

A quantitative study on the effect of cognitive trust and emotional violation on repurchase intention after a data breach

Author: Lauren van Leussen
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

ABSTRACT,

In today's society, where the internet continues to grow, more and more companies are using online data. Because these companies are so dependent on this online data, it makes them extra vulnerable to cyber security threats such as data breaches. An example of such a company is Netflix, one of the largest online streaming services at the moment. This study investigated the repurchase intent of Netflix customers after they read that their data had been leaked during a cyberattack. To be specific, we investigated the effect of cognitive trust and emotional violation on repurchase intention after reading a data breach announcement. This research was conducted by distributing online surveys, after which 265 people participated in the study. The study showed that, in a data breach context, cognitive trust has a positive and significant effect on repurchase intention and that emotional violation has a negative and significant effect on repurchase intention. Hence, this study emphasizes that it is imperative for companies to prioritize and invest in data security measures.

Graduation Committee members:

Dr. Agata Leszkiewicz

Dr. Letizia Alvino

Keywords

Data breach, data breach announcement, CIA triad, cognitive trust, emotional violation, repurchase intention

1. INTRODUCTION

In 2014, Home Depot was the victim of a cybersecurity attack. Because malware was installed on the self-checkout terminals, it was possible for criminals to access customer data. In total, more than 50 million American and Canadian customers have become victims of the data breach and names, email addresses and credit card information, among other things, have been leaked. Initially, Home Depot expected growth of 4.8% that year. However, analysts expected that the data breach could lead to high financial costs and that it needed to be more determined whether the expected growth would be feasible (Vinton, 2014).

In today's society, the internet is still growing, and so do the concerns about the use of customer information. There have been many technological developments in the area of storage technologies (Alshehri et al., 2020). Companies like Spotify, Netflix, and other smart service companies use those storage technologies and rely on the data it stores. The fact that these companies are so dependent on data and digital technologies makes them more vulnerable to cybersecurity threats like data breaches. The costs of these data breaches are sky-high: in 2020, the average cost of a data breach in the US was 9.44 million dollars, 5.04 million more than the global average (Ponemon Institute, 2020). In 2019 the average cost in the US was 8.19 million dollars, and the global average was 3.92 million dollars (Ponemon Institute, 2019). Comparing these costs with the costs of the years before, we can identify a positive trend.

According to the European Commission (2016), "A data breach occurs when the data for which your company/organisation is responsible suffers a security incident resulting in a breach of confidentiality, availability or integrity.". Data breaches are thus classified into three categories in terms of their effect: availability (i.e. "ensuring timely and reliable access to and use of information"), confidentiality (i.e. "preserving authorised restrictions on access and disclosure, including means for protecting personal privacy and proprietary information") and integrity (i.e. "guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity") (U.S. Government Publishing Office, 2015, p. 153). Sometimes a data breach can have more than one effect, for example, when a violation of the confidentiality of the information leads to a service being temporarily unavailable to users. Gordon et al. (2011) found that a breach associated with availability has the highest impact on a company's stock market return. If the individuals affected by the data breach are at high risk, the company is obligated to inform those individuals (European Commission, 2016). Due to the time and scope of the research, this thesis will focus on the confidentiality and integrity effect of a data breach.

Data breaches do not only affect a company's stock market return, but looking from a customer's perspective, it might also influence the behaviour of a customer. As a data breach containing customer information privacy is a violation of trust, it can be considered a service failure (Malhotra et al., 2011). This allows us to get more insight into the consequences of a data breach. Afroz et al. (2013) found that customers who were aware of privacy flaws like data breaches were less likely to trust a company in comparison to customers who were not aware of the privacy issues. The timing of the announcement of a data breach also has consequences; the longer companies wait with announcing the data breach, the more negative the impact on consumer trust (Muzatko et al., 2020). Janakiraman et al. (2018) found that customers who were a victim of a data breach were more likely to switch from a retailer's breached channel to an unbreached channel in comparison to a customer that was not victimised by a data breach. Therefore, they concluded that it was advisable for firms to invest in multiple channels to help absorb

the external shock of a data breach. Next to this, they also found that customers were more likely to cut back on their spending after a data breach announcement. They were, however, unable to identify the relationship with the severity of the breach.

1.1 Research objective and question

This thesis aims to better understand a customer's repurchase intention because of reading a data breach announcement. More specifically, the research objective is to assess the relationship between post-repurchasing behaviour and two independent variables concerning perceived vulnerability: emotional violation and cognitive trust. This research is intended to show whether the selected vulnerability perceptions influence customer behaviour and how strong the relationship is.

To reach this objective, the following research question has been formulated: *"What is the effect of cognitive trust and emotional violation on repurchase intention after reading a DBA?"*

1.2 Academic and practical relevance

In the literature, there can be found many studies on how to prevent a data breach (Muhammad, 2019; Bhalme et al., 2022) and strategies on how to recover from such a service failure (Hoehle et al., 2016; Rasoulia et al., 2023; Mohammed et al., 2023). However, research on the effects of a data breach and on the customers that were involved in it is currently missing (Schlackl et al., 2022). Chakraborty et al. (2016) found that the perceived severity of the failure and the perceived risk were both significant drivers for post-breach online shopping, but research on the effect of the emotional responses after reading a data breach announcement on customer's repurchase intention could be something to do more research on to get a better in-depth understanding. One research conducted by Choi et al. (2016) linked two psychological drivers, 'perceived breach' and 'feelings of violation', and two behavioural outcomes 'post-WOM' and 'post-likelihood of switching'. Other behavioural outcomes such as complaining, repurchase intention, and customer satisfaction have, to my best knowledge, not been researched in-depth in this setting by prior literature. The goal of this study is to partly fill this gap in the literature and expand the understanding of the relationship between psychological drivers and behavioural outcomes by assessing the effect of two independent variables, 'emotional violation' and 'cognitive trust', on the dependent variable 'repurchase intention'. It is important to research these variables to better understand what causes this type of customer behaviour and whether or not the selected variables influence it. In addition, it also comes in handy in the practical field of doing business. This research will also respond to the literature's call for further research on the effect of data breaches in combination with the use of non-U.S. data sets (Schlackl et al., 2022).

Besides the academic relevance of the thesis, this research is also valuable to the practical field of conducting business. Research has shown that data breaches can have a significant effect on the market value of a firm and the performance of a firm in general (Tripathi, 2020). Next to this, a service failure like a data breach can negatively impact the customer-firm relationship. From a firm's perspective, it is therefore useful to know what the exact impact of a data breach is in order to choose a proper recovery strategy. Knowing how customers will react to psychological factors caused by a data breach makes it easier for a company to respond to customer needs. This gives you more insight into how the customer-company relationship should be restored, and based on the existing research into recovery strategies, companies can act more efficiently. In addition, companies will also be able to better

estimate what they need to realise their recovery; think, for example, of the number of extra staff in a specific department.

2. LITERATURE REVIEW AND HYPOTHESES

2.1 CIA triad

As stated in the introduction, data breaches can be classified into three categories based on their effect. These three categories are described by the CIA triad (figure 1). CIA stands for confidentiality, integrity, and availability. The CIA triad is a well-known model in the information security sector, and it suggests that an IT security system should comply with three basic requirements. If these requirements are met, it can be more or less assured that the data of the IT system is secured. The triad can function as a checklist and guide organisations on how to develop security policies within their firm.

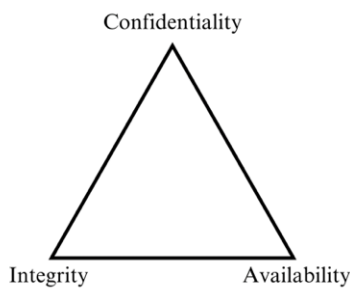


Figure 1 – CIA triad

2.1.1 Confidentiality

As a first requirement, the IT system should comply with the confidentiality aspect. This means that the system data should only be distributed to authorised persons. As data should only be accessible to intended users, measures regarding confidentiality are present to assure that sensitive data will not fall into the wrong hands of parties that are unauthorised to access the data. The strength of the measure can depend on the type of data and the damage that it can cause if it leaks.

2.1.2 Integrity

Secondly, the IT system should live up to the integrity requirement. The data of the IT system should be accurate, consistent, complete, and trustworthy. Therefore, the system data should only be altered by the persons that are authorised to do so. The measures taken to prevent a violation of integrity should make sure that data should be maintained in the correct state, exactly as it was received.

2.1.3 Availability

Lastly, the IT system should be available to use, and its data should be accessible at any time when needed by authorised persons. Uninterrupted access must be ensured in order to let appropriate users of the data utilise the system when necessary. The unavailability of data can also be a consequence of an integrity data breach or a confidentiality data breach.

2.2 Vulnerability perceptions

2.2.1 Cognitive trust

One of the vulnerability perceptions that comes in combination with a data breach is cognitive trust (Martin et al., 2017). According to Malhotra et al. (2011), data breaches can be

considered a service failure. As customers exchange their personal information in return for a certain product or service, it can be considered a social contract (Culnan et al., 1999) and they expect that their personal information will be handled with care. If this is not the case and a cybersecurity attack like a data breach occurs, customers can perceive this as a violation of the psychological contract and thus, a violation of trust. Wang et al. (2007, p.1035) state that “A violation of trust occurs when the buyer perceives that the seller’s failure violated a psychological contract between the seller and the buyer.”. Robinson et al. (1994) also found that violation of a psychological contract is negatively associated with trust.

2.2.2 Emotional violation

Violations of psychological contracts can cause not only cognitive responses but also emotional responses like feelings of violation (Malhotra et al., 2011). When customers who were victims of the data breach get aware of the fact that their information is in the hands of unauthorised parties, emotional reactions such as hurt and anger might arise (Lewicki, 1996). Dawson et al. (2014) found that a breach of a psychological contract could lead to fewer positive behaviours and feelings of violation. Violation is an emotional state and is characterised by “anger, resentment, bitterness, indignation, or even outrage” (Morrison et al., 1997, p.231).

2.3 Repurchase intention

Hellier et al. (2003, p.1764) defined repurchase intention as “The individual’s judgement about buying a designated service from the same company again, taking into account his or her current situation and likely circumstances.”. A customer’s repurchase behaviour is an important variable for a company’s profitability; if a customer decides to purchase a given product or service time and again, it has a positive effect on the company’s profits. Therefore, the repurchase intention of a firm’s customers is interesting to research. As data breaches contain personal and possibly sensitive information, customers might choose to avoid future possible data breaches by choosing not to repurchase any products or services anymore from the given provider or retailer.

2.4 Hypotheses

To answer the main research question of this thesis, “What is the effect of cognitive trust and emotional violation on repurchase intention after reading a DBA?”, two sub-questions have been formulated in the form of hypotheses.

2.4.1 Cognitive trust and repurchase intention

The overall satisfaction of the customer experience can be an indicator of a customer’s trust in a company. As online services are more present than ever in today’s society, the browsing experience of a customer, in combination with privacy and security concerns, can negatively impact a customer’s trust in the given company (Chakraborty et al., 2016). This trust can be a driver for customers to return to the specific provider or retailer and purchase the product or service again. Accordingly, the following has been hypothesised:

Hypothesis 1: Cognitive trust will be positively related to repurchase intention after reading a DBA.

2.4.2 Emotional violation and repurchase intention

An emotional response such as a feeling of violation is likely to happen after being a victim of a data breach. According to Morrison et al. (1997), feelings of bitterness, resentment, anger, and sometimes even outrage may be accompanied by not being able to stop thinking about the cause of the rising emotions. Next to this, they state that this intense emotional state can be deeply distressing. As a consequence of such deep negative feelings, customers might choose not to purchase any products or services anymore from the given provider or retailer. Accordingly, the following has been hypothesised:

Hypothesis 2: Emotional violation will be negatively related to repurchase intention after reading a DBA.

2.5 Conceptual framework

Consequently, the following conceptual framework has been designed:

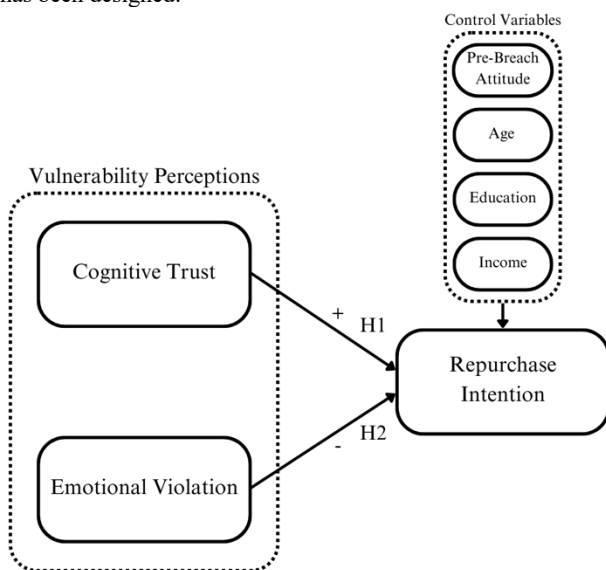


Figure 2 – Conceptual framework

3. METHODOLOGY

3.1 Sample

For this study, a total of 265 participants responded to an online distributed questionnaire. The survey was distributed in the English language through personal networks and three different social media platforms: LinkedIn, Instagram, and WhatsApp. To assure confidentiality, the surveys were completed anonymously. Next to this, participants could pause the questionnaire and continue it at a later moment, and, if preferable, they could withdraw from the research at any time.

Of the total of 265 respondents, 181 of them filled out the questionnaire completely. Subsequently, the respondents under the age of 16, the respondents who disagreed with the terms and conditions and the respondents who were not familiar with Netflix were also removed from the final sample. Ultimately, the sample size thus consists of 173 respondents.

3.2 Method

Questionnaires are often used for descriptive or explanatory research and work best when using standardised questions to guarantee that respondents will interpret the questions in the same way (Saunders et al., 2019). To test the

hypotheses and answer the research question of this thesis, quantitative data will therefore be gathered via online surveys.

The survey questions are adapted from existing literature and are measured using a seven-point Likert scale (1 = strongly disagree, 7 = strongly agree). Regarding the control variables age, education and income, existing scales from previous research by Dangelico et al. (2022) were used for the measurement. The respondents' pre-breach attitude was measured by one general question: "Generally speaking, are you currently satisfied with the Netflix subscription?". The respondent could answer this question by selecting yes, neutral or no. The questionnaire can be found in the Appendix (chapter 9.5) and is based on the operationalisation table in table 1.

The survey consisted of four parts. After verifying that the respondent was 16 years or older, the first part began with five questions about Netflix. It asked whether the respondent was familiar with the company, whether he/she currently has an active subscription and whether he/she was the person who paid for the subscription. If not, the respondent was also asked whether he/she participated in the decision-making process about whether or not to continue the subscription. The first part ended with a general question about their satisfaction with the Netflix subscription. Subsequently, in the second part, the respondents were shown a data breach announcement. In this data breach announcement, they read that there had been a data breach which had caused a confidentiality and integrity breach. After reading the announcement, in the third part of the questionnaire, participants were asked to indicate how much they agreed on a scale of 1 to 7, with six statements related to the topic of cognitive trust, three statements about emotional violation and finally, four statements related to his/her repurchase intention. In the final part, the questionnaire concluded with three socio-demographic questions about age, education, and monthly net income.

Table 1 – Operationalisation table

Variable	Source	Number of items
Cognitive trust (IV)	Xie et al., 2009	6 *
Emotional violation (IV)	Choi et al., 2016	3 *
Repurchase intention (DV)	Xu et al., 2023; Lu et al., 2023	4 *
Age, Education, Income (CV)	Dangelico et al., 2022	Ordinal variables
Pre-breach attitude (CV)	/	1: "Generally speaking, are you currently satisfied with the Netflix subscription?"

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

3.2.1 Control variables

To avoid third variables influencing the research, several control variables that are likely to affect the outcome of the questionnaires are included. Chakraborty et al. (2016) examined older and younger adults' online shopping intentions in the context of data breaches and found that there were significant differences between the two age groups. Another research conducted by Dölarslan (2014) showed that loyalty behaviours like repurchase intention are also affected by a person's age, but next to this, also by his or her level of education

and income. Accordingly, the following control variables will be considered: age, education, and income.

In order to correctly establish the person's level of cognitive trust, the control variable 'pre-breach attitude' will be taken into account. This variable measures how satisfied a Netflix customer is with his or her subscription before they are made aware of the data breach. This makes it easier to determine whether the person already had a negative attitude towards Netflix without there being a data breach, which could eventually influence the research.

Due to the time and scope of this research, more control variables will not be included.

3.3 Analysis

To analyse the collected survey data, the data will be imported into RStudio. The first step of the analysis is to check whether the data is normally distributed using a Shapiro-Wilk test. If this is the case, the Pearson correlation coefficient will be used later in the analysis as a method to test the correlation between the variables. If the data is not normally distributed, then Spearman's Rank Order will be used as method. Subsequently, the scales will first be validated by calculating Cronbach's Alpha. For this, Nunnally's (1978) thumb rule will be used, which suggests that an alpha of 0.7 or higher is acceptable to assume that the items of a variable are internally consistent. After calculating Cronbach's Alpha, a Kaiser-Meyer-Olkin test will be performed to test for sampling adequacy. Instead of directly accepting a score higher than 0.5, a score around 0.6-0.7 will be preferred, as recommended by Kaiser et al. (1974). As a next step, a principal component analysis will be performed to reduce the dimensionality of the dataset without losing important information. An eigenvalue higher than one will be used as the cut-off point. Principal components that have an eigenvalue lower than one will not be included in the regression analysis. Before the regression analysis is done as the last step of the analysis, the correlation between the variables will first be measured. The method that will be used for this depends on the outcome of the Shapiro-Wilk test. Finally, as mentioned earlier, a regression analysis will be performed to show whether there is a significant relationship between repurchase intention and cognitive trust and repurchase intention and emotional violation.

4. RESULTS

The dataset was imported and analysed in RStudio. After cleaning the data and removing incomplete responses, a Shapiro-Wilk Test was performed to indicate whether the data was normally distributed or not (table 6 in the Appendix). For both the independent variables, cognitive trust and emotional violation, as well as the dependent variable, repurchase intention, the test showed an insignificant result. This means that, given that the p-value is smaller than 0.05, the hypothesis that the data is normally distributed can be rejected. Because normal distribution cannot be assumed for any of the variables, the most suited measurement used for correlation would be Spearman's Rank Order. The histograms with the normal curve for each variable can be found in figure 4a-4c in the Appendix. In the histograms can be seen that the data of cognitive trust and repurchase intention is skewed to the left. Emotional violation, however, shows a skew that is more to the right.

4.1 Respondents' profile

Table 2 below shows the socio-demographic characteristics of the respondents, such as age, education, and monthly net income.

Table 2 – Socio-demographic characteristics (N = 173)

	Frequency	Percentage
Age		
Under 18	10	5.780
18 – 24	90	52.023
25 – 34	29	16.763
35 – 44	14	8.092
45 – 54	19	10.983
55 – 65	7	4.046
Over 65	4	2.312
Education		
Primary education	4	2.312
Lower secondary education	12	6.936
Upper secondary education	44	25.434
Bachelor's degree	83	47.977
Master's degree	25	14.451
PhD	3	1.734
Other education	2	1.156
Monthly net income		
Less than €1.000	61	35.260
€1.000 – €1.500	19	10.983
€1.501 – €2.000	21	12.139
€2.000 – €2.500	21	12.139
€2.501 – €3.000	16	9.249
Over €3.000	35	20.231

4.2 Descriptive analysis

Table 3 shows the descriptive statistics for the different items of the independent variables and the dependent variable. As can be seen in the table, all the items of repurchase intention have approximately the same mean and standard deviation. For cognitive trust, there is one item, CT5, which has a slightly higher mean (5.364) compared to the other items. The three items of emotional violation obtained a mean ranging from 3.092 to 4.133 and a standard deviation between 1.374 and 1.478. See table 11 in the Appendix for an overview of all the items.

Table 3 – Descriptive statistics

	Mean	SD	α
Repurchase intention			0.83
RI1	5.619	0.997	
RI2	5.491	1.108	
RI3	5.619	1.118	
RI4	5.653	1.082	
Cognitive trust			0.70
CT1	4.767	1.188	
CT2	4.757	0.970	
CT3	4.994	1.009	
CT4	4.717	1.550	
CT5	5.364	1.167	
CT6	4.873	1.323	

Emotional violation		0.81
EV1	4.133	1.478
EV2	3.659	1.374
EV3	3.092	1.399

4.3 Scale validation

4.3.1 Cronbach's Alpha

To test the reliability of the measurement scales, Cronbach's Alpha has been calculated (table 3). The first independent variable, cognitive trust, scored an alpha of 0.7. The second and last independent variable, emotional violation, scored an alpha of 0.81. Lastly, the dependent variable repurchase intention scored an alpha of 0.83. An alpha of 0.7 or higher indicates internal consistency between items (Nunnally, 1978). As both the independent variables, as well as the dependent variable scored 0.7 or higher, it can thus be said that the items of the variables are internally consistent.

4.3.2 Kaiser-Meyer-Olkin test

Prior to the principal component analysis, a Kaiser-Meyer-Olkin (KMO) test was performed to test for sampling adequacy (table 7a-7c in the Appendix). All items within the scales were tested on appropriateness. The six items for measuring cognitive trust scored a 0.7, a middling score according to Kaiser et al. (1974). The three items for emotional violation had a middling score (Kaiser et al., 1974) of 0.7. Lastly, the four items for the dependent variable repurchase intention scored a 0.73, also a middling score according to Kaiser et al. (1974). As suggested by Kaiser et al. (1974) to aim for a score around 0.6-0.7, rather than accepting a score higher than 0.5, sampling adequacy is detected.

4.3.3 Principal component analysis

To reduce the dimensionality of the data without losing important information, a principal component analysis (PCA) was performed for both independent variables as well as the dependent variable (table 8a-8c in the Appendix). The components with an eigenvalue greater than one, which are considered stable, will be used to perform the regression analysis (Girden et al., 2010). For the variable cognitive trust, the PCA shows that PC1 has an eigenvalue of 2.507 and PC2 has an eigenvalue of 1.177. Together, PC1 and PC2 explain 61.4% of the variance. To understand the difference between the two components of cognitive trust, table 9a-9c in the Appendix show the rotated component matrixes for the three variables. In table 9a can be seen that PC1 of cognitive trust correlates the most with CT1, CT3, CT5 and CT6. PC2, on the other hand, correlates the most with CT2 and CT4. Using the PCA, the six items have now thus been split into two components without losing much information. As the other components of cognitive trust have an eigenvalue smaller than one, these will not be considered for the regression analysis. The variables emotional violation and repurchase intention have both only one component with an eigenvalue greater than one. PC1 of emotional violation has an eigenvalue of 2.178 and explains 72.6% of the variance, and PC1 of repurchase intention has an eigenvalue of 2.681 and explains 67.0% of the variance. So, for the regression analysis PC1 of repurchase intention, PC1 and PC2 of cognitive trust, and PC1 of emotional violation will be used. For compactness, I will refer to the principal components by their concept names throughout the rest of the thesis.

4.4 Correlation

Based on the principal component analysis performed earlier, a correlation matrix was made. Table 4 below shows the simplified version of the matrix, including the correlations between the principal components of the independent variables and the dependent variable. The correlation matrix with the control variables included can be found in table 10 in the Appendix.

The tables show that both the first (0.42) and second factor (0.17) of cognitive trust seem to be significantly positively correlated with repurchase intention. Emotional violation shows a significant negative correlation of -0.38 with repurchase intention. Emotional violation is also significantly negatively correlated with the first factor of cognitive trust (-0.24).

Regarding the control variables, pre-breach attitude and repurchase intention seem to have a significant positive correlation of 0.24. Pre-breach attitude is also significantly positively correlated with the first (0.27) and second factor (0.26) of cognitive trust. Lastly, income seems to have a significant positive correlation with age (0.66) and education (0.22).

Table 4 – Correlation

	1	2	3
1 RI (PC1)			
2 CT (PC1)	0.42 ***		
3 CT (PC2)	0.17 *	-0.01	
4 EV (PC1)	-0.38 ***	-0.24 **	0.12

***, ** and *. Correlation is statistically significant at 0.001, 0.01 and 0.05, respectively (two-tailed)

4.5 Hypotheses testing

Table 5 shows the regression results of the relationship between the first and second principal component of cognitive trust (CT) and the first principal component of emotional violation (EV) towards the first principal component of repurchase intention (RI), including the control variables age, education, income, and pre-breach attitude. The adjusted R² for the regression model is 0.336, meaning that 33.6% of the variance of repurchase intention is accounted for by the whole model. The table also shows that the independent variables reliably predict the dependent variable, as the F-statistic scores a significant result.

4.5.1 Hypothesis 1

The results in table 5 show a β of 0.357 and a p-value of 9.24e-06 for the relationship between the first factor of cognitive trust and repurchase intention. The relationship between the second factor of cognitive trust and repurchase intention has a β of 0.210 and a p-value of 0.048. As there is a significant relationship found between the first factor of CT and RI and a smaller significant relationship (on the significance level of 5%) between the second factor of CT and RI, there is enough evidence to support H1. Accordingly, it can be said that cognitive trust is positively related to repurchase intention after reading a DBA.

4.5.2 Hypothesis 2

For the relationship between emotional violation and repurchase intention, table 5 shows a β of -0.346 and a p-value of 1.26e-05. There is enough evidence to support H2, as there is a significant relationship found between emotional violation and repurchase intention. Accordingly, it can be said that emotional

violation is negatively related to repurchase intention after reading a DBA.

Table 5 – Regression results

Variables	Coefficient	SE	Significance
(Constant)	0.140	1.559	0.928
Independent variables			
CT (PC1)	0.357	0.078	9.24e-06 ***
CT (PC2)	0.210	0.105	0.048 *
EV (PC1)	-0.346	0.077	1.26e-05 ***
Control variables			
18 – 24	-0.950	0.499	0.059 .
25 – 34	-0.926	0.564	0.103
35 – 44	-1.126	0.641	0.081 .
45 – 54	-1.163	0.579	0.046 *
55 – 65	-0.908	0.757	0.232
Over 65	-0.475	0.870	0.586
Lower secondary education	1.677	0.802	0.038 *
Upper secondary education	0.103	0.724	0.887
Bachelor's degree	0.724	0.721	0.317
Master's degree	0.892	0.758	0.241
PhD	0.120	1.131	0.916
Other education	1.439	1.211	0.237
€1.000 – €1.500	0.163	0.376	0.664
€1.501 – €2.000	-0.059	0.362	0.870
€2.000 – €2.500	-0.416	0.390	0.289
€2.501 – €3.000	-0.170	0.444	0.702
Over €3.000	-0.393	0.428	0.360
Positive pre-breach attitude	0.363	1.361	0.790
Neutral pre-breach attitude	0.049	1.379	0.972
Negative pre-breach attitude	0.514	1.639	0.754
Fit statistics			
Residual standard error: 1.334 on 149 DF			
R-squared: 0.423			
Adjusted R-squared: 0.336			
F-statistic: 4.78 on 23 and 149 DF			

***, **, * and . coefficients are statistically significant at 0.001, 0.01, 0.05 and 0.1, respectively.

4.6 Control variables

Regarding the control variables, age and education show a small significance. To be specific, the age group from 18 to 24 shows a significant result on the significance level of 10% with a β of -0.950 and a p-value of 0.059. The age group of 35 to 44 shows a significant result on the significance level of 10% as

well and has a β of -1.126 and a p-value of 0.081. The age group from 45 to 54 shows a significant result on the significance level of 5% (β = -1.163, p = 0.046). Lastly, the education level of lower secondary education shows a significant result on the significance level of 5% with a β of 1.677 and a p-value of 0.038, meaning that for every point increase in the education level of lower secondary education, repurchase intention will increase with 1.677.

4.7 Summary of the results

The Shapiro-Wilk test in the first step of the analysis indicated that none of the variables were normally distributed. Therefore, Spearman's Rank Order was used as the method to calculate the correlations of the variables. All three variables scored a Cronbach's Alpha of 0.7 or higher. Emotional violation scored a 0.81, cognitive trust a 0.7 and repurchase intention a 0.83. The Kaiser-Meyer-Olkin test indicated that sampling adequacy was detected as the independent variables scored both a 0.7 and the dependent variable repurchase intention scored a 0.73. The result of the principal component analysis determined which components were used to perform the regression analysis. For both emotional violation and repurchase intention, PC1 was used for the regression analysis as this component had an eigenvalue higher than one. Cognitive trust had two components with an eigenvalue higher than one, so for this variable, PC1 and PC2 were considered during the regression. The regression analysis showed significant results for the relationship between cognitive trust and repurchase intention. Therefore, there was enough evidence to support H1. There were also significant results found for the relationship between emotional violation and repurchase intention. Accordingly, there was enough evidence to support H2.

5. DISCUSSION

The goal of this research was to assess the relationship between two vulnerability perceptions, cognitive trust and emotional violation, and repurchase intention, in the context of a data breach. To reach this objective, the research question has been split up into two sub-questions in the form of hypotheses.

For the first hypothesis, "*Cognitive trust will be positively related to repurchase intention after reading a DBA.*" significant results were found during the regression analysis. The correlation matrix also indicated that cognitive trust is positively correlated with repurchase intention. This means that people with a high degree of cognitive trust are more likely to repurchase a product or service after reading a DBA. This conclusion is in line with the literature (Li et al., 2022; Dinev et al., 2006). Li et al. (2022) found that when the transactional context is perceived as riskful and uncertain, trust is an important element for customer retention and loyalty behaviour. As repurchase intention is a type of loyalty behaviour, this supports the findings of this research. In addition, Dinev et al. (2006) also stated that transactional behaviours can be a result of a beneficial factor like trust.

The second hypothesis, "*Emotional violation will be negatively related to repurchase intention after reading a DBA.*" was also supported as the regression analysis showed significant results for this relationship. Next to this, the correlation matrix showed that emotional violation is negatively correlated with repurchase intention. This means that people with a high degree of emotional violation are less likely to repurchase a product or service after reading a DBA. This finding is, like the first hypothesis, in accordance with the literature (Choi et al., 2016). Prior research done by Choi et al. (2016) already found that feelings of violation have significant effects on post-incident outcomes like post-word-of-mouth and post-switching behaviour. As switching from products and/or brands

automatically means that the initial product or service will not be purchased again, this finding is in line with the results obtained in the research of this thesis.

The study also showed that, of the selected control variables, age and education appear to have a small significant effect on repurchase intention. The age group of 45-54 in particular has a negative effect on repurchase intention. The education category lower secondary education appears to have a small positive effect on repurchase intention. The other two control variables, income and pre-breach attitude, showed no abnormalities.

6. CONCLUSION

The central question of this research was, “*What is the effect of cognitive trust and emotional violation on repurchase intention after reading a DBA?*”. The result of the study shows that emotional violation has a negative and significant effect on repurchase intention and that cognitive trust has a positive and significant effect on repurchase intention. This suggests that, in a data breach context, a high level of cognitive trust increases a customer’s intention to buy the product or service again in the future. On the other hand, customers who have very strong feelings of violation towards the seller of the product or service, are less likely to buy that product or service again. This conclusion emphasizes the relevance of ensuring the integrity and confidentiality of customer data as this could potentially lead to reduced repurchase intentions.

To conclude this thesis, some theoretical and practical implications of this study will be discussed below in section 6.1. In addition, limitations and recommendations for future research will be mentioned in section 6.2.

6.1 Implications

In terms of theoretical implications, in the existing literature about data breaches, Chakraborty et al. (2016) have previously conducted research into the effect of feelings of emotional violation on customer behaviour, such as post-WOM or post-likelihood of switching. Because this study investigated another type of customer behaviour, repurchase intention, as a dependent variable, it is a valuable addition to the existing literature. Since understanding customer behaviour helps to make important decisions in the workplace, it is all the more important that different types of customer behaviour are examined. The relationship between cognitive trust and repurchase intention has been researched before (Dinev et al., 2006; Li et al., 2022). However, to the best of my knowledge, this research holds academic relevance as it has not yet been studied in the setting of a data breach. Next to this, the CIA triad has been used as one of the theories for this research. Normally, this theory is mainly used in the literature about information security systems. By using this theory in combination with marketing-oriented research and distinguishing between different types of data breaches, the theory helps to better understand customer behaviour. This makes it easier to investigate whether customers have different reactions to different types of data breaches. This study has already made a start by examining the confidentiality aspect in combination with the integrity aspect of the CIA triad. Finally, this research has addressed the suggestion of Schlackl et al. (2022) to research the effect of data breaches on the customers that were involved in it and to do research with non-U.S. data sets.

From a managerial perspective, the aim of this research was not to generate a specific approach that suggests how to anticipate the happening of a data breach or how to act if a data breach has occurred. Nevertheless, this research does show that, because of the significant results, it is all the more important that

companies start to delve into the field of data security. By being able to assure customers of the confidentiality and integrity of their data and by knowing how to act in the event of a data breach, the impact of vulnerability perceptions on repurchase intention can be minimised. As a result, fewer long-term relationships with customers are likely to be compromised or lost. Since Netflix is a large and well-known streaming service, the managerial implications also apply to similar companies such as Amazon Prime Video or Disney+. These streaming services mainly depend on online data and are, therefore, particularly vulnerable to cyber security threats such as data breaches.

6.2 Limitations and future research

This study has some limitations. Firstly, everyone who was familiar with the company Netflix was included in the final sample. This does not take into account who was the person who actually paid for the subscription, since it is a subscription that you can share with several (family) members. The individual who pays for the subscription has more personal information that can leak, including details such as bank account number and email address, in comparison to the rest of the people with whom the subscription is shared. If the conditions for the sample were to be restricted to only members who are paying for the subscription, this would have led to a sample size that was too small. This choice could lead to different results as there might be underlying differences. Therefore, it would be interesting to investigate this in the future for a larger sample. Next to this, a more diverse sample is also advised. The sample that was used for this study consisted for more than fifty per cent of people in the age group of 18-24. This can be considered a limitation as it is not representative. Another limitation of this research is that it limits the generalizability of the results, as only the people who were familiar with Netflix were included in the sample. It is, therefore, not possible to say that the results will be the same for other types of companies and/or industries.

As a recommendation for future research, a similar study can be done for another industry to see if there are any differences between the results. In addition, only two of the three aspects of the CIA triad were included in this study. The data breach announcement related to confidentiality and integrity, but availability was not taken into account. Future research could examine only this last aspect or conduct a study in which respondents read a data breach announcement that pertains to the entire CIA triad. Finally, the personal network and the network that was reached via social media mainly consisted of Dutch people. Schlackl et al. (2022) recommended in prior literature to make use of non-US datasets for future research; that recommendation was listened to in this study. However, as the findings of this study cannot be generalised to other cultures, this would be a good starting point to investigate whether there are different results between different cultures within Europe and then compare them with studies already done in the US.

7. ACKNOWLEDGEMENTS

Finally, I would like to express my gratitude to my supervisors Dr. A. Leszkiewicz and Dr. L. Alvino, who helped me during the process of writing this thesis. I would like to thank them for their enthusiasm, guidance, critical view, and helpful comments during the course of this research. Secondly, I would like to thank all the participants who completed the survey for their efforts and contributions that enabled me to conduct this research. Finally, I would like to express my gratitude to my family and friends who have supported me throughout my whole studies.

8. REFERENCES

- Afroz, S., Islam, A. C., Santell, J., Chapin, A. L., & Greenstadt, R. (2013). How Privacy Flaws Affect Consumer Perception. *IEEE Computer Security Foundations Symposium*, 10–17. <https://doi.org/10.1109/stast.2013.13>
- Alshehri, M., & Panda, B. (2020). Minimizing Data Breach by a Malicious Fog Node within a Fog Federation. *International Conference on Cyber Security and Cloud Computing*, 36. <https://doi.org/10.1109/cscloud-edgecom49738.2020.00016>
- Bhalme, A., Pawar, A., Borkar, A., & Shriram, P. (2022). Cyber Attack Detection and Implementation of Prevention Methods For Web Application. *2022 IEEE Bombay Section Signature Conference (IBSSC)*. <https://doi.org/10.1109/ibssc56953.2022.10037431>
- Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*, 83, 47–56. <https://doi.org/10.1016/j.dss.2015.12.007>
- Choi, B. C. F., Kim, S. S., & Jiang, Z. (2016). Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior. *Journal of Management Information Systems*, 33(3), 904–933. <https://doi.org/10.1080/07421222.2015.1138375>
- Culnan, M. J., & Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1), 104–115. <https://doi.org/10.1287/orsc.10.1.104>
- Dangelico, R. M., Alvino, L., & Fraccascia, L. (2022). Investigating the antecedents of consumer behavioral intention for sustainable fashion products: Evidence from a large survey of Italian consumers. *Technological Forecasting and Social Change*, 185, 122010. <https://doi.org/10.1016/j.techfore.2022.122010>
- Dawson, G. S., Karahanna, E., & Buchholtz, A. (2014). A Study of Psychological Contract Breach Spillover in Multiple-Agency Relationships in Consulting Professional Service Firms. *Organization Science*, 25(1), 149–170. <https://doi.org/10.1287/orsc.2013.0834>
- Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Dölarıslan, E. Ş. (2014). Assessing the effects of satisfaction and value on customer loyalty behaviors in service environments. *Management Research Review*, 37(8), 706–727. <https://doi.org/10.1108/mrr-06-2013-0152>
- European Commission. (2016). *What is a data breach and what do we have to do in case of a data breach?* https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-to-do-in-case-of-a-data-breach_en
- Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services. *Omega*, 32(6), 407–424. <https://doi.org/10.1016/j.omega.2004.01.006>
- Girden, E. R., & Kabacoff, R. (2010). *Evaluating Research Articles From Start to Finish* (3rd ed.). SAGE Publications, Inc.
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19(1), 33–56. <https://doi.org/10.3233/jcs-2009-0398>
- Hellier, P. K., Geursen, G., Carr, R., & Wilkoff, B. L. (2003). Customer repurchase intention. *European Journal of Marketing*, 37(11/12), 1762–1800. <https://doi.org/10.1108/03090560310495456>
- Hoehle, H., Wei, J., Schuetz, S., & Venkatesh, V. (2021). User compensation as a data breach recovery action: a methodological replication and investigation of generalizability based on the Home Depot breach. *Internet Research*, 31(3), 765–781. <https://doi.org/10.1108/intr-02-2020-0105>

- Janakiraman, R., Lim, J. S., & Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing*, 82(2), 85–105. <https://doi.org/10.1509/jm.16.0124>
- Kaiser, H. F., & Rice, J. P. (1974). Little Jiffy, Mark Iv. *Educational and Psychological Measurement*, 34(1), 111–117. <https://doi.org/10.1177/001316447403400115>
- Lewicki, R. J., & Bunker, B. B. (1996). Developing and Maintaining Trust in Work Relationships. *SAGE Publications, Inc. eBooks*, 114–139. <https://doi.org/10.4135/9781452243610.n7>
- Li, C., & Tsai, M. (2022). What makes guests trust Airbnb? Consumer trust formation and its impact on continuance intention in the sharing economy. *Journal of Hospitality and Tourism Management*, 50, 44–54. <https://doi.org/10.1016/j.jhtm.2021.12.001>
- Lu, B., & Yi, X. (2023). Institutional trust and repurchase intention in the sharing economy: The moderating roles of information privacy concerns and security concerns. *Journal of Retailing and Consumer Services*, 73, 103327. <https://doi.org/10.1016/j.jretconser.2023.103327>
- Malhotra, A., & Malhotra, C. K. (2011). Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. *Journal of Service Research*, 14(1), 44–59. <https://doi.org/10.1177/1094670510383409>
- 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>
- Mohammed, Z. A., & Tejay, G. P. (2018). How to Compensate After a Data Breach? Investigating Compensation Types and Role of Fairness in Customer Repatronage Intentions. *The DATA BASE for Advances in Information Systems*, 54(1), 110–127. <https://doi.org/10.13140/RG.2.2.10046.77128>
- Morrison, E. W., & Robinson, S. L. (1997). When Employees Feel Betrayed: A Model of How Psychological Contract Violation Develops. *Academy of Management Review*, 22(1), 226–256. <https://doi.org/10.5465/amr.1997.9707180265>
- Muhammad, N. B. (2019). Nasn: A Novel Approach For Securing Network From Malware Injection. *International Journal of Scientific & Technology Research*, 8(11), 2517–2531. <https://www.ijstr.org/paper-references.php?ref=IJSTR-1019-23364>
- Muzatko, S., & Bansal, G. (2020). Consumer Skepticism as it Relates to E-Commerce Data Breaches and Company Efforts to Enhance Trust. *Proceedings of the Fifteenth Midwest Association for Information Systems Conference*, 1–5.
- Nunnally, J. C. (1978). *Psychometric Theory: McGraw-Hill series in psychology* (2nd ed.). McGraw-Hill.
- Ponemon Institute. (2019). *Cost of a Data Breach Report 2019*. <https://www.ibm.com/downloads/cas/RDEQK07R>
- Ponemon Institute. (2020). *Cost of a Data Breach Report 2020*. <https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf>
- Rasoulia, S., Grégoire, Y., Legoux, R., & Sénécal, S. (2021). The Effects of Service Crises and Recovery Resources on Market Reactions: An Event Study Analysis on Data Breach Announcements. *Journal of Service Research*, 26(1), 44–63. <https://doi.org/10.1177/10946705211036944>
- Robinson, S. L., & Rousseau, D. M. (1994). Violating the psychological contract: Not the exception but the norm. *Journal of Organizational Behavior*, 15(3), 245–259. <https://doi.org/10.1002/job.4030150306>
- Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). Research methods for business students. In *Pearson eBooks* (8th ed.). Pearson Education, Limited. <http://dspace.uniten.edu.my/handle/123456789/18304>
- Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, 59(4), 1–15. <https://doi.org/10.1016/j.im.2022.103638>

- Tripathi, M., & Mukhopadhyay, A. (2020). Financial Loss due to a Data Privacy Breach: An Empirical Analysis. *Journal of Organizational Computing and Electronic Commerce*, 30(4), 381–400. <https://doi.org/10.1080/10919392.2020.1818521>
- U.S. Government Publishing Office. (2015). Title 44 - Public Printing and Documents. In *U.S. Government Publishing Office*. <https://www.gpo.gov/docs/default-source/congressional-relations-pdf-files/uscode-2015-title44.pdf>
- Vinton, K. (2014, September 18). With 56 Million Cards Compromised, Home Depot's Breach Is Bigger Than Target's. *Forbes*. <https://www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets/?sh=48d032d63e74>
- Wang, S., & Huff, L. (2007). Explaining buyers' responses to sellers' violation of trust. *European Journal of Marketing*, 41(9/10), 1033–1052. <https://doi.org/10.1108/03090560710773336>
- Xie, Y., & Peng, S. (2009). How to repair customer trust after negative publicity: The roles of competence, integrity, benevolence, and forgiveness. *Psychology & Marketing*, 26(7), 572–589. <https://doi.org/10.1002/mar.20289>
- Xu, J., Song, H., & Prayag, G. (2023). Using authenticity cues to increase repurchase intention in restaurants: Should the focus be on ability or morality? *Tourism Management Perspectives*, 46, 101102. <https://doi.org/10.1016/j.tmp.2023.101102>

9. APPENDIX

9.1 Normality

Table 6 – Shapiro-Wilk test

	Shapiro-Wilk test	
	Statistic	Significance
Cognitive trust	0.955	2.139e-05
Emotional violation	0.980	0.01534
Repurchase intention	0.905	4.27e-09

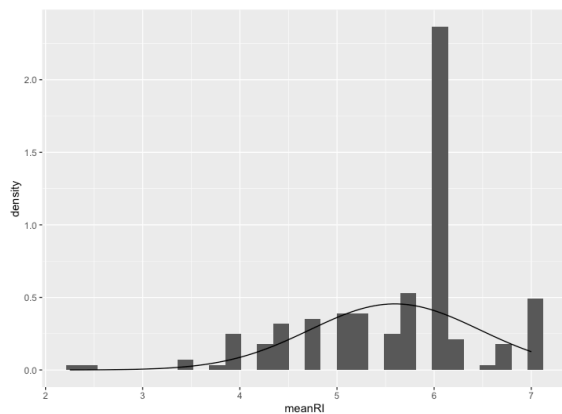


Figure 4a – Histogram repurchase intention

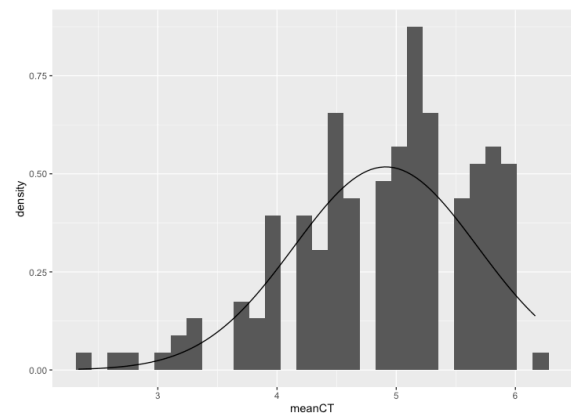


Figure 4b – Histogram cognitive trust

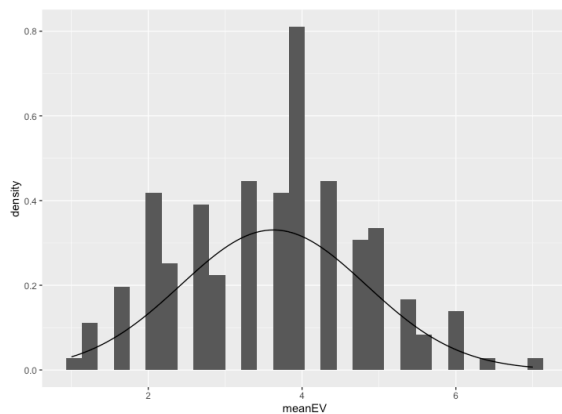


Figure 4c – Histogram emotional violation

9.2 Kaiser-Meyer-Olkin test

Table 7a – KMO test cognitive trust

Cognitive trust	
Overall MSA	0.7
MSA for each item	
CT1	0.77
CT2	0.65
CT3	0.69
CT4	0.67
CT5	0.74
CT6	0.68

Table 7b – KMO test emotional violation

Emotional violation	
Overall MSA	0.7
MSA for each item	
EV1	0.75
EV2	0.66
EV3	0.71

Table 7c – KMO test repurchase intention

Repurchase intention	
Overall MSA	0.73
MSA for each item	
RI1	0.76
RI2	0.70
RI3	0.74
RI4	0.72

9.3 Principal component analysis**Table 8a – PCA for cognitive trust**

Component	Standard deviation	Eigenvalue	% of variance	Cumulative %
1	1.583	2.507	41.787	41.787
2	1.085	1.177	19.615	61.402
3	0.900	0.810	13.493	74.895
4	0.755	0.570	9.497	84.392
5	0.725	0.525	8.757	93.149
6	0.641	0.411	6.851	100.000

Table 8b – PCA for emotional violation

Component	Standard deviation	Eigenvalue	% of variance	Cumulative %
1	1.476	2.178	72.610	72.610
2	0.692	0.479	15.978	88.588
3	0.585	0.342	11.412	100.000

Table 8c – PCA for repurchase intention

Component	Standard deviation	Eigenvalue	% of variance	Cumulative %
1	1.637	2.681	67.019	67.019
2	0.875	0.765	19.128	86.147
3	0.563	0.317	7.918	94.065
4	0.487	0.237	5.935	100.000

Table 9a – Rotated component matrix for cognitive trust

Item	PC1	PC2	PC3	PC4	PC5	PC6
CT1	-0.435	0.285	-0.367	0.528	-0.527	-0.197
CT2	-0.365	0.535	0.391	0.035	0.507	-0.411
CT3	-0.459	0.301	-0.354	-0.394	0.160	0.626
CT4	-0.321	-0.584	-0.421	0.227	0.541	-0.188
CT5	-0.451	-0.318	0.145	-0.619	-0.374	-0.390
CT6	-0.400	-0.317	0.624	0.362	-0.085	0.461

Table 9b – Rotated component matrix for emotional violation

Item	PC1	PC2	PC3
EV1	0.559	-0.781	-0.279
EV2	0.597	0.146	0.789
EV3	0.575	0.608	-0.548

Table 9c – Rotated component matrix for repurchase intention

Item	PC1	PC2	PC3	PC4
RI1	0.523	-0.339	0.640	-0.448
RI2	0.528	-0.389	-0.116	0.746
RI3	0.542	0.092	-0.706	-0.445
RI4	0.391	0.852	0.279	0.211

9.4 Correlation

Table 10 – Correlation

	RI (PC1)	CT (PC1)	CT (PC2)	EV (PC1)	Age	Education	Income	PBA
RI (PC1)	1.000							
CT (PC1)	0.42 ***	1.000						
CT (PC2)	0.17 *	-0.01	1.000					
EV (PC1)	-0.38 ***	-0.24 ***	0.12	1.000				
Age	-0.11	0	-0.07	0.01	1.000			
Education	0.04	0.1	0.06	0.04	0.08	1.000		
Income	-0.09	-0.09	-0.03	0	0.66 ***	0.22 **	1.000	
PBA	0.24 **	0.27 ***	0.26 ***	0.03	0.08	0.06	0.08	1.000

***, ** and *. Correlation is statistically significant at 0.001, 0.01 and 0.05, respectively (two-tailed)

9.5 Survey

Thank you for participating in this study. In this study, we are interested in people's attitudes towards their personal data. The survey will take approximately 5-10 minutes and the results will remain anonymous.

By continuing the survey, you agree to participate in this study. If you wish, you may withdraw from this research at any time. Your data will be used for scientific and educational purposes only.

If you have any questions, please reach out to:

Lauren van Leussen
l.vanleussen@student.utwente.nl

- Agree
 - Disagree
-

Are you 16 years or older?

- Yes
 - No
-

For this study, a hypothetical case from Netflix will be used. Netflix is one of the world's leading entertainment services with over 232 million paid memberships in over 190 countries enjoying TV series, films and games across a wide variety of genres and languages. Before reading the case, some Netflix-related questions are asked. Please answer these questions and then continue the survey.

Are you familiar with Netflix?

- Yes
 - No
-

Have you watched movies and/or series via Netflix?

- Yes
 - No
-

Do you currently have access to a Netflix account?

- Yes
 - No
-

Are you the person that pays for the Netflix subscription?

- Yes
 - No
-

Are you involved in the decision-making process of continuing/repurchasing the subscription?

- Yes
 - No
-

Generally speaking, are you currently satisfied with the Netflix subscription?

- Yes
 - Neutral
 - No
-

Below you will read a hypothetical data breach announcement about Netflix. As you read this announcement, imagine that you are currently a customer of Netflix and that the announcement also involves your personal data. Read the announcement carefully and then proceed to the next page.

Netflix hit by a cyber-attack

PR Newswire

May 17, 2023 Wednesday 4:30 PM EST

Announcement

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

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

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

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

Please indicate your level of agreement with the following statements on cognitive trust (from 1 = "strongly disagree" to 7 = "strongly agree"):

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
Generally speaking, I trust Netflix.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Generally speaking, Netflix is dependable.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Generally speaking, Netflix is reliable.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I will buy Netflix' products when I want to watch movies and/or series.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am willing to recommend Netflix to my relatives and friends.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I am willing to try new products introduced by Netflix.

Please indicate your level of agreement with the following statements on emotional violation (from 1 = “strongly disagree” to 7 = “strongly agree”):

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
I feel extremely frustrated by how my data was treated by Netflix.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The more I think about it, the more hostile I feel towards Netflix.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel a great deal of anger towards Netflix.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please indicate your level of agreement with the following statements on repurchase intention (from 1 = “strongly disagree” to 7 = “strongly agree”):

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
I intend to use Netflix again.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I intend to continue using Netflix on a regular basis.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
In the short term, I will use Netflix again.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
In the long term, I will use Netflix again.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To conclude, we ask you to answer three sociodemographic related questions.

Please select your age range:

- Under 18
 - 18 - 24
 - 25 - 34
 - 35 - 44
 - 45 - 54
 - 55 - 65
 - Over 65
-

Please select your highest level of education:

- Primary education
 - Lower secondary education
 - Upper secondary education
 - Bachelor's degree
 - Master's degree
 - PhD
 - Other, please explain:
-

Please select your monthly income range:

- Less than €1.000
- €1.000 – €1.500
- €1.501 – €2.000
- €2.001 – €2.500
- €2.501 – €3.000
- Over €3.000

9.5.1 Scales

Table 11 – Scales

	Items
<hr/>	
Please indicate your level of agreement with the following statements on cognitive trust (from 1 = “strongly disagree” to 7 = “strongly agree”):	
Cognitive trust (adapted from Xie et al., 2009)	Generally speaking, I trust Netflix. Generally speaking, Netflix is dependable. Generally speaking, Netflix is reliable. I will buy Netflix’ products when I want to watch movies and/or series. I am willing to recommend Netflix to my relatives and friends. I am willing to try new products introduced by Netflix.
Please indicate your level of agreement with the following statements on emotional violation (from 1 = “strongly disagree” to 7 = “strongly agree”):	
Emotional violation (adapted form Choi et al., 2016)	I feel extremely frustrated by how my data was treated by Netflix. The more I think about it, the more hostile I feel towards Netflix. I feel a great deal of anger toward Netflix.
Please indicate your level of agreement with the following statements on repurchase intention (from 1 = “strongly disagree” to 7 = “strongly agree”):	
Repurchase intention (adapted from Xu et al., 2023; Lu et al., 2023)	I intend to use Netflix again. I intend to continue using Netflix on a regular basis. In the short term, I will use Netflix again. In the long term, I will use Netflix again.
