived Risk

In the analysis, it becomes apparent that the variable perceived risk revealed valuable insights into its role within this research context. The participant's perception of risk was assessed using Likert scale questions scaled from 1 to 7 (strongly disagree – strongly agree). Together with a descriptive statistics

summary, indicating a mean of 4.19 and a standard deviation of 1.03. This indicates that on average the participants chose the option “neither agree nor disagree”. Yet, the standard deviation of 1.03 reveals that there is variation in the responses.

To examine the impact of perceived risk, a linear regression analysis has been conducted to investigate the significance of this variable. A linear regression model is a procedure for calculating the values of the dependent variable from the independent variables. It is a technique to analyze the strength and relation between a dependent and (a) predictor variable(s) (Kumari & Yadav, 2018). The results of the linear regression analysis revealed that perceived risk plays a significant role in the model. Thus, the variable perceived risk being significant emphasizes the impact of people’s risk perception in this study.

By including perceived risk as an independent variable in this study, we gain a more in-depth insight into how people’s perception towards risk contributes to the research area.

4.2.2 Cognitive Trust

The Likert Scale questions for the variable cognitive trust revealed interesting insights in the responses collected. They provide insight into the trust participants have towards data breaches. 59% of the participants expressed their agreement/strong agreement with the assumption that Netflix will do everything in its power to solve the problem. Indicating that among the participants, Netflix holds a strong commitment to addressing and solving issues for its users.

Furthermore, it is worth mentioning that the median values of the cognitive trust questions fall within the range of 5 or 6. This indicates that participants generally answered questions with a level of agreement, reflecting the positive side of cognitive trust.

In terms of descriptive statistics, the analysis shows cognitive trust having a mean of 5.02 and a standard deviation equaling 0.89. These statistics show that the participants on average have a moderate level of cognitive trust. Moreover, the standard deviation of 0.89 indicates a limited dispersion around the mean, thus implying a consistent degree of trust among the participants.

Lastly, the linear regression model supports that cognitive trust is also a significant contributor to the dependent variable. It highlights the influence of cognitive trust towards the dependent variable which is customer satisfaction. The significance demonstrates its relevance in shaping an individual's perceptions and behaviours to, in the context of this study, customer satisfaction. These findings can also be seen in Table 3, which gives a neat and short overview of the linear regression. Appendix – section 3 gives an overview of the entire linear regression model.

Independent variables	Coefficient	SE	Significance
Perceived Risk	-0.358	0.101	<0.001***
Cognitive Trust	0.448	0.114	<0.001***
Age (CV)	Included		
Education (CV)	Included		
Service (CV)	Included		

Table 3 - Linear Regression

4.2.3 Control variables

The linear regression analysis, which can be found in Appendix – Section 3, reveals that non of the control variables are found to be significant. This means that these control variables do not have a significant influence on the dependent variable, namely, customer satisfaction.

4.3 Correlations between the variables

Correlation is an important aspect of research. It is a measure that shows how two variables are related to each other. If one variable changes, the other will change too. In the table below we can find the correlations between the variables used in this study.

	Cognitive Trust	Perceived Risk	Customer Satisfaction
Cognitive Trust	1	-0.267	0.469
Perceived Risk	-0.267	1	-0.367
Customer Satisfaction	0.469	-0.367	1

Table 4 - Correlation Table

Looking at the numbers in Table 4, it is noticeable that between the variables “cognitive trust” and “customer satisfaction” a positive correlation exists ($r = 0.47$). This means that participants that have a higher level of trust, also tend to have a higher level of customer satisfaction. Next, we can observe a negative/weak correlation between the variables “cognitive trust” and “perceived risk” ($r = -0.27$). This suggests that as the cognitive trust level among participants/individuals increases, the level of perceived risk decreases. Similar to the variables “perceived risk” and “customer satisfaction” ($r = -0.37$), also a negative observation. An increase in the level of risk tends to decrease the level of customer satisfaction.

To finalise this analysis, the results of the regression analysis show that both of the variables are significant. This confirms that perceived risk and cognitive trust have an impact on a customer’s satisfaction. The correlation analysis shows that cognitive trust is positively correlated with customer satisfaction. The analysis also reports that higher levels of perceived risk are negatively correlated with customer satisfaction. Based on these results, both hypotheses are supported.

5. FINDINGS

In the first part of this section, the findings of the analysis are evaluated and light will be shed on whether the hypotheses are supported or will be rejected. Afterwards, implications are made based on the findings and resulting in answering the research question of this paper, namely what will the impact be of data breaches customer's satisfaction?

5.1 DISCUSSION

The findings of this study shed light on the relationship between the variables. The data obtained from the analysis provide useful insights into the factors influencing customer satisfaction. To reach the objective of this study, the research question has been split up into two subquestions in the form of hypotheses.

The first hypothesis, “a higher level of cognitive trust increases customer satisfaction”, suggested that there is a positive link between the variables. In other words, individuals who have a greater level of trust in an organization’s handling

and/or its ability to resolve the problem, are expected to have a higher level of satisfaction. To test this hypothesis, a linear regression analysis has been performed as well as a correlation test. The results showed a strong significance and a positive correlation ($r = 0.469$, $p < 0.001$) between cognitive trust and customer satisfaction. As customer satisfaction is closely related to cognitive trust, it is logical to expect that a customer's level of trust will have an impact on a customer's satisfaction. In the exemplary DBA, a customer with high levels of trust believes that the company will have the right necessities to resolve the issue and protect their data. This trust makes them satisfied customers as they trust the company to take care of their data. Therefore, the results support the hypothesis, confirming that cognitive trust has a positive impact on customer satisfaction

The second hypothesis stated; "*a higher level of perceived risk reduces customer satisfaction*", suggesting there is a negative relation between the variables. The findings indicated a significant negative relationship between the impact of risk and customer satisfaction ($r = -0.267$, $p < 0.001$). Therefore, this result also validates the hypothesis and will not be rejected. A higher level of perceived risk associated with the Data Breach Announcement (DBA) negatively impacts the satisfaction of a customer. Thus, when individuals associate a high level of risk the moment their confidential data is exposed, they are more likely to be less satisfied customers. The hypothesis is also supported by the CIA Triad. As mentioned in Chapter 2; "a data breach occurs when the data of whom a company is responsible suffers a security incident." After a confidential data leak, customers are most likely to experience heightened levels of perceived risk and are more concerned about an organisation's ability to protect their data. Resulting in less satisfied customers.

The purpose of this research was to explore the relationship between cognitive trust, perceived risk, and customer satisfaction in context of a data breach. In line with this objective, the following research question had been formulated: "*What is the impact of perceived risk and cognitive trust on customer satisfaction with online services in the aftermath of service failures caused by cyber incidents?*". Two hypotheses were formulated to answer this question. Evidence from this research supports both hypotheses, showing that perceived risk has a negative impact on customer satisfaction, while cognitive trust has a positive impact. Concluding, customer satisfaction declines after a cyber incident as customers perceive increased risks with online services. Conversely, customers have a greater level of trust in the organization's ability to handle service failures and protect their data.

5.2 Implications

Based on the findings, general implications can be drawn. The results highlight the importance of cognitive trust and perceived risk in shaping a customer's satisfaction when experiencing a data breach.

5.2.1 Practical implications

First, this study emphasizes the importance for organizations to prioritize and take an effort in maintaining and building trust among customers as trust has a critical role in influencing customers' perceptions towards, in this case, a breach containing confidential data. Moreover, the importance for organizations to ensure an adequate level of trust among customers is essential for establishing long-term customer relationships. Secondly, this research can aid organizations to highlight the importance of taking steps to address the relationship between perceived risk and its negative influence on

customer satisfaction. Understanding how perceived risk can negatively impact customer satisfaction with regards to a DBA, organizations can work on mitigating and managing these risks effectively. Organizations being proactive in this matter benefits the relationship between them and their customers.

5.2.2 Theoretical implications

This research makes valuable contributions to existing literature. First of all, it addresses a gap identified by Schlackl et al., (2022) who called for further research on data breaches combined with non-US data sets. This study expands the geographical scope and enhances the requirement of conducting research beyond the US-data sets. Next, this study introduces the variable cognitive trust and perceived risk in relationship with customer satisfaction to the existing literature on data breaches. While previous studies have explored the relationship of e.g. perceived risk and post-breach shopping (Chakraborty et al., 2016), there remains a gap in the understanding of cognitive trust (and perceived risk) and its impact on customer satisfaction.

Furthermore, the use of the CIA Triad model is important for understanding the impact of a data breach on customer satisfaction, focusing on the confidentiality aspect. This aspect emphasizes the protection and distribution of confidential, sensitive data (U.S. Government Publishing Office, 2015, p. 153). Incorporating this model in this research has been useful to understand the importance of confidentiality. The CIA Triad model has helped to explore how data breaches can affect customer satisfaction and how organizations need to prioritize the protection of customers' data.

Additionally, zooming in on three risks mentioned by Jacoby & Kaplan, (1972), namely psychological, financial and performance risk, the findings show implications for both customers and organisations. The findings indicate that a higher degree of perceived risk associated with a data breach is linked to decreased customer satisfaction. Thus, organizations should focus on enhancing data protection (performance risk), acknowledge and address the emotional impact of the breach to restore trust (psychological risk) and lastly, organizations must prioritize the protection of customers' data as these incidents can be financially harmful (financial risk).

In conclusion, this study contributes to the existing literature by filling a research gap. The research gap addresses the relationship between vulnerability perception and failure characteristics and its influence on customer satisfaction in the context of a confidentiality data breach announcement. Using the CIA Triad model, with a focus on the confidentiality aspect, this study gained insights into the importance of data protection.

6. CONCLUSION

In this research paper, the influence of a data breach on customer satisfaction has been investigated. In more detail, this study answers the research question that aims to understand the impact of service failures caused by cyber incidents on customer satisfaction with online services. The findings in this study provide evidence that supports both hypotheses as both variables were significant. This study also examined and included control variables to ensure validity. No abnormalities in the control variables were discovered. Concluding, the impact of perceived risk and cognitive trust on customer satisfaction followed by a data breach announcement highlights the importance for organizations to ensure confidentiality.

7. LIMITATIONS AND FUTURE RESEARCH

There were certain limitations encountered during the timeline of this research. First of all, due to time constraints, not all aspects of the CIA (Confidentiality, Integrity and Availability) Triad model were evaluated and included in this study. The focus was primarily on the confidentiality aspect. Therefore, future research could dive deeper into one of the other components or every triad of the model to gain more understanding of the impact of a service failure on customer satisfaction. Secondly, this paper only looked at one individual company. Meaning, that the findings and results might not apply to other companies or industries. Every organization may have their unique characteristics that might influence outcomes. Future research could address and explore this limitation by including multiple companies from different industries/sectors. Lastly, the sample size ought to be 193, yet after subtracting invalid responses, the final sample was 134. Due to time constraints, this study had a relatively small number of participants. A larger sample size would have allowed for a more thorough analysis.

8. ACKNOWLEDGEMENTS

First and foremost I am truly grateful to my supervisors Dr Leszkiewicz and Dr Alvino, my bachelor's circle and the University of Twente for the guidance, feedback and criticism throughout writing this bachelor's thesis. Especially the help with RStudios. To continue, I want to express my gratitude to the 193 people that have responded to my questionnaire. I would like to extend a special thank you to those who not only participated in my survey but also engaged in forwarding and spreading the word about my bachelor's thesis. Finally, I want to thank my friends and family for supporting me throughout this process and my entire study.

9. REFERENCES

- Afroz, S., Islam, A. C., Santell, J., Chapin, A., & Greenstadt, R. (2013). How Privacy Flaws Affect Consumer Perception. *2013 Third Workshop on Socio-Technical Aspects in Security and Trust*, 10–17. <https://doi.org/10.1109/STAST.2013.13>
- Ariffin, M. A. M., Rahman, K. A., Darus, M. Y., Awang, N., & Kasiran, Z. (2019). Data leakage detection in cloud computing platform. *International Journal of Advanced Trends in Computer Science and Engineering*, 8(1.3 S1), 400–408. Scopus. <https://doi.org/10.30534/ijtcse/2019/7081.32019>
- Baehre, S., O’Dwyer, M., O’Malley, L., & Lee, N. (2022). The use of Net Promoter Score (NPS) to predict sales growth: Insights from an empirical investigation. *Journal of the Academy of Marketing Science*, 50(1), 67–84. <https://doi.org/10.1007/s11747-021-00790-2>
- Baker, M. J. (2001). *Marketing: Critical Perspectives on Business and Management*. Taylor & Francis.
- Becker, H. S. (2008). *Tricks of the Trade: How to Think about Your Research While You’re Doing It*. University of Chicago Press.
- Carre, J. R., Curtis, S. R., & Jones, D. N. (2018). Ascribing responsibility for online security and data breaches. *Managerial Auditing Journal*, 33(4), 436–446. <https://doi.org/10.1108/MAJ-11-2017-1693>
- Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*, 83, 47–56. <https://doi.org/10.1016/j.dss.2015.12.007>
- Coleman, J. S. (1990). *Foundations of social theory* (1st paperback edition). Belknap Press of Harvard Univ. Press.
- Confidentiality, Integrity, and Availability: The CIA Triad | Office of Information Security | Washington University in St. Louis*. (n.d.). Retrieved 26 March 2023, from <https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/>
- Dangelico, R. M., Alvino, L., & Fraccascia, L. (2022). Investigating the antecedents of consumer behavioral intention for sustainable fashion products: Evidence from a large survey of Italian consumers. *Technological Forecasting and Social Change*, 185, 122010. <https://doi.org/10.1016/j.techfore.2022.122010>
- Data Breach Chronology | PrivacyRights.org*. (n.d.). Retrieved 24 March 2023, from <https://privacyrights.org/data-breaches>
- European Commission. (2016). *What is a data breach and what do we have to do in case of a data breach?* https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-to-do-in-case-data-breach_en
- Greve, M., Masuch, K., & Trang, S. (2020). *The More, the Better? Compensation and Remorse as Data Breach Recovery Actions – An Experimental Scenario-based Investigation* (p. 1293). https://doi.org/10.30844/wi_2020_12-greve
- Hardin, R. (2002). *Trust and trustworthiness*. Russell Sage Foundation.
- Hartley, J. (2014). Some thoughts on Likert-type scales. *International Journal of Clinical and Health*

- Psychology*, 14(1), 83–86.
[https://doi.org/10.1016/S1697-2600\(14\)70040-7](https://doi.org/10.1016/S1697-2600(14)70040-7)
- Hess Jr., R. L., Ganesan, S., & Klein, N. M. (2003). Service Failure and Recovery: The Impact of Relationship Factors on Customer Satisfaction. *Journal of the Academy of Marketing Science*, 31(2), 127–145.
<https://doi.org/10.1177/0092070302250898>
- Hill, N., Brierley, J., & MacDougall, R. (2003). *How to Measure Customer Satisfaction*. Gower Publishing, Ltd.
- Hope, A. (2023, March 23). *Latitude Financial Services Data Breach Leaked Customer Data From Two Service Providers*. <https://www.cpomagazine.com/cyber-security/latitude-financial-services-data-breach-leaked-customer-data-from-two-service-providers/>
- Jacoby, J., & Kaplan, L. (1972). The Components Of Perceived Risk. *Advances in Consumer Research*, 3.
- Komiak, S. Y. X., & Benbasat, I. (2006). The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents. *MIS Quarterly*, 30(4), 941–960. <https://doi.org/10.2307/25148760>
- Kumari, K., & Yadav, S. (2018). Linear regression analysis study. *Journal of the Practice of Cardiovascular Sciences*, 4(1), 33.
https://doi.org/10.4103/jpcs.jpcs_8_18
- Likert Scale Definition, Examples and Analysis*. (2022, November 3).
<https://www.simplypsychology.org/likert-scale.html>
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, 81(1), 36–58.
<https://doi.org/10.1509/jm.15.0497>
- Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft?: Do Data Breach Disclosure Laws Reduce Identity Theft? *Journal of Policy Analysis and Management*, 30(2), 256–286. <https://doi.org/10.1002/pam.20567>
- Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students*. Pearson Education, Limited.
<http://ebookcentral.proquest.com/lib/itc/detail.action?docID=5774742>
- Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, 59(4), 103638.
<https://doi.org/10.1016/j.im.2022.103638>
- Sousa, R., & Voss, C. A. (2009). The effects of service failures and recovery on customer loyalty in e-services: An empirical investigation. *International Journal of Operations & Production Management*, 29(8), 834–864. <https://doi.org/10.1108/01443570910977715>
- Srinivasan, S. S., Anderson, R., & Ponnavaolu, K. (2002). Customer loyalty in e-commerce: An exploration of its antecedents and consequences. *Journal of Retailing*, 78(1), 41–50. [https://doi.org/10.1016/S0022-4359\(01\)00065-3](https://doi.org/10.1016/S0022-4359(01)00065-3)
- U.S. Government Publishing Office. (2015). *Title 44—Public Printing and Documents*. <https://www.gpo.gov/docs/default-source/congressional-relations-pdf-files/uscode-2015-title44.pdf>
- Williamson, O. E. (1993). Calculativeness, Trust, and Economic Organization. *The Journal of Law and Economics*, 36(1, Part 2), 453–486. <https://doi.org/10.1086/467284>
- Zeithaml, V. A., Berry, L. L., & Parasuraman, A. (1993). The nature and determinants of customer expectations of service. *Journal of the Academy of Marketing Science*, 21(1), 1–12. Scopus.
<https://doi.org/10.1177/0092070393211001>

10. APPENDIX

10.1 Section 1 – Questions Questionnaire Qualtrics

Dear Participant, I would like to invite you to take part in my survey. Your input is important to me and will contribute to valuable insights into the topic of my research. I am conducting a research about the impact of a data breach on customer satisfaction.

To ensure that you are completely acquainted about what will happen during the survey, I want to make you aware of a few important points:

- Your data will be stored in a secure and confidential manner.
- The survey is estimated to take approximately 5-15 minutes of your time.
- The data collected will only be used for the purposes of this research.
- Your responses will be anonymous, and your personal information will not be shared with any third parties.
- Your participation in the survey is voluntary, and you are free to withdraw at any time.

I appreciate your time and effort in providing me with your insights. Thank you for your participation in advance!

If you have any questions please reach out to:

Mart Riefel

m.t.riefel@student.utwente.nl

I consent. (1)

I do not consent. (2)

Skip To: End of Survey If Dear Participant, I would like to invite you to take part in my survey. Your input is important t... = I do not consent.

This survey will consist of two parts. In the first part, you will be presented with possible scenario about Netflix. Please take the time to read the scenario thoroughly and ensure that you understand the information provided.

The second part of the survey will consist of a series of questions related to the scenario. You will be asked to respond to each question using a Likert scale, where 1 represents "strongly disagree" and 7 represents "strongly agree".

Please consider each question carefully and provide your most accurate response based on your personal opinion.

Please answer beforehand the following questions about your familiarity with Netflix.

Are you familiar with the company Netflix?

- Yes, I am. (1)
 - No, I am not (2)
-

I have watched movies/series on Netflix

- Yes, I have. (1)
 - No, I have not. (2)
-

Display This Question:

If I have watched movies/series on Netflix = Yes, I have.

I have my own Netflix account

- Yes, I have. (1)
 - No, I have not (2)
-

Please indicate your age range:

- Under 18 (1)
 - 18 - 24 (2)
 - 25 - 34 (3)
 - 35 - 44 (4)
 - 45 - 54 (5)
 - 55 - 64 (6)
 - 65 and older (7)
-

Please select your highest level of education.

- Primary education (1)
 - Lower secondary education (2)
 - Upper secondary education (3)
 - Bachelor's degree (4)
 - Master's degree (5)
 - PhD (6)
-

Control variable How would you rate the services from Netflix?

0 1 2 3 4 5 6 7 8 9 10

Use the slider. (0 very bad, 10 very good) ()



Streaming giant Netflix hit by a cyber-attack

PR Newswire

May 17, 2022 Monday 4:30 PM EST

Announcement

Customers of the streaming platform Netflix (**NASDAQ: NFLX**) have been notified of a data breach when the company suffered a phishing attack. This resulted in an unauthorized access to Netflix users' information.

Shortly before the cyber-attack, the hacking network PoodleCorp took responsibility for it via Twitter.

"We're currently informing affected users and working to resolve the issue as fast as possible." tweeted John Smith, the CEO of Netflix via their Twitter account.

Sean Newman, Director at Corero Network Security, said that the attack was "proof that organisations which depend on their online presence need a protection against cyber-security threats."

Please indicate your opinion about the following statements about Netflix:

	Strongly disagree (1)	Disagree (2)	Somewhat disagree (3)	Neither agree nor disagree (4)	Somewhat agree (5)	Agree (6)	Strongly agree (7)
Netflix is a trustworthy company. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Netflix is a reliable company. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have confidence in Netflix's action/behaviours (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I expect Netflix to do everything in its power to solve the problem. (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I expect Netflix to have done everything in its power to prevent the problem. (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please answer the following questions with regards to the given scenario

	Strongly disagree (1)	Disagree (2)	Somewhat disagree (3)	Neither agree nor disagree (4)	Somewhat agree (5)	Agree (6)	Strongly agree (7)
If the data I share with Netflix, was involved in a cyber incident it would be a serious problem for me. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer's information stored by Netflix is not safe. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer's are vulnerable if Netflix faced incidents of hacking. (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q18 How likely are you to recommend Netflix to a friend or colleague?

- 0 (0)
- 1 (1)
- 2 (2)
- 3 (3)
- 4 (4)
- 5 (5)
- 6 (6)
- 7 (7)
- 8 (8)
- 9 (9)
- 10 (10)

Q19 How likely are you to recommend Netflix as a secure environment for your personal data?

- 0 (0)
- 1 (1)
- 2 (2)
- 3 (3)
- 4 (4)
- 5 (5)
- 6 (6)
- 7 (7)
- 8 (8)
- 9 (9)
- 10 (10)

Q20 How likely are you to recommend Netflix based on recent experiences?

- 0 (0)
- 1 (1)
- 2 (2)
- 3 (3)
- 4 (4)
- 5 (5)
- 6 (6)
- 7 (7)
- 8 (8)
- 9 (9)
- 10 (10)

10.2 Section 2 - Questionnaire overview

Control questions (YES or NO)

- Are you familiar with the company Netflix?
- Have you watched movies/series on Netflix?
 - IF YES: Do you currently have an active Netflix subscription?

IV Cognitive Trust; scale 1 (strongly disagree) – scale 7 (strongly agree) (Martin et al., 2017) (Hess Jr. et al., 2003)

- CT1 Netflix is trustworthy
- CT2 Netflix is reliable
- CT3 I have confidence in Netflix behaviours/actions
- CT4 I expect Netflix to do everything in its power to solve and prevent the problem.

IV Perceived Risk; scale 1 (strongly disagree) – scale 7 (strongly agree) (Chakraborty et al., 2016)

- PR1 If a service/company where I store data faced a cyber incident, it would be a serious problem for me
- PR2 Customers' information stored at online service providers is not safe.
- PR3 Customers are vulnerable in online websites that had incidents of hacking

DV Customer Satisfaction; Net Promotor Score; Scale 0 (not likely at all) – scale 10 (extremely likely)

- How likely are you to recommend Netflix to a friend or colleague?
- How likely are you to recommend Netflix as a secure environment for your personal data?
- How likely are you to recommend Netflix based on recent experiences?

CV: Age (Dangelico et al., 2022)

Please indicate your age range:

- Under 18
- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65 and older

CV: Education (Dangelico et al., 2022)

Please select your highest education level

- Primary education
- Lower secondary education
- Upper secondary education
- Bachelor's degree
- Master's degree
- PhD

CV: Service; scale 0 (very bad) – scale 10 (very good)

- How would you rate the services from Netflix?

10.3 Section 3 – Linear Regression Model (Rstudio)

Call:

```
lm(formula = fun_controls1, data = mydata_analysis)
```

Residuals:

Min	1Q	Median	3Q	Max
-2.93716	-0.54267	0.00655	0.59241	2.37339

Coefficients: (2 not defined because of singularities)

	Estimate	Std. Error	t value	Pr(> t)	
(Intercept)	7.0724	1.2845	5.506	2.43e-07	***
meanPR	-0.3586	0.1017	-3.525	0.000618	***
meanCT	0.4485	0.1144	3.921	0.000154	***
Control.variable2	-2.9157	1.5151	-1.924	0.056876	.
Control.variable3	-2.7271	1.5190	-1.795	0.075342	.
Control.variable4	-2.6105	1.5155	-1.722	0.087795	.
Control.variable5	-2.4810	1.5402	-1.611	0.110096	
Control.variable6	-2.6810	1.5940	-1.682	0.095414	.
Control.variable7	-3.0269	1.8541	-1.633	0.105424	
Control.variable.12	0.4534	1.0823	0.419	0.676103	
Control.variable.13	0.4785	0.7705	0.621	0.535820	
Control.variable.14	0.6177	0.7626	0.810	0.419683	
Control.variable.15	0.3912	0.8068	0.485	0.628698	
Control.variable.16	NA	NA	NA	NA	
Control.variable_15	-0.8669	1.3171	-0.658	0.511815	
Control.variable_16	-0.4019	0.8691	-0.462	0.644735	
Control.variable_17	0.8664	0.8251	1.050	0.296016	
Control.variable_18	1.0185	0.8195	1.243	0.216557	
Control.variable_19	1.2288	0.8557	1.436	0.153839	
Control.variable_110	NA	NA	NA	NA	

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 1.037 on 110 degrees of freedom

(3 observations deleted due to missingness)

Multiple R-squared: 0.409, Adjusted R-squared: 0.3177

F-statistic: 4.478 on 17 and 110 DF, p-value: 5.771e-07
