MASTER THESIS

CUSTOMER'S PERCEPTIONS OF AN ONLINE SERVICE FAILURE WITH APPLICATION OF THE CIA MODEL

AUTHOR: THOM STORTELER

STUDENT NUMBER: 2732394

FACULTY BMS | MSC BUSINESS ADMINISTRATION

SPECIALIZATION | STRATEGIC MARKETING SERVITIZATION

1ST SUPERVISOR: DR. AGATA LESZKIEWICZ

2ND SUPERVISOR: DR. LETIZIA ALVINO

DATE: 18/12/2023

ACKNOWLEDGEMENTS

I enjoyed carrying out this research as it is an interesting and current topic. For this I am very thankful as my 1st supervisor, Dr. Agata Leszkiewicz supported me during the research. Her guidance and clear explanations helped me to progress during the master thesis process. Due to these in-depth analyses, I acquired some helpful new knowledge. Next to that, I am grateful for the patience and expertise from my 1st supervisor as this makes working together more comfortable. We discussed about topics and in the end we came up with this topic where we both felt satisfied with. Additionally, I would like to thank my 2nd supervisor, Dr. Letizia Alvino as she was already familiar with a topic like this and therefore a good fit. Finally, I want to thank all the respondents in this study for their time to fill in the questionnaire which was an essential part of this study. Their input was very helpful as it contributed to making an adequate data set that could be analysed in order to finish the research.

ABSTRACT

As companies are more and more steering their operations based on the acquired data of their customers, the value of this data is on the rise. The arrival of the internet is underlying to this change in doing business. Nowadays, companies acquire data of their customers, and this makes it possible to make the best suitable offer. This might seem as a very good method as the companies can make a personalized offer for each of their customers. However, the downside of this is that a data breach can expose all the valuable and classified data of customers while customers trusted the company. This research aims to discover how customers will react after a Data Breach Announcement (DBA). This study derived important literature by executing a systematic literature review. The derived literature was helpful in order to determine constructs that can be measured by executing the questionnaire whereafter the results could be analysed. The empirical research has been conducted, resulting in 135 valid responses. The valid responses were then used for data analysis. The data was analysed in a quantitative way as exploratory factor analysis and regression analysis has been conducted. The results expose a direct effect of the types of data breaches on the reactions of the customers. Because the introduction of the DBA (IV) influences customer reactions (DV's). For example, the outcome of the statistical software shows a decrease in trust after the Data Breach Announcement has been made. Another example is the decrease in customer satisfaction after the introduction of the DBA. The DBA is something negative so it was also expected that it will affect some reactions in a negative way. Next to the direct effects, the moderation effect has also been studied. Apology as a service recovery action shows a moderation effect as it softens the reaction a customer has after a DBA occurred.

Keywords: Customer's Perceptions; Emotional Response; Online Service Failure; Confidentiality; Integrity; Availability; Data Breach Announcements

Table of Contents

1. Introduction 5

1.1. Situation and Complication 5

1.2. Research Goal and Research Question 6

1.3. Theoretical Background 6

1.4. Academic and Practical Relevance 15

1.4.1. Academic Relevance 15

1.4.2. Practical Relevance 15

1.5. Outline 16

2. Literature Review and Hypotheses Development 17

2.1. Materials and Methods 17

2.2. Results 18

2.2.1. Conceptual Framework 19

2.2.2. Main Findings and Hypotheses Development 19

2.2.3. Interpreting the Main Findings 25

2.3. Discussion 26

3. Methodology 27

3.1. Research Design 27

3.2. Selection 29

3.3. Sample 29

3.4. Measurement 30

3.5. Data Collection 30

3.6. Data Analysis 32

4. Results 32

4.1. Descriptive Statistics 32

4.2. Exploratory Factor Analysis 33

4.3. Regression Analysis 34

4.3.1. Regression for Trust 35

4.3.2. Regression for Quality of Service 36

4.3.3. Regression for Failure Attribution 36

4.3.4. Regression for Customer Satisfaction 37

4.3.5. Regression for Severity of Service Failure 38

4.3.6. Regression for Frustration 38

4.3.7. Regression for Anger 39

4.3.8. General Findings 39

5. Conclusions and Discussion 42

5.1. General Discussion 42

5.2. Conclusion 43

5.3. Theoretical and Managerial Implications 44

5.3.1. Literature Review 44

5.3.2. Empirical Study 45

5.4. Limitations and Future Research 46

5.4.1. Literature Review 46

5.4.2. Empirical Study 46

References **48**

Appendices **54**

Appendix A – Manipulated Announcements 54

1. Introduction

1.1. Situation and Complication

With the increasing importance of data, it is key to look at information security threats at service providers. When information security is not up to date, service providers are vulnerable, and this can cause a leak of data due to various reasons such as hacker attacks. These firms have to protect their data at all costs because it is a valuable asset in the way they are doing business. There are multiple ways in which a data breach can occur, and this can harm a service provider and its users. This makes it interesting which reaction it provokes by the customers. The customer's perception is therefore a great construct to research because perception is a broad construct as it is about interpretation and observation of something. When a data breach occurs, customers may also react in an emotional way as this is human to happen. There revolves a lot around the topic of data breaches and that is what makes it an interesting matter.

As is said before, the importance of data and digital technologies is massively increasing and especially in the last decade. Due to this, there is an increasing amount of smart service companies who use data to operate in their business such as Netflix. This research revolves around Netflix because Netflix is very well known by a lot of people in the world. Next to that, the phrase smart service companies is very broad. Netflix is a smart service company and thus it is easier to get an idea by it. Via the data from their members, Netflix can for example track down their viewing behaviour. This is very helpful for Netflix because they have an algorithm that triggers the members to keep watching something that is alike the series or movies that they are currently watching or have previously watched. This algorithm is very advanced and enhances the viewing numbers substantially. Information such as ratings, what members play, browse or search is very helpful to be able to personalize Netflix's service (Amatriain, 2013). Due to the fact that this is the force of data, it is becoming very valuable. In fact, they rely on data to thrive in their business. At the end of 2022, Netflix nearly had 231 million paid subscribers. Netflix is appealing for subscribers from all age groups. These subscribers are also from diverse ethnic backgrounds and that is the reason why Netflix has such a broad range of series and movies.[1] This is a classic example of knowing their subscribers and tailoring the offer to the needs of the subscribers. Furthermore, Netflix spends a huge amount on marketing activities. Last year, it was around 2.53 billion U.S. dollars. The

[1] https://www.statista.com/statistics/250934/quarterly-number-of-netflix-streaming-subscribers-worldwide/

strength from Netflix's marketing team is that they are able to increase the audience engagement by operating on a personalized level. By doing this, Netflix can eventually notify their subscribers with upcoming releases that are relevant for its subscribers.[2]

For this research, seven conditions have been chosen to measure the customer's perception. More information about how this has been conducted can be found in the part about the research design. To be able to assess information security, the literature provided lots of information about confidentiality, integrity and availability. These three components together form the CIA Triad which is a model designed to guide policies for information security within an organization (Fenrich, 2008). In this research, the CIA Triad is the independent variable as this variable is already established when a data breach occurs. The customer's perception is the dependent variable as this variable is a reaction to the independent variable. When a data leak occurs, a company might not act in a desirable way to search for solutions. This means that customers are going to behave differently. Due to that, service recovery has also been assessed in this research. The reason for this is that it is also important how a service provider behaves after a data breach. When their reaction is appreciated by the customers, it might possibly retain them.

1.2. Research Goal and Research Question

The goal of this research is to explore the effect of an online service failure within a service provider on the customer's perceptions. The entire research will revolve around the main question. Therefore, the following research question has been formulated: *"Based on the CIA dimensions, to what extent does an online service failure change customer's perceptions of the service provider?"*

1.3. Theoretical Background

In this section, the constructs that are at the centre of this paper are being discussed. Based on previously conducted research, every construct is explained and if necessary with the help of examples.

Hacker Attacks

The internet is continuously developing as it is a platform where nearly all the people in the world have access to. Due to this increase from the internet, the online businesses are also

[2] https://www.statista.com/statistics/1097045/netflix-marketing-expenditure/

progressing because they gain with the development of the internet. Over the past decades, the internet has brought numerous good things such as email and electronic commerce. More and more computers are getting connected to the internet and another thing that is still upcoming is IoT (Internet of things). For example, nowadays it is possible to connect smart and wireless devices to the internet such as a watch and a washing machine. Because of the propel innovation of the internet, the administration, private industry and the regular computer client have fears of their information or private data being contained by a criminal hacker (Sanctum Inc, 2002). Lots of people do think that hacking is a basic activity. The truth is that hacking is far from a basic activity, it is a so called aptitude and you have to have a natural talent for it. As a person, you have to have interest in IT and all that has to do with computers. Hacking is unapproved utilization of computer and system assets. The hacker who is guilty of hacking is a programmer who breaks in the computer of another person without authorization. Often with the goal to steal information of the party and benefit by the data leak (Kumar & Agarwal, 2018). According to Madarie (2017), the motivation of hackers is based on intellectual challenge and curiosity. Hackers are rather motivated by what they dislike instead of being motivated by what they value. Engaging in hacker activities is an intellectual challenge as hacking is often seen as something that is difficult. The people engaged in hacking are often smart people that know how to work with computers. Curiosity is a relatively innocent motivator, however if the hacker succeeds it still harms the hacked company. Curiosity is all about how far an individual dares to go with their hacking actions. “Hacking is the technique of finding the weak links or loopholes in the computer systems or the networks and exploiting it to gain unauthorized access to data or to change the features of the target computer systems or the networks. Hacking describes the modification in the computer hardware, software or the networks to accomplish certain goals which are not aligned with the user goals.” (Gupta & Anand, 2017).

Service Interruptions

Smart service companies are relying very much on data as data is one of the most important aspects for a smart service company to do the job. As previously has been explained, the data tells the companies a lot about their members. In fact, their operations are tailor made based on the data of their members. Due to this, the power of these companies is to make a personalized offer to their members. This is also what today’s customer is looking for. The mentality of the customers has drastically changed in the last decades. Today’s customers like to be spoilt as it gives them the feeling that everything has been customised to their wants and needs. Personalization is used to improve customers' lives while increasing their engagement and loyalty to a firm. It is often seen as a good incentive to retain the customers as the customers are feeling comfortable at this service and are willing to stay (Pappas et al., 2017). Service interruptions can be caused by several incidents. Obviously, the target for a company is to minimize service interruptions. Even minor service interruptions may cause problems for the companies because it is outside their control. The companies want to control everything on the area of service because in that way they are able to provide the best service possible to their members. Malfunctions are unfortunately part of a smart service company as data and internet are underlying to do their business. Previous conducted research resulted in the fact that malfunctioning and IT problems impacted severely on the quality of service provided, resulting in a lack of trust from clients and a serious reputational loss for the company (Annarelli et al., 2020). On the other hand, to try and manage service interruptions there are several actions that companies can do. Constant monitoring support, development of specific procedures to assist peripheral offices and guarantees of continuity of service provision, extension of opening hours, and the establishment of a task force dedicated to handling the problem. The downside of these articulated actions is that it will cost a lot of money. That is the consideration that a company should make which is easier said than done (Annarelli et al., 2020).

Data Breaches

"A data breach is a security incident in which sensitive, protected, or confidential data are copied, transmitted, viewed, stolen, or used by an unauthorized individual." (U.S. Department of Health and Human Services, 2015). According to Sen and Borle (2015), the sensitive, protected or confidential data may include personal health information, personal identifiable information, trade secrets or intellectual property, and personal financial data. As all these aspects are very personal, it may harm an individual when these credentials are being exposed. With the importance of data, data breaches are commonplace. Major data breaches are publicly known but minor breaches are occurring each day. These data breaches are happening in various industries. Examples of industries are insurance, social media, healthcare, financial services and more. These industries contain a lot of data and that is why a data breach can be very harmful (Khan et al., 2021). "A data breach is the intentional or inadvertent exposure of confidential information to unauthorized parties." (Cheng et al., 2017). Currently, humankind is living in a fast pacing environment. The reason for this fast pacing environment is because humans have entered the digital era. In this digital era, data has become one of the most critical components of an enterprise. Data breaches poses serious threats to enterprises. With reputational damage and financial losses being the biggest threats. Due to the growing volume of data, detecting and preventing data loss has become one of the most pressing security concerns for enterprises. Despite a plethora of research efforts on safeguarding sensitive information from being leaked, it remains an active research problem (Cheng et al., 2017). The upcoming subsections are about the CIA Triad to explain what confidentiality, integrity and availability entails.

Confidentiality

Organizations rely heavily on the use of information technology (IT) products and services to run their day-to-day activities. Ensuring the security of these products and services is of utmost importance for the success of the organization (Nieles et al., 2017). Confidentiality is basically about authorized persons which have access to specific data because the data should only be accessible to intended users. Sensitive data must not fall into the wrong hands. Parties with unauthorized access to the data are seen as the wrong hands. Any loss of control over the data is assumed to be a confidentiality breach. Confidentiality is different from privacy. Confidentiality concerns agreements about how to handle the data. Privacy is more about the human side because it is their desire to limit access to themselves in ways that may or may not involve information. Confidentiality applies to data because the data needs to be handled in a confidential way so that it does not distribute to other parties (Ethicist, 2015).

Integrity

Integrity is about ensuing the completeness, accuracy and validity of information (Da Veiga & Martins, 2015). Integrity data breaches are often caused by retrofitting incomplete or improperly configured technical solutions, misappropriating intellectual property and media breaches, unintentional insertion of computer viruses, or extortion to release transfer information or technology assets (Khan et al., 2021). Data integrity ensures that data is not corrupted or modified in an unauthorized manner, either intentionally or unintentionally (Duggineni, 2023). Data integrity is important in the context of data storage, data flow and data management. Data integrity is essential for reliable and effective operation of systems and business critical possesses that rely on data.

Availability

Availability is about ensuring that information could be accessed at all times (Da Veiga & Martins, 2015). Furthermore, availability is an attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction (Whitman & Mattord, 2021). There are multiple problems that impact the availability aspect. One of these problems is the denial of service. It is one of the most common forms of attack, typically the result of the network being flooded with unwanted data to prevent legitimate users from accessing the site or services (Khan et al., 2021). Another way of an availability breach is stolen data, and this includes theft of intellectual property, customer data, patient information, employee data, and any non-public sensitive data. An availability breach might be the most annoying breach as it makes sure that persons allowed to work with data cannot work with it for a duration of time.

Trust

Defining trust is difficult because trust is seen as a value between two or more individuals that they can operate in their tasks without betraying one or another. However, there are two definitions that have consistently emerged from recent literature. The first well-known definition of trust is: “intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another” (Rousseau et al., 1998, p. 395). Another definition of trust is: “the extent to which a person is confident in, and willing to act on the basic of, the words, actions and decisions of another” (McAllister 1995, p. 25). Trust is especially important when it comes down to the attitude of a person. The attitude of a person consists of three components, cognitive, affective and conative. The cognitive component describes the beliefs and expectations, the affective component is about emotional and feelings, and the cognitive component is about the actual behaviour of an individual. Trust is a mutual relationship; it is therefore very fragile because one party does not know to what extent they can trust the other party. The behaviour of another influences the decisions and reactions of the other. Therefore, it is an ongoing process (Lewicki & Brinsfield, 2017).

Service Quality

Service quality is interpreted as the overall impression of a customer’s judgment concerning service provided (Culiberg & Rojšek, 2010). Service quality consists out of expected service and the perceived service. The expected service entails the expectation an individual has when it comes down to the service. The expected service is logically before the actual service when put in chronological order. When the service is actually executed the perceived service comes up. If the perceived service is at the same level with the expected service, then the service is satisfactory. However, the perceived service can also be better than expected or the other way around that it is below the expected service. This means that the quality of service is dependent on whether the desires and needs are fulfilled or not. There is a coherence with customer satisfaction because when the quality of the service is sufficient, the customer is satisfied. The strategic importance of quality is often underestimate, continuously upgrading quality is not costly in the long term; rather, it is an investment that will generate even greater profits (Hussain et al., 2015).

Failure Attribution

The goal of entrepreneurs is obviously to make great amounts of money and to cover the needs and wants of everybody. However, this is far more easily said than done. Every customer is different and therefore numerous variables are involved. This means that it is impossible to satisfy everybody in a way that there are no complaints whatsoever. Thriving in the entrepreneurial world cost a lot of time and money. Furthermore, making mistakes is human thus there are also entrepreneurial mistakes. When these mistakes or failures occur, it is up to the entrepreneur and firm how to deal with this. The best way to deal with this is attribution during failure. Mostly, the entrepreneurs can rebound from this failure to do better next time. This is also better for the customers because customers rather do business with a company that admits their failures instead of pretending that nothing is wrong about the failure that occurred. Failure is also not wrong as long as the firm extracts learnings out of it which are applicable to do better the next time. What does not shut the company down makes it only stronger and it gives the company incentives to do better next time to interact with customers. Failure attribution is a difficult construct, but it comes down to admitting the mistakes which have been made and come back stronger. Doing this means also that customers do have a better feeling when thinking about the firm (Yamakawa et al., 2015).

Customer Satisfaction

Customer satisfaction is one of the best-studied areas in marketing, because it has become a principal factor in achieving organizational goals and is considered a baseline standard of performance and a possible standard of excellence for any organization (Munusamy and Chelliah, 2011). An often-heard slogan in The Netherlands is “customer is king” which only enforces the thought that customers are important for organizations. Ideally, an organization or brand gets in a sort of relationship with its customers. The target is to initiate brand loyalty by its customers so that no matter what, the customers choose for their favourite brand at any time. For an organization it is important to retain their customers so that they have a constant flow of revenue. In order to keep it like that they have to invest in customer satisfaction (Hill & Alexander, 2017). The importance of customer satisfaction goes hand in hand with word-of-mouth. For example, when the customer is very satisfied they praise the organization, and this hopefully means that the organization gets more customers. Word-of-mouth in a negative way can harm the organization because people talk negatively about the organization in their local surroundings. This means lower profits because more and more people rely on the word of another. This may also result in reputational losses (Hussain et al., 2015).

Severity of Service Failure

Failure severity refers to the magnitude or intensity of the service failure. Customers who experience severe failure are likely to perceive greater loss, evaluate the service unfavourably and report dissatisfaction (Sengupta et al., 2015). The severity of a service failure is based on perception because one individual might find something very severe, but another individual can have a different opinion about it. Severity of service failure goes together with human reactions. When the perception of a failure is severe, human often cope with this in an emotional venting way. On the contrary, when experiencing a less severe failure, the customer might neglect the negative feelings. In such situations customers are less likely to blame the service provider and try to remove themselves from the stressful situation (Gelbrich, 2010).

Frustration

"Frustration is a key negative emotion that roots in disappointment (Latin frustrā or "in vain") and can be defined as irritable distress after a wish collided with an unyielding reality (Jeronimus & Laceulle, 2017). Genetically, frustration is embedded in every person to a certain extent. The difference is that some people can control it better than others. People that go from zero to one hundred in a split second do have a short fuse because they have temper tantrums out of nothing. When something needs to happen, but it does not go the way it is supposed to go, frustration arises. It is important to know how to deal with frustration because yelling or whatsoever is never the solution. Previous research taught that there is a difference in the level of frustration between male and female. Male infants are typically less able to regulate their frustration reactivity physiologically via behaviours (Jeronimus & Laceulle, 2017). Generally speaking, humans have their own way of how to deal with frustration. For one it can be helpful to immediately burst and let the frustration go. Other humans can have the mindset to hold their thoughts for themselves. Eventually this will be impossible, and they have to express themselves. Couple of decades ago, people where frustrated at themselves or other individuals. With the presence of the internet, humans have an additional factor that can frustrate them. It is also interesting to compare the roll of emotion in customer satisfaction and in severity of service failure. The company tries to satisfy their customers, they can succeed in this when their products or services align with the wants and needs of the customer. The paper of Leninkumar (2017) state that being satisfied after the purchase process is an indication of being pleased with a product or a service. The overall satisfaction with the buying experience is proposed to have a positive impact on the trust a customer has in the company. The study by Dabholkar and Sheng (2012) found that satisfaction correlates in a positive way with trust. This means that when the customer is satisfied, they develop trust and get more comfortable with the company. This is positive for the relationship between the company and customer. This is a different story for severity service failure. Frustration is a negative emotion, and it might only get worse when the service failure is even more severe (Sengupta et al., 2015). Customers show aversion towards continuing relationship and indulge in negative word-of-mouth towards the service provider. Customers may deliberately take efforts to reduce the greater perceived loss and negative emotions.

Anger

Frustration and anger are very much related to each other. It starts with being frustrated and then anger is a way to let go of things. Anger is the effect of being frustrated because frustration is often inside of the human body and when being anger the person express themselves. Anger is typically seen as a negative emotion. It is elicited by situations that are seen as undesirable, it feels bad (i.e., it has a negative valence), it motivates goals of getting back at others, and leads to behaviours that are generally disadvantageous to others, such as complaining, exclusion, and overt aggression and punishment (Nelissen & Zeelenberg, 2009). Anger itself is neither positive nor negative, only its consequences can be classified as such. For many people, anger is an outlet to let go of negative feelings or things that they do not agree with. Anger is embedded in the human beings but more important is anger management. Anger management is about whether or not it is good to let go of things. Sometimes it is better to suppress because the negative consequences might not be worth it (Van Doorn et al., 2014). Severe failures evoke anger which intensifies expressive tendencies and retaliatory behaviours (Bonifield & Cole, 2007). In order to manage high severe service failures, the customers will use action coping, emotional venting and instrumental support (Sengupta et al., 2015). Furthermore, anger is often the result of being dissatisfied. Customers may experience both anger and dissatisfaction in response to waiting for service, dealing with unresponsive or impolite employees, and core service failures such as billing errors (Bougie & Pieters, 2003). Anger and dissatisfaction correlate with each other as being dissatisfied can make a customer angry. Anger and dissatisfaction are distinctive emotions because they affect the behaviour of customers. Eventually resulting in negative word-of-mouth or migrating towards competitors.

The reason to include all these concepts and terms in the theoretical background section is because they are all related with each other. At the start of this section, several examples have been given in order to give more context about online service failures and how each failure can influence a company. Next to that, literature about the components of the CIA Triad is presented. The literature about these components provides theory that a data breach can be allocated to one of these three. This depends on the effect the data breach has on the company. Having made that clear, multiple customer related responses have been presented related to information security threats. The overarching word for the customer responses is named customer perception in this study. Next to the perception, the emotional responses are also interesting to measure and that is why the terms frustration and anger have been included in this study. These terms help to picture what an online service failures entails and provide information about possible reactions a customer might have and what the impact is on a company. It is relevant to study them together as these terms are interrelated in this study. The following paragraph is about service recovery. Service recovery is a huge part in this study as it is important for companies to know how they can recover from a breach without harming their customers.

Service Recovery

When a data breach has occurred, data breach recovery is a reactive technique which is utilised in order to manage the impact of the data breach. Khan et al (2021) identified six actions of the data breach recovery category. The first one is cybersecurity insurance which basically means that an enterprise is secured against any cybersecurity risk. It is up to the enterprise to configure the cybersecurity insurance as it is an aspect with many variables involved. The goal from cybersecurity insurance is to eventually help enterprises to recover from their losses. Secondly, a so called Computer Security and Incident Response Team (CSIRT). This is a team that provides service and support regarding a computer security incident. The CSIRT is especially helpful to prevent, detect and respond to the incidents. Another action is a root cause analysis. The word “root” reveals it already, but this analysis describes everything from the start of the process in order to locate evidence of misuse. Furthermore, the classical one is lessons learned. This one is self-explanatory as the enterprise learns by trial and error. Once a lesson is learned from a previous data breach the enterprise can use their newly gained knowledge to prevent things from happening in the future. The fifth action is resolution before resuming operations. The idea of this action is to find a solution or workaround when a data breach occurs. The target here is to contain the threat so that it does not do more damage. Lastly, response strategies are actions that organizations can take. Response strategies do influence the internal and external environment of an organization. Good communication is a requirement because a data breach can have a huge impact on an organization. This means that people related to the organization have the right to know about it. Response strategies are being deployed in order to try to reduce the impact of a data breach and to make an apology to those affected (Khan et al., 2021).

1.4. Academic and Practical Relevance

1.4.1. Academic Relevance

By conducting this research, the information which will be obtained is an addition to the existing literature with logics and facts. Several cybersecurity incidents have happened in the past and there has been some research conducted about this topic. However, the link with the change in customer’s perceptions has not been made often. It is of great importance to conduct research because humanity is more and more relying on data. As is said before, data is very valuable so the backlash of a negative way of dealing with this data might be catastrophic for smart service companies. It also depends on the type of data which has been leaked from the members. This is because of the fact that humans are very confidential with their information and the same is expected from the company involved with it.

Thus, this research provides insights in the risks of an online service failure and what it means for the customer’s perceptions. It lies in line with the previous named research in the theory part. Internet is here to stay, and it is only a matter of time when the following data breach occurs. This study contributes to the literature about the dangers of poor data security management and the consequence of it.

1.4.2. Practical Relevance

By conducting this research, smart service companies get to know the damage which can be done when having to deal with an online service failure. It might seem innocent at first, but the perception of their members can change drastically. The customers trust the company that it will work with their data in a trustworthy manner. Companies must also be resistant when an online service failure occurs because this sometimes happens. This might happen in several forms such as data breaches or hacker attacks but at the end of the day, they should be aware of the fact that they may be targeted as well. It is very harmful for the companies when data of their members leak because often it is about confidential information. When this happens, the members can get upset because their data is up for grabs as the company did not protect it at all costs. These online service failures are often big news so it will most definitely show up in any news announcement so that the world gets aware of it. At the end of the day, this research should be an eyeopener for service providers that data protection is a must in nowadays world. It should give them something to work with and what is applicable for the service providers to make sure they benefit from the research that has been done.

Eventually this research might be beneficial for both stakeholders. As is already touched on, in the first place it provides service providers with information and make them aware of the risks of data. On the other side, the customers are also stakeholders. When they make use of the service from a certain company, they ideally hold on to that company. But when something like a data breach occurs, the customers will think twice before using such services again. Thus, customers also benefit from this research because preventing a data breach from happening is always better than solving it. So, when a service provider is trustworthy, the customers will make use of a provider because due to conveniency they will stay with what is best for them.

1.5. Outline

This paper has two different methodological approaches. It contains a systematic literature review and a survey study. It starts with an introduction, whereafter the literature review follows including the most important constructs for this research. These constructs are related to the themes customer's perceptions and emotional response and are presented in-depth. The literature review is accompanied with some hypotheses as the literature makes it possible to develop hypotheses. The next chapter contains information about the data collection of the empirical method. The analysis of the gathered data can be seen in the results part. To finalise this paper, conclusions along with limitations and further recommendations are being presented.

2. Literature Review and Hypotheses Development

The literature review summarises relevant research themes and constructs relating to confidentiality, integrity and availability. Next to that, this section contains hypotheses development as it is possible to develop hypotheses based on the retrieved theories.

2.1. Materials and Methods

To be able to conduct a literature review, there has to be a search based on scientific articles, journals and books in order to answer the research question. Due to the fact that all documents were found on the internet, this means that this literature review has been conducted by only making use of desk research. A predetermined path is needed to conduct a literature review because all criteria need to be clear before even conducting the review. Multiple databases and literature are used for the search, and it is reproducible for other researchers. The review indicates the type of information which is used in order to provide a critical perspective. Part of the review is to include terms that have been used in order to search, the strategy for this and the limits. A constant need of literature was needed in order to conduct this research. The kind of literature are articles, reports, books and other scholarly documents. The goal of this study was to find valuable insights about security threats and confidentiality, integrity and availability. Furthermore, additional research has been done about the customer's perceptions. The Scopus-database has been used to retrieve relevant literature for this review. Scopus made sure that the articles are retrieved based on a combination of the keywords. Other databases that have been used are Google Scholar and Nexis Uni (previously Lexis Nexis). Nexis Uni is accessible via the databases provided by the university. Both of these databases were helpful to search for additional documents. During the literature review, only documents from 2014-2023 have been used. This timeframe is based on the information available. The reason for using this timeframe is also to use the most recent literature available. Scopus, Google Scholar and Nexis Uni, provide possibilities to adjust a custom range for the timeframe. The selected language for the papers is English, this means automatically that non-English papers are excluded during the selection process. Another criterium is that the articles need to be academic. When selecting this criterium, non-academic articles will be excluded. The reason for this is that the literature needs to be of quality and reliability. The way to obtain this goal is to only make use of academic books, journals and other documents. The keywords that are used in order to get the required papers are visible in Table 1.

Table 1. Keywords for the Literature Review.

Search Words	Hits	Papers Selected Based on Abstract	Additional Related Papers Selected Based on Abstract	Papers Excluded after Reading the Full Text	Total Chosen Papers
"Hacker Attacks" OR "Data Breaches" OR "Service Interruptions"	26	12	6	9	9
Confidentiality* OR Integrity* OR Availability*	33	10	2	4	8
	43	14	/	6	8

When conducting the search in Scopus, an informative diagram can be created. This diagram can display what has been done throughout the search. An overview of this diagram has been listed in Figure 1.

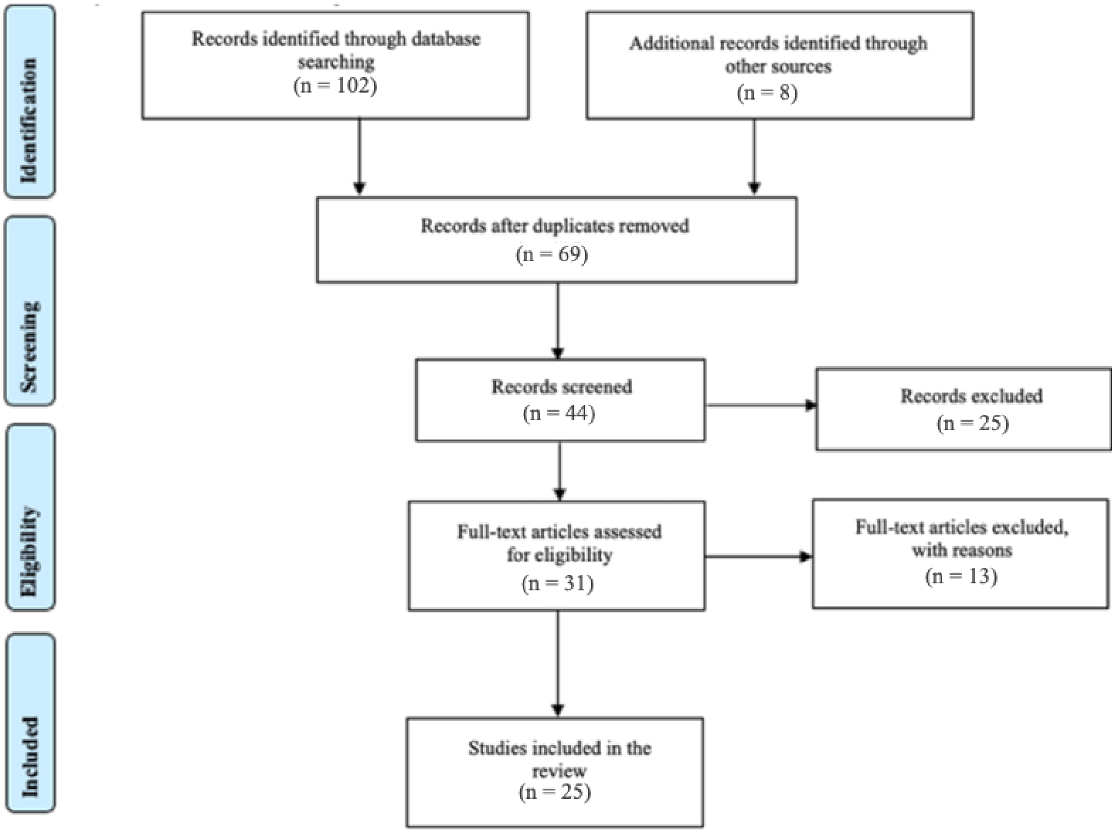
Identification
Screening
Eligibility
Included
Records identified through database searching (n = 102)
Additional records identified through other sources (n = 8)
Records after duplicates removed (n = 69)
Records screened (n = 44)
Records excluded (n = 25)
Full-text articles assessed for eligibility (n = 31)
Full-text articles excluded, with reasons (n = 13)
Studies included in the review (n = 25)

Figure 1 – Informative diagram

2.2. Results

In this section, the results are being displayed. This is done on the basis of a descriptive overview which serves as a way to summarize the main findings and ensures a development of hypotheses. On the other hand, a thematic overview gives room to interpretate the findings and discuss whether findings were similar or different.

2.2.1. Conceptual Framework

The conceptual framework provides an overview of all the constructs that are used in this research. The constructs are derived from existing literature. Together, the constructs form a framework, and the framework has been made in a way to connect the constructs with each other. The framework is also helpful later on in this chapter by creating hypotheses about the potential relationships.

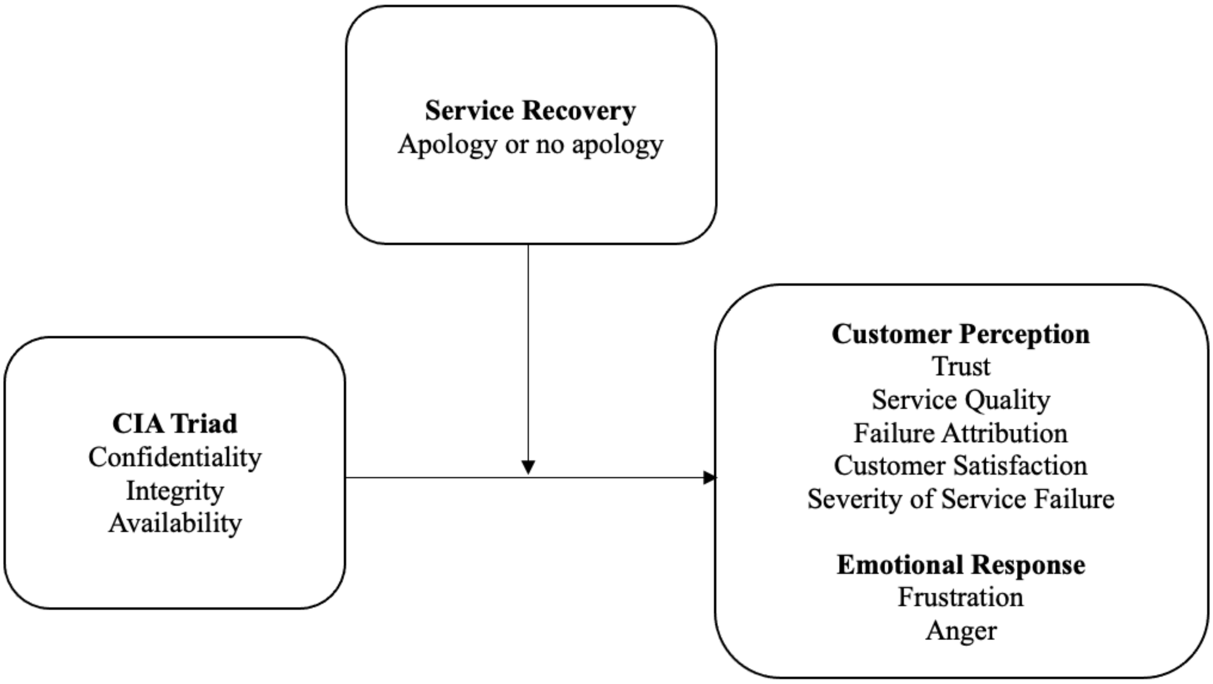

Figure 2 – Conceptual Framework

2.2.2. Main Findings and Hypotheses Development

The papers have been selected with the constructs in mind. Due to the fact that the search engine automatically matches the relevant words, these constructs are often combined in the selected papers. As is stated before, the timeframe which has been used is 2014-2023. The reason for this timeframe is that recent information about the constructs is more valuable than information from decades ago.

As data becomes more and more important for smart service companies, so does the security of all these data. Information security threats are all around the smart service companies and therefore they have to invest in security to make sure that they are as good protected as they can be. If not, these companies are vulnerable for data breaches which can occur by for example hacker attacks or service interruptions. As previously has been stated, there are three types of data breaches. These types are confidentiality breaches, integrity breaches and availability breaches.

2.2.2.1. Creating Hypothesis about Trust

It is interesting to search for the impact of these data breaches and how to be able to recover from it. As is stated by Richards & Hartzog (2017) it can be easy to get depressed about the state of privacy these days. Humans are surrounded by networked digital information and the result of this is that many people feel disempowered by the various governments, companies and criminals which are trying to collect the digital data trails. The downside of the digital revolution is that new problems regarding information security arise. One of these is whether the customers trust the smart service companies how they deal with the customer's data. In the context of privacy, trust allows to develop long-term, sustainable information relationships by sharing meaningful but often sensitive information and having sincere exchanges with the confidence that what customers share will be used for their benefit and not come back to haunt or harm them (Hardin, 2002). Due to the fact that Netflix is a streaming service it can be seen as active in the field of e-business. Trust is a primary factor in the process of e-business. Trust relates to the correlation between seller and buyer and even third parties. The market where Netflix in operates is a business to consumer (B2C) market. Thus, Netflix is the seller because they provide the customers with movies and series. In the field of e-business, the service provider needs to have personal information of their customers in order to maintain business. In this case, the customer needs to trust the service provider that they will manage the data in a responsible manner without harming the customer (Marianus & Ali, 2021). The studied papers about trust learnt that trust is a primary factor. It might decrease after a company is not careful enough with the data of their customers. To assess the effect of trust in a service provider after a data breach announcement, the following hypothesis is proposed.

Hypothesis 1: There exist a significant, negative relationship between data breach announcements and trust.

2.2.2.2. Creating Hypothesis about the Severity of Service Failure

With firms expanding their efforts to collect and use customer data, customers grow more concerned about their privacy and the potential harm. Martin et al (2017) proposes to use the construct of customer data vulnerability to assess the concerns about customer privacy. Vulnerability implies susceptibility to injury or harm (Smith and Cooper-Martin, 1997). Due to the potential for harm, the feeling of vulnerability increases when a company collects, stores and uses customer's personal information. According to Scharf (2007), most negative customer effects resulting from data use thus stem from customer's anxiety about the potential for damage or feelings of violation, rather than actual data misuse or financial or reputational harm. Customer data vulnerability can be divided into four gradations. These are in increasing order: data access vulnerability, spill over vulnerability, data breach vulnerability and data manifest vulnerability. Vulnerability is always present when customers rely on the companies to handle their data in a responsible manner. Therefore, the customers expect that those companies invest in information security to prevent it from a data breach or hacker attack (Martin et al, 2017).

Privacy concerns are always around the corner when personal data gets distributed to other parties because in doing so it is out of the customers' control. This means that there is always a risk to it when the other parties have access to customer data. Havlena and DeSarbo (1991) call this perceived risk as it is regarded as the uncertainty resulting from the potential for a negative outcome. In total, four types of risk can be distinguished. These types are *monetary, psychological, physical,* and *social* because these reflect the most common concerns for customers. Milne et al (2016) gave the following definitions to the four types of risk: (1) monetary risk is the risk associated with potential financial loss, (2) psychological risk is the risk associated with potential negative emotions such as anxiety, distress, and/or conflicts with self-image, (3) physical risk is the risk associated with bodily injury, and (4) social risk is the risk associated with threats to an individual's self-esteem, reputation, and/or the perceptions of others (Milne et al., 2016). The literature gave meaningful insights as the severity of service failure depends on what is stated in the data breach announcement. The study of Milne et al (2016) showed that there are multiple risks. Each of these risks can be perceived at a different severity level. It can therefore be postulated that:

Hypothesis 2: There exist a significant, negative relationship between data breach announcements and severity of service failure.

2.2.2.3. Creating Hypothesis about Quality of Service

Because of the fact that Netflix's customers can watch what they want based on a subscription, Netflix needs to have their account numbers to be able to monthly withdraw money from their accounts. These account numbers are private thus when it leaks it results in a monetary risk as there is a potential financial loss. Psychological risks may arise when private information leaks that can harm an individual. The threat of unwanted exposure can make someone uncomfortable. Especially when this causes for example virtual harassment. Physical risk can arise when a third party uncovers an individual's name and home address via the internet. When this person does not have the right intentions it may result in physical stalking which is anxious for the person being stalked. As this may sound over the top, a leakage of private information can still cause this. It is a reaction from a third party on the leaked information by a company. Lastly, social risk can be seen as damaging the reputation of an individual. This might occur during identity theft by a third party.

In general, Netflix is globally doing an amazing job. They have a lot of subscribers all around the world because their offers are in several languages and based on several cultures and age groups. This means that Netflix is attractive for all kinds of humans, and this is a strength of Netflix. Based on this the customers are satisfied with the quality of service from Netflix. However, cybersecurity breaches adversely affect business performance and thus quality of service (Corallo et al., 2020). Service is a broad construct as it entails a lot. It obviously is about bringing the joy towards their customers as that is the primary service from Netflix. But behind the scenes, service is also about managing customer data in a responsible manner. When a confidentiality breach occurs and it appears that the data storage was not secure, the service aspect goes down drastically. The digital era is the reason for the importance of service and that it is so thought of. Service is about value creation and that is why service-dominant logic is also emerging (Barrett et al., 2015). The results of Corallo's study supported the fact that a cybersecurity breach affect business performance. It can therefore be postulated that:

Hypothesis 3: There exist a significant, negative relationship between data breach announcements and quality of service.

2.2.2.4. Creating Hypothesis about Failure Attribution

According to Rid & Buchanan (2015), it is important for a company to engage in failure attribution after a data breach occurred. Rid & Buchanan (2015) state that communication is key in failure attribution as it is about asking the right questions to get familiar with the situation and size. Failure attribution is an art as there is no routine for it how to deal with it. Each breach is different and thus the situation that needs to be solved. The organizational culture is very important as the skills and tools are a part of it. Approaching the customer in the right way to make them feel comfortable and assured that the problem will be solved by the company is a solid start. The process of attribution requires careful management, training and leadership. Failure attribution is changing in a contradictory fashion. On one hand, it is getting easier because companies are harvesting more knowledge about it and may react to a breach in an earlier stage. On the other hand, attribution is also getting harder because attackers learn from publicised mistakes. The evolvement of the internet makes sure that failure attribution also needs evolving (Rid & Buchanan, 2015). Therefore, the following hypothesis about failure attribution is proposed.

Hypothesis 4: There exist a significant, negative relationship between data breach announcements and failure attribution.

2.2.2.5. Creating Hypothesis about Customer Satisfaction

Big data analytics can integrate data from multiple communication channels (e.g., phone, email, instant message) and assist customer service personnel in understanding the context of customer problems holistically and addressing problems quickly. Lots of companies use big data to improve customer satisfaction. Beneficial about this is that companies are able to provide the customers in a way that addresses there wants and needs in the best way. This gives a level of satisfaction to the customers and is good to retain customers. The downside is that a massive amount of data is a necessity to be able to engage in big data analytics. Once the data management is not up to date, the data of all these customers might leak and customer satisfaction will decrease. Another possibility is that a customer is already dissatisfied. Due to the internet, customer dissatisfaction can spread rapidly and contribute negatively to a companies' reputation, through the use of social media (Shiue & Li, 2013). Therefore, it is recommended by a lot of experts to keep engaging in information security in order to take on future challenges (Lee, 2017). As a data breach might harm the customers, it also possibly affects their satisfaction. It can therefore be postulated that:

Hypothesis 5: There exist a significant, negative relationship between data breach announcements and customer satisfaction.

2.2.2.6. Creating Hypotheses about Emotional Response

The reaction of a customer towards a cybersecurity incident is often an emotional response as the cause of a breach has consequences for both the company and their customers. In this section, frustration and anger are reviewed. Customers especially get frustrated when availability breaches occur because the effect of this breach is that systems are temporarily being knocked down so that the customer does not have access. More and more hacker attacks aim to frustrate customers that could ultimately cause a financial loss to the company (Tariq, 2018). Frustration is also a natural response when something does not go the way that had been kept in mind. Data breaches are out of the customers control thus this brings also frustration with it because the customers cannot solve it by themselves. The study of Tariq (2018) state that hacker attacks aim to frustrate customers. Thus, when hacking a company, that company has eventually the duty to announce what has happened. This ensures that customers are even more frustrated when taking note of the data breach. Therefore, the following hypothesis about frustration is proposed.

Hypothesis 6: There exist a significant, positive relationship between data breach announcements and frustration.

Eventually, frustration can get accompanied by anger. When humans are angry they can get impulsive and say or write things that can get interpreted in a wrong or heavier loaded way. Being angry is an expressive way in order to let others know that an individual is dissatisfied with whatever has happened. When an individual is angry at a company this may result in negative word-of-mouth. Negative word-of-mouth communication can adversely affect the attitudes and purchasing intentions of customers and a firm's brand image. The power of the worldwide web is extreme when a group of angry customers bundle their strengths. They can go viral and cause a public relations crisis for a firm (Balaji et al., 2016). Hence, the following hypothesis is proposed.

Hypothesis 7: There exist a significant, positive relationship between data breach announcements and anger.

2.2.2.7. Creating Hypothesis about Service Recovery

In order to manage data breaches and as a result unhappy customers, companies can engage in data breach recovery action. Apologising for example, may be a good recovery action depending on the severity of the data breach. When making an apology, the company creates goodwill as they show their willingness to make amends. This might trigger the customers to adjust their opinion about the company and retain as a customer. Possibly a more effective and meaningful recovery action might be user compensation as the firm insists to compensate whatever damage the customers have suffered. Previous research has shown that compensation as a service failure recovery strategy has a positive effect (Goode et al., 2017). According to Gelbrich (2010) there is less clarity on how to best match customers' expectations and compensation levels. Customers' expectations of compensation vary depending on the service failure severity and the context in which the service failure occurs. There are several variables that need to be considered in order to come up with a suitable compensation. Arguably, the best way to compensate is full compensation in order to restore perceptions of the service to the original level that existed prior to the service failure. It is definitely a large expense to cover full compensation and it might look like bribing the customer in order to get positive feedback and positive word-of-mouth (Goode et al., 2017). The study of Goode (2017) supports the use of a service failure recovery strategy in order to restore the relationship between company and customer. It can therefore be postulated that:

Hypothesis 8: Service recovery has a moderating effect on the relationship between data breach announcements and customer's perceptions.

2.2.3. Interpreting the Main Findings

It is also important to interpret the findings from the previous section. A lot of research has been conducted about the constructs, but the essence is on how it all fits together and whether the constructs enhance each other.

As has been discussed previously, data becomes more and more important in order to operate in a business. Data is extremely valuable as a lot of things can be steered with the help of data in order to achieve competitive advantage. The downside of data is that it is also vulnerable because personal information may harm an individual. To be able to personalize an offer, companies need to have the data from their customers. However, a data leakage can happen in a split second, and this impacts the customers. Therefore, it is interesting to look at the willingness to provide information. Phelps et al., (2000) suggest five broad categories, namely, demographic characteristics, lifestyle characteristics, purchasing habits, financial data, and personal identifiers, finding that consumers are most willing to provide demographic and lifestyle information and reluctant to provide financial or user identification information. This outcome is not surprising as financial and identification information can be more harmful for an individual than the other three can be. This is because demographic characteristics, lifestyle characteristics and purchasing habits might be interesting for big data analytics. With the help of these analytics, it is easier to engage in customer mapping and make personal tailored offers (Kim & Kim, 2018).

When talking about willingness to provide information, it might be in conflict with the privacy paradox. People often talk about how important their privacy is and it is their primary concern for citizens in the digital age. On the other hand, individuals provide information when there is an incentive for them. They sometimes provide their information quite easily for a relatively small reward. This is naïve behaviour as the things which are being stated on the internet do have a longevity. This inconsistency of privacy attitudes and privacy behaviour is often referred to as the privacy paradox (Kokolakis, 2017). This also includes that when customers are willing to have a personal offer from a company they are doing business with, they need to provide the company with valuable personal information. It is in their interest to provide personal information in order to get the best suitable offer. This means that customers are focused on getting the best offer to provide in their wants and needs. This is their privacy behaviour because they provide information for their sake and without second thoughts. However, as for whatever reason the information may harm them. Their privacy attitude is completely different than their privacy behaviour in the first place. It is up for debate, but it seems that there needs to happen something in a negative way which has an impact on the data to make customers aware what the downside of a data breach can be. When this has happened once to them, their behaviour is more responsible, and they think twice when providing information (Kokolakis, 2017).

Central in this research are the constructs confidentiality, integrity and availability. These constructs are derived from information security as humans have entered the digital age in the last decades. This implies that humans became vulnerable on a whole new level as they have a virtual life next to their social life. These three constructs make it possible to divide information security in three different dimensions. Although they are very much connected to each other, they stand for something different. This means that an information security system needs to be advanced enough to minimize a confidentiality, integrity or availability breach. Obviously, this has an impact on customers and the customer’s perceptions might change and it results in an emotional response. Emotional responses are depending on the severity of the service failure. The customer’s perceptions are expected to change because a data breach is harmful for them. This will be tested by study two with the help of a survey.

2.3. Discussion

The literature review yielded a sufficient amount of literature and theories about the different constructs. Hacker attacks, data breaches and service interruptions are increasing as the services via the internet are increasing as well. This means that there is a constant need of awareness on how to deal with data in a responsible manner. The chosen constructs for the themes customer’s perceptions and emotional response gave clear insights in the relationship between the provider and its member. This means that trust is a necessity in order to do business with each other and thrive from it. Without trust, it is hard to connect with each other as there are second thoughts all the time, especially from the side of the user because the user is more vulnerable. The quality of service can also differ when companies do not succeed in a solid way of data management. When talking about data, it is the data of the members and thus the members can be harmed when there is a lack of sufficient data management. The consequences of a service failure are depending on the severity of the failure. When it is somehow within constraints, it can be that the company retains the customer. If not, the customers will look for competitors as they do not want to continue with the breached service provider. The emotional responses that can come up are different for each human being as their temper is different from each other. However, if there are emotional responses on the rise it can result in negative word-of-mouth which might be harmful for the company. Next to that, a small aspect of service recovery action has been analysed. The theory learned that companies who actively engage in service recovery action are more likely to retain some of its customers.

3. Methodology

3.1. Research Design

Several sources such as NASDAQ and PR Newswire release announcements about huge service providers and these announcements are about cybersecurity incidents, such as data breaches, service interruptions or hacker attacks. The university provides students with access to databases and one of these databases is NexisUni (previously LexisNexis). With the help of NexisUni, it is possible to do an advanced search. An advanced search is a method which makes it possible to include important keywords in order to find the right articles. The released announcements about service providers with regard to cybersecurity incidents are helpful in order to be able to manipulate an announcement.

The independent variables within this research are the components of the CIA Triad, confidentiality, integrity and availability. When a data breach occurs, it can be allocated to one of these three components. The dependent variables are customer perception and emotional response. The operationalization table is shown in Table 3, and it contains the constructs and their measurement items. It also includes the sources from where the measurement items have been derived. The idea behind this research is to find out how the customer's perceptions change when an online service failure occurs. The research method is a survey as this is a helpful method where customer reactions to different data breaches can be measured. It is interesting to compare different types of data breaches (CIA) and their impact on the customer's perceptions. To be able to successfully conduct a survey, chapter eleven of the book from Saunders et al (2019) will be useful and therefore read.

The components of the CIA Triad are the independent variables because these variables will be shown in the survey as a short story. This short story is a manipulated announcement as it is based on a real announcement derived from PR Newswire. The difference is that the data breach in the announcement has been made up in order to be best suitable for the research. There will be an announcement for confidentiality, integrity and availability. The dependent variable customer perception will be measured with the help of seven predetermined conditions. The first five conditions are about the service provided by the service provider. Furthermore, the conditions frustration and anger are emotional responses. This is because when the service from the service provider does not full fill the demands of the customers, the customers might react in an emotional way. The third variable, service recovery can be seen as a 'moderator' variable. This variable makes sure that there are in the end six different manipulated announcements. As is said before, there will be announcements for confidentiality, integrity and availability. These three announcements will contain an apology. But there are also three announcements which will not contain an apology. Table 2 provides an overview of the number of manipulated announcements.

Table 2. Overview of the number of manipulated announcements

	Apology	No Apology
Confidentiality	1	2
Integrity	3	4
Availability	5	6

Table 2 provides an overview as it visualizes the CIA Triad with and without service recovery in the form of an apology. The reason for this, is that it is interesting to measure whether service recovery action has an impact or not. The three announcements without the service recovery as an aspect can be seen as a control variable as this gives the opportunity to solely measure the possible impact of an apology given or not. As has been discussed in the literature review, there are more data breach recovery action strategies. However, it has been decided to only test apology as otherwise the size and number of the manipulated announcements are disproportionate and not feasible anymore.

The survey has been created with the help of Qualtrics which is also available through university. The survey starts with a welcome screen where an informed consent is included. After that, the questions start about demographics as it is important to get to know the respondent to a certain extent. The core from the survey starts after the demographics and has been divided into six blocks where every block is one manipulated announcement. Every respondent answers the questions for only one manipulated announcement. This has been done because otherwise the survey is way too long and takes a lot of time. With the help of randomization, each respondent gets a random block allocated to answer the questions about that specific announcement. Qualtrics is advanced in a way that it allocates the blocks to the customers in an equal way. This means that every block has the same amount of response in the end. This is necessary as it is otherwise hard to compare the several manipulated announcements with each other. In order to keep the respondent interested, page breaks have been added. This is a method which prevents the respondent from scrolling down as this can be boring for them. This also means that every question category has their own page. When the respondents went through the survey, it closes with an end of survey message in which the researcher thanks them for participating.

3.2. Selection

The respondents targeted for this research are people who make use of Netflix's services. Since Netflix has a broad offer in its movies and shows for all ages, the respondents in this research can also be of all ages. Thus, to be eligible for participation in this research, the respondents must make use of Netflix's services and be proficient in English to a certain extent. This is because the questions in the survey are compiled in the English language. At the start of the survey, demographic questions are asked to filter the respondents. The demographic part consists out of three questions, these questions are about age, gender and whether they make use of Netflix's services. If they do not make use of Netflix's services, the respondents skip to the end of the survey as their input is not of use for this research.

3.3. Sample

In order to get a sufficient number of respondents, the survey was distributed to several possible Netflix users. In total, 193 respondents filled in the survey. Some of these respondents did fill in the survey although they do not make use of Netflix's services. This means that they do count as a respondent, but their provided information is not usable. Furthermore, there were a couple of responses in progress. By closing the survey, these responses were automatically added to the total amount of responses. These answers were also removed which resulted in 135 usable respondents which will be used for data analysis. Many statisticians concur that a sample size of 100 is the minimum for meaningful results (Delice, 2010). This is also the target set by the 1st supervisor and has been achieved.

3.4. Measurement

The questionnaire measurement items are presented below in Table 3, and these are derived from previous studies. Some of these previous studies are decades old as it is important to get to the original source in order to conduct this research with the same constructs. In total, 7 constructs were used to measure 2 variables. These variables are divided as follows: Customer Perception consists of 5 constructs (trust, service quality, severity of service failure, failure attribution, customer satisfaction), Emotional Response consists of 2 constructs (frustration, anger). Each of the constructs have a minimum of three measurement items. This has been done to define the constructs in the best way possible. A total of 22 items were measured by using a 7-point Likert scale, ranging from 1 – strongly disagree to 7 – strongly agree. Some items have been recoded to be suitable for the survey. Previous research has shown that the 7-point Likert scale is more reliable than others as the 7-point Likert scale is also more common (Bishop & Herron, 2015).

3.5. Data Collection

The collection of data is a time-consuming task. For this research, the data collection period was three weeks, from 15th of September until 6th of October. To start with the distribution of the survey, it has been sent to some acquaintances within the personal network of the researcher. This was a good start as it yielded a sufficient number of respondents and thus information. The survey has been sent as an anonymous link via email and WhatsApp as this is an option within Qualtrics. As the links were sent to a targeted sample, this can be seen as snowball sampling because ideally the reached respondents forward it within their personal network. Furthermore, the survey has been placed on several social media platforms such as LinkedIn, Instagram and Facebook. In order to get the required respondents, Reddit has also been used to distribute the survey. The platform Reddit yielded a sufficient number of respondents so that the minimum target of 100 respondents could be achieved. Due to the way the distribution of the survey on Reddit went, it is safe to say that this is a form of random sampling. In this case a simple random sample as every member of the population has an equal chance of being selected into the study (Etikan & Bala, 2017).

Table 3. Questionnaire measurement items

Variables	Constructs	Items	Sources
Customer Perception	**Trust**	1. This [company] can’t be trusted, it’s just too busy looking out for itself.	Chow & Holden (1997)
		2. I have found that I can rely on this [company] to keep the promises that it makes.	Chow & Holden (1997)
		3. This [company] is basically honest.	Chow & Holden (1997)
	Service Quality	1. You are satisfied with the products or services provided by the [website].	Wang et al., (2004)
		2. The digital products or services provided by the [website] meet your needs.	Wang et al., (2004)
		3. The [website] provides high-quality products or services.	Wang et al., (2004)
	Failure Attribution	1. I think the [company]’s service failure was avoidable	Chang et al., (2015)
		2. I think the [company]’s service failure was preventable	Chang et al., (2015)
		3. I think the [company] should be blamed for any undesirable outcomes.	Chang et al., (2015)
	Customer Satisfaction	1. The [website] provides information that exactly fits your needs.	Wang et al., (2004)
		2. The [website] provides innovative products or services.	Wang et al., (2004)
		3. The [website] responds to your requests fast enough.	Wang et al., (2004)
	Severity of Service Failure	1. This situation is unfair	Tsarenko & Tojib (2011)
		2. This problem caused a high level of inconvenience.	Tsarenko & Tojib (2011)
		3. My daily life was hampered due to failure.	Wang et al., 2011)
Emotional Response	**Frustration**	1. Trying to get this [job] done was a very frustrating experience.	Peters et al., (1980)
		2. Being frustrated comes with this [job].	Peters et al., (1980)
		3. Overall, I experienced very little frustration on this [job].	Peters et al., (1980)
	Anger	1. I felt angry.	Fuqua et al., (1991)
		2. I was furious.	Fuqua et al., (1991)
		3. I felt mad.	Fuqua et al., (1991)
		4. I was burned up.	Fuqua et al., (1991)

3.6. Data Analysis

The statistical software used for data analysis in this research is SPSS. This software lends itself to process huge amounts of data. In order to get to the actual analysis of the data, the dataset self needs to be prepared first to work with it. Excel is a helpful program to sort all the respondent data in an easy manner. Due to the fact that the experiment has been conducted with a 7-point Likert scale, it contained a lot of text. Excel made it possible to replace all these text answers with a numerical code. For example, strongly disagree gets replaced by 1. After making the dataset as concise as it can be, the dataset can easily be exported in SPSS where the actual data analysis can start.

After making the data set ready to work with, the descriptive statistics are the first statistics that will be derived from the data set. These statistics will tell something about the respondent such as gender and age. This is eventually very interesting in order to compare different gender groups or age groups with each other in the latter stages of this research. Furthermore, Exploratory Factor Analysis (EFA) will be conducted. This analysis is generally used to discover the factor structure of a measure and to examine its internal reliability. Next, linear regression will be conducted in order to test the proposed hypotheses. Linear regression is used to test coherent variables and to what extent (Weisberg, 2005).

4. Results

The results section provides the results of the data analysis. This section starts with the descriptive statistics to get some additional information about the respondents. Later on in this section, factor analysis and regression analysis will be addressed whereafter the hypotheses are examined.

4.1. Descriptive Statistics

The descriptive statistics ensure the researcher to get to know the respondents better by asking about several demographics. This makes it better understandable as it allows to divide the respondents based on age and gender. The demographic questions were at the beginning of the survey and are analysed and presented. More than half of the respondents consists of 74 males (54,81%) and 52 females (38,52%). Furthermore, 6 respondents are non-binary/third gender (4,44%) and 3 preferred not to say (2,22%). The majority of the respondents belong to the age group of 18-27 years old (40,74%). The next biggest age group and in descending order is 28-39 years old (28,15%). The age groups of 0-17 years old and 40-50 years old are equal and consists out of 15 respondents (11,11%). The smallest age group is the group of 51 years or older, this group contains out of 12 respondents (8,89%). Another demographic question was whether the respondents make use of Netflix in order to filter them. All the 135 respondents used for data analysis selected that they make use of Netflix. However, before filtering there were also some respondents that did not make use of Netflix. Instead, they make use of other streaming services such as Hulu. This is often geography related as other streaming services might be more popular.

4.2. Exploratory Factor Analysis

The extraction method selected for EFA is Principal Component Analysis. This method has been executed for each construct with Varimax as an orthogonal rotation which is used for uncorrelated factors (Jackson, 2005). When conducting EFA, an option within SPSS is to tick the box of the Kaiser-Meyer-Olkin measure of sampling adequacy. This is a measure that has been intended to measure the suitability of data for factor analysis. The KMO value varies from 0 to 1. But if the value is less than 0.5 the results of the EFA are not very suitable for analysis of the data (Shrestha, 2021). In this research, the results of the KMO measure are all exceeding the threshold of 0.5 so it is suitable for EFA. Next to the KMO test, the Bartlett's test of Sphericity is another important test in factor analysis. When the Bartlett's test of Sphericity is significant it shows that the correlation matrix has significant correlations among at least some of the variables (Shrestha, 2021). In this research, the Bartlett's test of Sphericity for each construct is significant ($P<0.001$) and this indicates that a factor analysis may be worthwhile for the data set. Furthermore, the total variance explained by the 7 factors fluctuate between 50% to 83%. According to criteria, the total variance explained by all criteria should be between 70% to 80%. However, this may be untenable for social science research where extracted factors usually explain only 50% to 60% (UCLA: Statistical Consulting Group, 2021). The reliability and internal consistency of the constructs are assessed by using another statistic, the Cronbach's Alpha. According to Taber (2018) a wide range of different qualitative descriptors was used to interpret alpha values calculated. For this research the range acceptable (0.45-0.98) has been used and all constructs comply to this thus ensure reliability. Table 4 contains an overview of the used factors with their descriptive statistics, their item's factor loadings and the Cronbach's Alpha coefficients.

Table 4. Descriptive statistics, Factor Loadings and Reliability

Factors	**Measurement items**	**Mean**	**SD**	**FL**	**α**
Trust	Trust 1	4,710	1,209	0,900	0,893
	Trust 2	4,620	1,332	0,922	
	Trust 3	4.440	1,454	0,907	
Service Quality	ServQual 1	5,040	1,321	0,952	0,901
	ServQual 2	5,040	1,360	0,933	
	ServQual 3	5,120	1,350	0,857	
Failure Attribution	FailureAtt 1	5,280	1,048	0.883	0,790
	FailureAtt 2	5,300	1,044	0,754	
	FailureAtt 3	5,170	1,150	0,885	
Customer Satisfaction	CustomerSat 1	5,070	1,582	0,890	0,608
	CustomerSat 2	5,240	1,422	0,904	
	CustomerSat 3	4,290	1,387	0,378	
Severity of Service Failure	Severity 1	4,990	1,022	0,695	0,495
	Severity 2	4,800	1,274	0,673	
	Severity 3	3,470	1,520	0,760	
Frustration	Frustration 1	4,410	1,278	0,921	0,808
	Frustration 2	4,430	1,182	0,828	
	Frustration 3	3,710	1,540	0,817	
Anger	Anger 1	4,040	1,284	0,791	0,869
	Anger 2	3,720	1,347	0,870	
	Anger 3	3,740	1,333	0,847	
	Anger 4	3,360	1,285	0,879	

Notes: SD = Standard Deviation, FL = Factor Loadings, α = Cronbach's Alpha coefficient

4.3. Regression Analysis

Regression analysis is a statistical tool for the investigation of relationships between variables (Sykes, 1993). It is a helpful tool in order to look for a causal effect of one variable on the other variable. In this research, the CIA Triad is central. Confidentiality breaches, integrity breaches and availability breaches have been presented to the respondents. Together with apology, these variables are the IV's. It is expected that these IV's have an influence on the DV's which contain out of two categories, customer perception and emotional response. Regression analysis is used to test these relationships including how strong or weak they are and whether they are significant. The questionnaire has been made with a randomizer in Qualtrics. In total, 135 responses have been yielded. Confidentiality has 47 responses; integrity has 46 responses and availability has 42 responses. These numbers are roughly equal which is necessary in order to compare them with each other. In total there are 69 responses with apology integrated in the DBA and this roughly equals half of the total valid responses which is a good number for comparison. It is interesting to measure whether the integration of apology in the DBA results in a different reaction from the customers. All regression analyses in this section contain stars to flag levels of significance. If a p-value is less than 0,05, it is flagged with one star. If a p-value is less than 0,01, it is flagged with 2 stars. If a p-value is less than 0,001, it is flagged with three stars as this statistically means highly significant. Another option is n.s. and this means that it is not statistically significant. Later on, Table 12 contains all the hypotheses and whether they are supported by the outcome of this study or not. In most sciences, results yielding a p-value of 0,05 are considered on the borderline of statistical significance. This is also the value that is used for Table 12 in order to reject or accept the hypotheses.

4.3.1. Regression for Trust

The first regression analysis has been conducted for the dependent variable trust. As has been made clear in chapter 2, trust is a primary factor in building a relationship between a company and its customers. Table 5 shows the results of the regression analysis for trust, starting with the main effects in the first column. Every coefficient value is negative, this means that when introducing a DBA, it has a negative effect on trust. As the independent variable increases, the dependent variable tends to decrease. This means that a worse DBA has an even stronger effect on the decrease in trust. This is also what was expected as a data breach normally has a negative effect on trust. The main effects of the model are the direct effects where a confidentiality breach has the worst effect on trust. Followed by availability and integrity has a smaller effect. Unfortunately, only apology is statistically significant, and the CIA is not. The indication n.s. means not significant as the p-value is greater than the usual significance level of 0,05. Apology is a little bit lower than alpha thus it receives 1 star to indicate its significance. The second column is the model with interaction to analyse the effect a service recovery strategy has. In this study, only apology has been used. Apologising in a DBA is definitely a good thing to do as it decreases the effect the DBA has on trust. The values are still negative but not as negative as the direct effect. This means that apologising softens the effect the DBA has on the customers' trust.

Table 5. Regression Analysis for Trust

	Main effects model B(SE)	**Model with Interaction**
Confidentiality	-0,320 (0,658) n.s.	
Integrity	-0,080 (0,662) n.s.	
Availability	-0,254 (0,678) n.s.	
Apology	-0,805 (0,624) *	
Confidentiality*Apology		-0,090 (0,835) n.s.
Integrity*Apology		-0,032 (0,869) *
Availability*Apology		-0,197 (0,897) *
Intercept = 14,182		
R^2	0,018	0,256

4.3.2. Regression for Quality of Service

Quality of service is also an important dependent variable as the service a company provides is often the reason to get involved. Just like with trust, Table 6 shows that all the direct effects are negative. This means that introducing a DBA for confidentiality, integrity or availability has a negative direct effect on the quality of service. This effect was also expected as the service of a company entails a lot including security. When a data breach occurred, the quality of the service decreases as the company is not as good secured as they might have thought they are. Confidentiality and availability scored one star on the significance level, meaning that it is below the predetermined p-value level. Apology also has a moderating role on the relationship between DBA and quality of service. The coefficients are still negative, but they are a lot closer to zero which indicates that there still is a negative effect but not as strong as the direct effect is.

Table 6. Regression Analysis for Quality of Service

	Main effects model B(SE)	**Model with Interaction**
Confidentiality	-0,775 (0,665) *	
Integrity	-0,117 (0,671) n.s.	
Availability	-0,943 (0,682) *	
Apology	-0,632 (0,634) n.s.	
Confidentiality*Apology		-0,635 (0,893) n.s.
Integrity*Apology		-0,067 (0,879) n.s.
Availability*Apology		-0,344 (0,908) n.s.
Intercept = 15,530		
R^2	0,034	0,296

4.3.3. Regression for Failure Attribution

Table 7 contains the results of the regression analysis for the concept of failure attribution. Failure attribution means that a company admit it when they make a fault and whether they attribute to it to solve the problems it may have caused. Also here, the direct effects are negative. Confidentiality and integrity are both in the higher regions as their coefficient is pretty close to minus 1. Remarkable, their significance level scored 2 stars which means that they both have a low p-value. When introducing apology in the DBA, the coefficient values decrease, and this is also the expectation. It seems that an apology eases the problem as it shows that the company is willing to stand up for the occurred problem. The interaction effect from integrity multiplied with apology scores 3 stars which means that it is very significant. This can be explained as integrity might be the toughest data break a company can suffer.

This is because the data might get modified, and this impedes both the company and their customers.

Table 7. Regression Analysis for Failure Attribution		
	Main effects model B(SE)	**Model with Interaction**
Confidentiality	-0,909 (0,487) **	
Integrity	-0,838 (0,491) **	
Availability	-0,084 (0,508) n.s.	
Apology	-0,582 (0,468) n.s.	
Confidentiality*Apology		-0,042 (0,646) n.s.
Integrity*Apology		-0,531 (0,636) ***
Availability*Apology		-0,013 (0,656) n.s.
Intercept = 16,045		
R^2	0,083	0,317

4.3.4. Regression for Customer Satisfaction

The direct effect a DBA has on customer satisfaction is very noticeable when it comes down to a confidentiality breach. The coefficient has a very negative value which implies that the confidentiality breach does have damage to the customer satisfaction. An availability breach also hampers the customers very heavily. This value is even higher which means that when customers can't have access to the service the dissatisfaction occurs. Confidentiality and integrity are both also significant as they score some stars at the predetermined significance level. Again, when introducing an apology, it seems that apology has a moderating role to soften the reactions customers might have in response to a DBA. The interaction effect is a multiplication of the two variables that have a joint effect on the dependent variable customer satisfaction.

Table 8. Regression Analysis for Customer Satisfaction		
	Main effects model B(SE)	**Model with Interaction**
Confidentiality	-1,324 (0,586) *	
Integrity	-0,130 (0,600) n.s.	
Availability	-1,538 (0,600) **	
Apology	-0,709 (0,566) n.s.	
Confidentiality*Apology		-1,107 (0,783) *
Integrity*Apology		-0,071 (0,771) *
Availability*Apology		-0,702 (0,796) n.s.
Intercept = 14,970		
R^2	0,086	0,344

4.3.5. Regression for Severity of Service Failure

Table 9 contains the values of regression analysis for severity of service failure after a DBA. Severity of service failure is a difficult concept as it is often related to perception. In other words, the opinion of a person might be that it is severe while another person thinks that it is not so bad. This has to do with different standards. However, the analysis shows that each of the coefficients are negative. This implies that there is a negative direct effect from a DBA on the severity of service failure. Unfortunately, none of the CIA breaches are significant. Also, with severity of service failure, introducing an apology softens the direct effect. This can be explained by the fact that an apology shows goodwill. In this case, the goodwill to solve the problem as quickly as possible. The reaction from the people is that it is less severe with an apology as the correct step in the right direction has already been made. There still is a negative effect but not so strong as before. It would be strange to have a positive effect as the expectation is that the DV changes in a negative way.

Table 9. Regression Analysis for Severity of Service Failure

	Main effects model B(SE)	**Model with Interaction**
Confidentiality	-0,364 (0,493) n.s.	
Integrity	-0,613 (0,494) n.s.	
Availability	-0,257 (0,508) n.s.	
Apology	-1,019 (0,463) **	
Confidentiality*Apology		-0,267 (0,655) n.s.
Integrity*Apology		-0,488 (0,645) *
Availability*Apology		-0,157 (0,666) n.s.
Intercept = 13,773		
R^2	0,049	0,267

4.3.6. Regression for Frustration

Frustration is a negative emotion. Therefore, it is expected that there is a positive relationship between the DBA and frustration. This means that when the independent variable increases, the dependent variable also increases. In more meaningful words, when the DBA increases, the effect it has on frustration increases to. This does not come as a surprise because it is expected that when the DBA does a lot of damage, the customers might get more frustrated. However, apology again has a moderating role. The customers are less frustrated when the company apologises in the DBA making the DBA less severe. The results of the regression analysis for frustration are shown in Table 10 below.

Table 10. Regression Analysis for Frustration

	Main effects model B(SE)	Model with Interaction
Confidentiality	-1,134 (0,612) *	
Integrity	-0,367 (0,623) n.s.	
Availability	-0,816 (0,634) n.s.	
Apology	-0,806 (0,587) n.s.	
Confidentiality*Apology		-0,585 (0,813) n.s.
Integrity*Apology		-0,223 (0,800) n.s.
Availability*Apology		-0,649 (0,826) *
Intercept = 13,545		
R^2	0,059	0,288

4.3.7. Regression for Anger

In the previous section frustration has been named a negative emotion. The same applies for anger as anger is often the result of being frustrated. Thus, it is expected that an increase in the DBA might also cause an increase in the dependent variable anger. This can also be measured with the help of introducing apology. As is shown in Appendix A, there are several announcements made and introduced in the survey. An apology eases the anger a person feels when being confronted with the DBA in comparison with the anger the customer shows when being confronted with a DBA where apology is left out.

Table 11. Regression Analysis for Anger

	Main effects model B(SE)	Model with Interaction
Confidentiality	-1,489 (0,796) *	
Integrity	-0,116 (0,811) n.s.	
Availability	-1,455 (0,820) *	
Apology	-0,750 (0,766) n.s.	
Confidentiality*Apology		-0,453 (1,073) n.s.
Integrity*Apology		-0,101 (1,056) n.s.
Availability*Apology		-1,076 (1,091) *
Intercept = 15,242		
R^2	0,040	0,258

4.3.8. General Findings

The previous subsections have been made in order to present and discuss the results for each dependent variable in a separate way. But there are also some findings the dependent variables have in common and therefore this general section has been made.

The word significance is often used in the previous section because in science it is important that the results are significant. Table 12 provides an overview of every hypothesis and whether it is significant or not. Unfortunately, not every result is significant, and it is also important to investigate why this can be. There are two possibilities for a non-significant result. It might be that there is no real effect, in that case the null hypothesis is true. The other possibility is that the study hypothesis could be true but that there is not enough evidence to support the hypothesis. That Netflix has to make a DBA is in itself already something bad as it could be an attack from the outside. Thus, the expectation is that the customers react in a negative way. The unstandardized beta (B) coefficient confirms this as they are negatively influencing the perceptions and emotional responses from the customers towards Netflix.

Furthermore, moderation is a recurring theme as it is interesting to analyse whether there is a moderating variable that has an influence on the relationship between an IV and a DV. The systematic literature yielded some theories about DBA's and one of these theories is service recovery action. The theory is that service recovery actions should temper down the reactions from the customers. In this study, the service recovery action that has been considered is apology. Expected is that an apology makes up for relatively a good amount as it is a good thing that the company makes an apology in order to restore the relationship. As has been discussed before, there is a direct effect from the IV's on the DV's. Whether there is a moderate effect means that making an apology weakens the effect the IV's have on the DV's. This can also be tested by regression analysis as the outcomes are comparable when adding an extra variable to the equation. As is shown in the subsections for each DV, apology definitely has a moderating effect on the relationship between the IV's and the DV's. Also, from a psychological point of view, apologizing is the right thing to do after an adverse event (Bismark, 2009). An apology has a meaningful purpose as it can bring comfort to the harmed customers and forgiveness to the company that harmed their customers. This might in the end be helpful to restore the relationship between buyer and seller. Of course, not every customer is satisfied with just an apology, and this is because every human being is different. But overall, it is a step in the right direction as the company is brave enough to admit their flaws. It also depends on the severity of the data breach. If the breach is severe, an apology might not be enough. In such cases, a financial compensation might be more suitable.

The previous tables also contain a column where the interaction term has been presented. The used software, SPSS makes it relatively easy to create these interactions. By using the compute function, the interaction variable can be made as it is the product of the predictors in question. By doing so, three new variables are created as confidentiality, integrity and availability are all multiplied with apology. The presence of an interaction indicates that the effect of one predictor variable on the response variable is different at different values of the other predictor variable. When adding an interaction term to a model, this drastically changes the interpretation of all the coefficients. The effect of a confidentiality breach on trust is different for different values of apology. This basically counts for every interaction term. As there are not a lot of values possible for both IV's. The data set works with zeroes and ones as these values represent whether there has been a breach that can be allocated to confidentiality, integrity or availability. Next to that, there are also zeroes and ones allocated to apology as there are only two options, there is an apology in the DBA or there is no apology in the DBA. There is an interaction effect as the value for the data breaches differ when the value of an apology differs.

The intercept has also been included in Table 5 till 11. It lies for every regression analysis more or less in the same range as all the DV's are measured on the same 7-point Likert scale. It varies from 13 to 16, this is not a strange value as every variable consists at least out of three items. The intercept is often defined as the mean of the dependent variable when all of the IV's in the model are set to zero. The intercept corresponds with the IV's in order to compute a value for the dependent variable. The intercept is a fixed value and is the first value in the equation. Another important statistical is R-squared. R-squared is used to determine the percentage of the dependent variable variation that a linear model explains. It is always a value between one and zero. The larger R-squared, the better the regression model fits the observations. However, in social science the R-squared is often low due to human behaviour as people are harder to predict. The low values for R-squared means that the model explains very little variance. This means that the dispersion in the dependent variable is only for a small part explained by the IV's. The model with interaction shows a higher R-squared because adding variables into the model increases the R-squared.

Table 12. Hypotheses Testing

Hypotheses	**Result**
H1. Trust	Not Supported
H2. Severity of Service Failure	Not Supported
H3. Quality of Service	Supported
H4. Failure Attribution	Supported
H5. Customer Satisfaction	Supported
H6. Frustration	Not Supported
H7. Anger	Not Supported
H8. Service Recovery	Supported

Notes: P<0,05

5. Conclusions and Discussion

5.1. General Discussion

The smart service industry is thriving at the moment and there are more and more companies who are offering their services via the internet. As is famously known all over the world, Netflix is a huge streaming platform, and they offer a variety in movies and series. Over the last couple of years, Netflix has increasing competition as the competitors have found their way on the market. In order to stay relevant and obtain competitive advantage, Netflix has evolved into a personalized provider. For this, they need more personal information about their customer so that Netflix can provide them with movies and series that are aligned with their viewing history. Thus, the influx from data is crucial for Netflix in order to operate. But an aspect which is often missed when it comes down to a huge amount of data is data management. Data management is important to keep track of all customers' data. As data is transferred via the internet, data breaches are a huge risk for the service providers. These providers must protect and invest in their data security at all costs in order to stay a reliable service provider. This research's aim is to analyse the effect a data breach has on the customer's perceptions and their emotional responses. There are three types of data breaches, and these are included in the CIA Triad. The types are confidentiality, integrity and availability breaches. This research focuses on those types of breaches and the effect they have on the customers. Khan et al (2021) touched on the types of breaches already but without connecting it to customers. This research investigates the consequences a data breach has and the possible reactions from customers towards the service provider. The study of Janakiraman et al (2018) is pretty similar but they are more focused on the behaviour of the customer and whether the customers will migrate to unbreached channels. Next to that, a huge difference is that their research focuses on the retailing industry instead of service providers via internet.

This study investigates seven constructs, and these constructs are compiled in order to investigate customer perception and emotional response. Five of the constructs measure customer perception and two constructs measure emotional response. Prior academic studies did not consider investigating a mix of possible responses. While it is interesting to compare the different reactions witch each other because it may strengthen each other or the other way around and weaken the connection. This study addresses the gap because one thing does not preclude the other. To make a thorough investigation happen, extensive research has been done to each construct in order to come up with the best way to measure them. Eventually, multiple measurement items have been formed to cover the variables because the variables entail a lot. The construct trust has been used as one of the subjects to investigate the customer's perception. Trust is an undisputed construct as it is involved in a lot that daily life has to offer. Hallikainen & Laukkanen (2018) have studied consumer trust in e-commerce, and they found out that a lack of trust a major barrier is in the adoption of e-commerce. Furthermore Kim & Park (2013) even discussed that trustworthiness is among the most important factors distinguishing buyers from non-buyers. This is evidence for the importance of trust, as trust is fundamental for making transitions. So, if a data breach occurs, the first thing that is impaired is trust as it is vital in life.

To reflect emotional responses, frustration and anger have been chosen. These two are in line with each other as anger is often the result of being frustrated. A customer can get frustrated after a data breach occurs because the mistake of insufficient data security can be blamed on the company. The company needs to cope with the consequences after a data breach, however this can also happen in an insufficient way. When that is the case, frustration turns into anger because the company has been incompetent. When a company takes responsibility and deal with the problem in the best possible way, the emotional response of a customer is not too severe. When emotions take the better of the customer, they show complaint behaviour. The recollection of an unfavourable service experience is likely to be associated with the negative emotions at the time of the event (Tronvoll, 2011).

5.2. Conclusion

Based on the above discussion and to answer the research question. There is a relationship between the customer reactions and the emotional responses when it comes down to a data breach. Obviously, a data breach is something negative for both company and customer. The consequences of a data breach negatively influence the investigated variables. Trust is fundamentally between parties and this decreases when there is a data breach. The quality of service is also negatively impacted by a data breach as good service should prevent a data breach from happening. Next to that, the severity of service failure is indistinct as for one individual something might be severe but for the other not. Severity is often related with the other consequences the data breach has. Failure attribution is good for acknowledging mistakes and try to do better next time. Customers appreciate that a company is transparent about this. The aspect of customer satisfaction also decreases after a data breach. This is in line with the expectation as someone would not be satisfied with the occurrence of a data breach and even worse leakage of their private data. This may result in frustration and even worse in anger with the result that eventually the individual will migrate towards a competitor of Netflix. The CIA dimensions are helpful measurements to get to know where the data breach occurred and what the exact consequences are.

5.3. Theoretical and Managerial Implications

Theoretical implications are important to write down as they consist of speculations on how the findings in this study can potentially impact and contribute to other studies in this field. Managerial implications summarize what the results mean and indicate whether an action should be taken in response. The implications are formulated for both the literature review and the empirical study.

5.3.1. Literature Review

This literature review congregated insights into cybersecurity incidents based on the CIA Triad and customer's perceptions. Since humans have entered the digital age where data has become very valuable, data management has become more important than ever. Companies that accumulate a lot of data from their customers need to invest in cybersecurity because possible attacks are on the rise. Data has become so valuable as it allows companies to steer their customers because those companies know exactly what customers are looking for based on previous behaviour. There is a lot at stake for both parties. Some operations within companies revolve around data. On the other hand, customers are getting more aware of it and the possible consequences a data leak might have for them. That is why customers consider what data they want to divulge before actually transferring the data. The possible change in customer behaviour means that customers are likely to spend less and visit less often following a security violation.

As has been found out through PR Newswire which has been used during this study, data breach announcements typically contain information about the number of people affected and specify the time period during which a particular breach took place. This study argues about data breach vulnerability as stolen data can be potentially misused and might have a change in customer behaviour as a result. This strengthens the negative effects of a data breach. The findings in this study also contribute to the literature on customer relationship management. Communication with the customer is very important and especially after a breach. It is up to the company to solve this problem without harming the customer. When the data breach has been solved in the least harming way, the company might retain their customers. If not, customers are reluctant to return to a company because they are harmed by the company. This means that customers are then looking for other companies. Janakiraman et al. (2018) have conducted a similar study, and they offer the same prescriptions. Due to the fact that data breaches are on the rise, companies should engage actively in damage control and address customer vulnerability. Broadly, this literature review contributes to the growing literature on data breach announcements and the impact it has on customers.

5.3.2. Empirical Study

This study investigated the customer's perceptions and emotional responses in an extensive way with regards to the CIA components. Various theoretical implications contribute to the academic literature and could be useful for others with the provided theories. The input for this study is derated from other studies and is a blend of theories and frameworks in order to investigate something new. Compared to other studies, this study analyses more different reactions in order to investigate perception as perception is such a indistinct construct and cannot be measured by one item. Instead of the usual variables such as money and time, this study includes more cognitive variables. This is the first study that contains a mix of possible customer reactions with regards to an online service failure.

Aside from the theoretical implications, this study also contains managerial implications. It starts with preventing the online service failures from happening. This means that service providers should invest in data security as this makes them aware that they possess valuable, private data. Besides that, maintaining a positive relationship with their customers is also important in order to retain customers. When the relationship is positive, the customers will also speak positively about the service provider. In other words, there will be a positive word-of-mouth. This might persuade other individuals in their surroundings to use Netflix as well which is good for Netflix's revenue. In the worst case scenario, a data breach will occur at the service provider. It is key to counter this immediately so that the damage will not be too severe, this also shows willingness to search for solutions. Customers appreciate this when a provider actively engages in service recovery actions. It is up for debate in which form as this is depending on the severity of the breach (Grewal et al., 2008).

5.4. Limitations and Future Research

Writing down limitations is an important aspect of conducting a study. Limitations provide context and shed light on gaps in the prevailing inquiry and literature. The purpose of future research is to systematically understand what is possible and desirable in the future and what events, actions and policies lead to these futures.

5.4.1. Literature Review

There has been some research conducted about data breach announcement (DBA). However, the connection between DBA and customer's perceptions has not often been made. The impact a DBA has on the customers is relatively new. Due to the fact that every person is different, they perceive the severity from a DBA also in a different manner. This makes it a complex matter as there are several reactions possible. This study only addresses one type of data breach recovery action namely apology. Thus, for future research it might be interesting to conduct research about other data breach recovery actions (compensation vs. remorse). This research touched a little bit on compensation but there is a lot more to achieve. Due to the fact that data breaches are on the rise it might be helpful for companies to have theory about data breach recovery actions. Furthermore, the prevention of data breaches might be even more important. It is always better to prevent something from happening than recovering from it. Few studies have done this and therefore it is a direction for future research. Another recommendation is to school the users about the danger of the internet. There is already an increase in the awareness of the downside of the internet. Many internet users have superficial knowledge about it and therefore it is a good idea to conduct research about actions that customers can take after a DBA.

5.4.2. Empirical Study

To make an overview of limitations is important for future research. In these future studies the problems faced in this research can be addressed so that it might not happen again. The first limitation is that this study is focused on online service providers. Nowadays, a lot of companies offer their services on the internet but there are a lot of different services, and this is why the findings are not generalisable. Similar research should be conducted in other contexts in order to explore this.

The second limitation is the relatively small sample size and that every respondent is from the east of the Netherlands. This might not seem a problem but for future research it might be better to investigate different places in the Netherlands as the findings might not be generalisable due to the difference in mentality.

The third limitation can be the lack of demographics. In this study only the demographics gender and age are investigated. This makes it possible to make a statement about age groups or gender and their perception towards a data breach. However, for future research it might be interesting to include for example education as well as this can offer new perspectives with regards to data breaches.

The fourth limitation might be that this study is only focused on quantitative research. The term triangulation means that the research makes use of more research techniques such as combining quantitative research with qualitative research. For future research this might be a good idea as when the outcomes of both techniques are equal, the findings strengthen each other because two methods come up with the same outcome.

References

Amatriain, X. (2013, August). Big & personal: data and models behind Netflix recommendations. In *Proceedings of the 2nd international workshop on big data, streams and heterogeneous source Mining: Algorithms, systems, programming models and applications* (pp. 1-6). https://doi.org/10.1145/2501221.2501222

Annarelli, A., Battistella, C., & Nonino, F. (2020). A framework to evaluate the effects of organizational resilience on service quality. *Sustainability*, *12*(3), 958. https://doi.org/10.3390/su12030958

Balaji, M. S., Khong, K. W., & Chong, A. Y. L. (2016). Determinants of negative word-of-mouth communication using social networking sites. *Information & Management*, *53*(4), 528-540. https://doi.org/10.1016/j.im.2015.12.002

Barrett, M., Davidson, E., Prabhu, J., & Vargo, S. L. (2015). Service innovation in the digital age. *MIS quarterly*, *39*(1), 135-154. https://www.jstor.org/stable/26628344

Bishop, P. A., & Herron, R. L. (2015). Use and misuse of the Likert item responses and other ordinal measures. *International journal of exercise science*, *8*(3), 297.

Bismark, M. M. (2009). The power of apology. *Clinical Correspondence*.

Bonifield, C., & Cole, C. (2007). Affective responses to service failure: Anger, regret, and retaliatory versus conciliatory responses. *Marketing Letters*, *18*, 85-99. DOI:10.1007/s11002-006-9006-6

Bougie, R., Pieters, R., & Zeelenberg, M. (2003). Angry customers don't come back, they get back: The experience and behavioral implications of anger and dissatisfaction in services. *Journal of the academy of marketing science*, *31*(4), 377-393.

Chow, S., & Holden, R. (1997). Toward an understanding of loyalty: the moderating role of trust. *Journal of managerial Issues*, 275-298. https://www.jstor.org/stable/40604148

Chang, H. H., Tsai, Y. C., Wong, K. H., Wang, J. W., & Cho, F. J. (2015). The effects of response strategies and severity of failure on consumer attribution with regard to negative word-of-mouth. *Decision Support Systems*, *71*, 48-61. https://doi.org/10.1016/j.dss.2015.01.007

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211. https://doi.org/10.1002/widm.1211

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in industry*, *114*, 103165. https://doi.org/10.1016/j.compind.2019.103165

Culiberg, B., & Rojšek, I. (2010). Identifying service quality dimensions as antecedents to customer satisfaction in retail banking. *Economic and business review*, *12*(3). https://doi.org/10.15458/2335-4216.1245

Dabholkar, P. A., & Sheng, X. (2012). Consumer participation in using online recommendation agents: effects on satisfaction, trust, and purchase intentions. *The Service Industries Journal*, 32(9), 1433–1449.

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, *31*(2), 243-256. https://doi.org/10.1016/j.clsr.2015.01.005

Delice, A. (2010). The Sampling Issues in Quantitative Research. *Marmara University Faculty of Atatürk Education.* https://files.eric.ed.gov/fulltext/EJ919871.pdf

Duggineni, S. (2023). Impact of Controls on Data Integrity and Information Systems. *Science and Technology*, *13*(2), 29-35. DOI: 10.5923/j.scit.20231302.04

Ethicist, P. (2015). Simplifying the complexity of confidentiality in research. *Journal of Empirical Research on Human Research Ethics*, *10*(1), 100-102. https://doi.org/10.1177/1556264614568783

Etikan, I., & Bala, K. (2017). Sampling and sampling methods. *Biometrics & Biostatistics International Journal*, *5*(6), 00149. DOI: 10.15406/bbij.2017.05.00149

Fenrich, K. (2008). Securing your control system: the" CIA triad" is a widely used benchmark for evaluating information system security effectiveness. *Power Engineering*, *112*(2), 44-49.

Fuqua, D. R., Leonard, E., Masters, M. A., Smith, R. J., Campbell, J. L., & Fischer, P. C. (1991). A structural analysis of the state-trait anger expression inventory. *Educational and Psychological Measurement*, *51*(2), 439-446. https://doi.org/10.1177/0013164491512018

Gelbrich, K. (2010). Anger, frustration, and helplessness after service failure: coping strategies and effective informational support. *Journal of the Academy of Marketing Science*, *38*, 567-585. https://doi.org/10.1007/s11747-009-0169-6

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action. *MIS Quarterly*, *41*(3), 703-A16. https://www.jstor.org/stable/26635011

Gupta, A., & Anand, A. (2017). Ethical hacking and hacking attacks. *Int. J. Eng. Computer. Science*, *6*(6), 2319-7242. https://doi.org/10.18535/ijecs/v6i4.42

Grewal, D., Roggeveen, A. L., & Tsiros, M. (2008). The effect of compensation on repurchase intentions in service recovery. *Journal of retailing*, *84*(4), 424-434. dx.doi.org/10.1016/j.jretai.2008.06.002

Hallikainen, H., & Laukkanen, T. (2018). National culture and consumer trust in e-commerce. *International journal of information management*, *38*(1), 97-106. https://doi.org/10.1016/j.ijinfomgt.2017.07.002

Hardin, R. (2002). *Trust and trustworthiness*. Russell Sage Foundation.

Havlena, W. J., & DeSarbo, W. S. (1991). On the measurement of perceived consumer risk. *Decision Sciences*, *22*(4), 927-939. https://doi.org/10.1111/j.1540-5915.1991.tb00372.x

Hill, N., & Alexander, J. (2017). *The handbook of customer satisfaction and loyalty measurement*. Routledge.

Hussain, R., Al Nasser, A., & Hussain, Y. K. (2015). Service quality and customer satisfaction of a UAE-based airline: An empirical investigation. *Journal of Air Transport Management*, *42*, 167-175. https://doi.org/10.1016/j.jairtraman.2014.10.001

Jackson, J. E. (2005). Varimax rotation. *Encyclopedia of biostatistics*, *8*. https://doi.org/10.1002/0470011815.b2a13091

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behaviour: Evidence from a multichannel retailer. *Journal of marketing*, *82*(2), 85-105. https://doi.org/10.1509/jm.16.0124

Jeronimus, B.F., Laceulle, O.M. (2017). Frustration. In book: Encyclopaedia of Personality and Individual Differences, Edition: 1, Publisher: Springer, New York, Editors: Virgil Zeigler-Hill and Todd K. Shackelford, pp.1-8. Doi: 10.1007/978-3-319-28099-8_815-1

Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management: An integrated risk model. *Information & Management*, *58*(1), 103392. https://doi.org/10.1016/j.im.2020.103392

Kim, M. S., & Kim, S. (2018). Factors influencing willingness to provide personal information for personalized recommendations. *Computers in Human Behaviour*, *88*, 143-152. https://doi.org/10.1016/j.chb.2018.06.031

Kim, S., & Park, H. (2013). Effects of various characteristics of social commerce (s-commerce) on consumers' trust and trust performance. *International Journal of Information Management*, *33*(2), 318-332. https://doi.org/10.1016/j.ijinfomgt.2012.11.006

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Kumar, S., & Agarwal, D. (2018). Hacking attacks, methods, techniques and their protection measures. *International Journal of Advance Research in Computer Science and Management*, *4*(4), 2253-2257.

Lee, I. (2017). Big data: Dimensions, evolution, impacts, and challenges. *Business horizons*, *60*(3), 293-303. https://doi.org/10.1016/j.bushor.2017.01.004

Leninkumar, V. (2017). The relationship between customer satisfaction and customer trust on customer loyalty. *International Journal of Academic Research in Business and Social Sciences*, *7*(4), 450-465. DOI: 10.6007/IJARBSS/v7-i4/2821

Lewicki, R. J., & Brinsfield, C. (2017). Trust repair. *Annual review of organizational psychology and organizational behaviour*, *4*, 287-313. https://doi.org/10.1146/annurev-orgpsych-032516-113147

Madarie, R. (2017). Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. *International Journal of Cyber Criminology*, *11*(1). DOI: 10.5281/zenodo.495773

Marianus, S., & Ali, S. (2021). Factors determining the perceived security dimensions in B2C electronic commerce website usage: an Indonesian study. *Journal of Accounting and Investment*, *22*(1), 104-132. https://doi.org/10.18196/jai.v22i1.8171

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

McAllister, D. J. (1995). Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of management journal*, *38*(1), 24-59.

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs*, *51*(1), 133-161. https://doi.org/10.1111/joca.12111

Munusamy, J., & Chelliah, S. (2011). An investigation of impact of service strategy on customers' satisfaction in the budget airline industry in Malaysia: a case study of air Asia. *Contemporary Marketing Review*, *1*(1), 1-13.

Nelissen, R. M. A., & Zeelenberg, M. (2009). Moral emotions as deter- minants of third-party punishment: Anger, guilt, and the functions of altruistic sanctions. *Judgment and Decision Making*, *4*, 543–553. https://doi.org/10.1017/S1930297500001121

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security. *NIST special publication*, *800*(12), 101. https://doi.org/10.6028/NIST.SP.800-12r1

Pappas, I. O., Kourouthanassis, P. E., Giannakos, M. N., & Chrissikopoulos, V. (2017). Sense and sensibility in personalized e-commerce: How emotions rebalance the purchase intentions of persuaded customers. *Psychology & Marketing*, *34*(10), 972-986. DOI: 10.1002/mar.21036

Peters, L. H., O'Connor, E. J., & Rudolf, C. J. (1980). The behavioural and affective consequences of performance-relevant situational variables. *Organizational Behaviour and Human Performance*, *25*(1), 79-96. https://doi.org/10.1016/0030-5073(80)90026-4

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of public policy & marketing*, *19*(1), 27-41. https://doi.org/10.1509/jppm.19.1.27.16941

Richards, Neil M. and Hartzog, Woodrow, Privacy's Trust Gap (January 15, 2017). 126 Yale Law Journal 1180 (2017), Washington University in St. Louis Legal Studies Research Paper 17-02-04, Available at SSRN: https://ssrn.com/abstract=2899760

Rid, T., & Buchanan, B. (2015). Attributing cyber-attacks. *Journal of Strategic Studies*, *38*(1-2), 4-37. https://doi.org/10.1080/01402390.2014.977382

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review*, *23*(3), 393-404. https://doi.org/10.5465/amr.1998.926617

Sanctum Inc, "Ethical Hacking techniques to audit and secure web enabled applications", 2002.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students*. Pearson Education, Limited.

Scharf, S. (2007). Report casts doubt on the impact of data breaches on identity theft. *Internal Auditor*, *64*(4), 23-24.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314-341. https://doi.org/10.1080/07421222.2015.1063315

Sengupta, A. S., Balaji, M. S., & Krishnan, B. C. (2015). How customers cope with service failure? A study of brand reputation and customer satisfaction. *Journal of business research*, *68*(3), 665-674. https://doi.org/10.1016/j.jbusres.2014.08.005

Shiue, Y. C., & Li, L. S. H. (2013). Brand involvement in retaining customers despite dissatisfaction. *Social Behavior and Personality: an international journal*, *41*(4), 643-650. https://doi.org/10.2224/sbp.2013.41.4.643

Shrestha, N. (2021). Factor analysis as a tool for survey analysis. *American Journal of Applied Mathematics and Statistics*, *9*(1), 4-11. DOI:10.12691/ajams-9-1-2

Smith, N. C., & Cooper-Martin, E. (1997). Ethics and target marketing: The role of product harm and consumer vulnerability. *Journal of marketing*, *61*(3), 1-20. https://doi.org/10.1177/002224299706100301

Sykes, A. O. (1993). An introduction to regression analysis.

Taber, K.S. The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Res Sci Educ* 48, 1273–1296 (2018). https://doi.org/10.1007/s11165-016-9602-2

Tronvoll, B. (2011). Negative emotions and their effect on customer complaint behaviour. *Journal of Service Management*, *22*(1), 111-134. DOI: 10.1108/09564231111106947

Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce*, *23*(2), 1-11.

Tsarenko, Y., & Tojib, D. (2012). The role of personality characteristics and service failure severity in consumer forgiveness and service outcomes. *Journal of Marketing Management*, *28*(9-10), 1217-1239. https://doi.org/10.1080/0267257X.2011.619150

UCLA: Statistical Consulting Group. (2021). *A PRACTICAL INTRODUCTION TO FACTOR ANALYSIS: EXPLORATORY FACTOR ANALYSIS.* Retrieved 11 10, 2023, from Advanced Research Computing. Statistical Methods and Data Analytics: https://stats.oarc.ucla.edu/spss/seminars/introduction-to-factor-analysis/a-practical-introduction-to-factor-analysis/

U.S. Department of Health and Human Services, State and Tribal Child Welfare Information Systems, Information Security Data Breach Response Plans, Administration for Children and Families, 2015. https://www.acf.hhs.gov/sites/ default/files/cb/im1504.pdf.

Van Doorn, J., Zeelenberg, M., & Breugelmans, S. M. (2014). Anger and prosocial behaviour. *Emotion Review*, *6*(3), 261-268. https://doi.org/10.1177/1754073914523794

Wang, Y., Lo, H. P., & Yang, Y. (2004). An integrated framework for service quality, customer value, satisfaction: Evidence from China's telecommunication industry. *Information systems frontiers*, *6*, 325-340. https://doi.org/10.1023/B:ISFI.0000046375.72726.67

Wang, Y. S., Wu, S. C., Lin, H. H., & Wang, Y. Y. (2011). The relationship of service failure severity, service recovery justice and perceived switching costs with customer loyalty in the context of e-tailing. *International journal of information management*, *31*(4), 350-359. https://doi.org/10.1016/j.ijinfomgt.2010.09.001

Weisberg, S. (2005). *Applied linear regression* (Vol. 528). John Wiley & Sons.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

Yamakawa, Y., Peng, M. W., & Deeds, D. L. (2015). Rising from the ashes: Cognitive determinants of venture growth after entrepreneurial failure. *Entrepreneurship Theory and Practice*, *39*(2), 209-236. https://doi.org/10.1111/etap.12047

Appendices

Appendix A – Manipulated Announcements

Streaming giant Netflix hit by a cyber-attack.

Confidentiality with apology:
Customers of streaming service Netflix **(NASDAQ: NFLX)** have been made aware of a data breach when the company suffered a large-scale hacker attack.
This resulted in unauthorized access and loss of control with regard to Netflix user information. On behalf of Netflix's CEO Ted Sarandos, the company apologises to the affected users.

Streaming giant Netflix hit by a cyber-attack.

Confidentiality without apology:
Customers of streaming service Netflix **(NASDAQ: NFLX)** have been made aware of a data breach when the company suffered a large-scale hacker attack.
This resulted in unauthorized access and loss of control with regard to Netflix user information.

Streaming giant Netflix hit by a cyber-attack.

Integrity with apology:
Customers of streaming service Netflix **(NASDAQ: NFLX)** have been made aware of a data breach when the company suffered a large-scale hacker attack.
This resulted in unauthorized access and modification of data with Netflix user information.
On behalf of Netflix's CEO Ted Sarandos, the company apologises to the affected users.

Streaming giant Netflix hit by a cyber-attack.

Integrity without apology:
Customers of streaming service Netflix **(NASDAQ: NFLX)** have been made aware of a data breach when the company suffered a large-scale hacker attack.
This resulted in unauthorized access and modification of data with Netflix user information.

Streaming giant Netflix hit by a cyber-attack.

Availability with apology:
Customers of streaming service Netflix **(NASDAQ: NFLX)** saw their access to the service disrupted after a distributed denial of service (DDoS) attack hit Netflix's servers.
This resulted in a service outage and viewing downtime for a short amount of time.
On behalf of Netflix's CEO Ted Sarandos, the company apologises to the affected users.

Streaming giant Netflix hit by a cyber-attack.

Availability without apology:
Customers of streaming service Netflix **(NASDAQ: NFLX)** saw their access to the service disrupted after a distributed denial of service (DDoS) attack hit Netflix's servers.
This resulted in a service outage and viewing downtime for a short amount of time.