Perception of Data Security in e-Commerce

by Felix Balzer and Bastian Bollig
255513, 254940

Hochschule Furtwangen University

Course of Studies
International Management M.Sc.

Lecture
Project Report

Professor
Prof. Dr. Lars Binckebanck

Contents

1. Abstract

In this paper, different factors influencing the perceived data security (PDS) of online shoppers are analyzed. For this purpose, the authors first conduct a literature review and later analyze the results of an empirical study, by applying a regression analyses. Based on the findings of this research, the paper identified the frequency of gathering information on the topic of data security and the experience of being hacked as factors with a significant negative impact on PDS. In addition, a well perceived benefit and, in special cases, an e-Commerce business' brand can positively influence PDS of customers. In conclusion, the paper delivers insights into the perceptions of data security and delivers some suggestions on how a company could improve the PDS of their customers.

2. Introduction

Since the invention of the first personal computer in 1981 (IBM, 1981), both technology as well as its' applications have seen constant improvements over the years. Innovation in both hard- and software results in more powerful, efficient and versatile machines on a regular basis and make the computer one of the most useful instruments for almost every imaginable application. Today, we have reached a point in time, where almost every task relies on the help of computers. Furthermore, most of these tasks also require connectivity to the internet. Exactly this generates valuable data which many companies seek to gather for analyzing them.

Having started with mainly statistical methods and databases in the 1970s, development moved further to first data mining techniques enabling clustering and segmentation of data, first regression analysis and modelling functions. Later, when computers went online, the utility of them increased drastically, as this was the starting point for any online research about products, companies or industries. Adding social media brought internet users' interaction into place which again enlarged the amount of data available. Soon, companies recognized the great potential in this huge amount of data, known as Big Data. Finally, the introduction of mobile devices and the

usage of applications and mobile online services revealed information about individual people which has hardly been available for companies before. Providers of an application (e.g. an e-Commerce application) could collect information about an individual's current location, contact lists, pictures saved on the mobile devices and other context relevant topics. Companies could easily track what the market was talking about by using applications and social media, so market intelligence is becoming crucial for e-Commerce companies. Mobile devices completed the evolution from Business Analytics 1.0 established in the 1970s to Business Analytics 3.0. (Chen, Chiang, & Storey, 2012).

Billions of people use those applications, social media and many other online services every day, knowing that they generate user specific data which can be used for commercial purposes. However, there is a misconception between the security people attribute to being online using all these services and reality. Data breaches are much more frequent than publicly assumed, whether a single person is affected or a company finds itself being hacked and facing a loss of millions of datasets (Rashid et al., 2017).

This research builds upon the proven connection between trust and expertise about how to use an online service and customer behavior (Oliveira, Alhinho, Rita, & Dhillon, 2017). Specifically, this paper focuses on e-Commerce services. As students in field of Business Management, we find our research to be value-adding to the field, as the impact of e-Commerce users' knowledge about computer security in general in relation with their perception of data security, a field on which very little scientific research exists, is analyzed. This includes the extent of each individual's ability to operate a computer, knowledge about security certifications in the e-Commerce industry and the amount of information about data security consumed.

We now proceed by explaining the methodology used and presenting the hypothesis tested. Thereafter, we give an overview of the current state of literature and close with the presentation of the research results.

3. Methodology

In the following, the methodology applied for this research is described. It is based on literature review, serving as a basis for a survey out of which we later constructed a regression model analysis of the findings.

Literature review

For the literature review, a variety of different academic journal articles covering a range of topics was collected. The articles discuss proceedings in computer technology, psychological traits of human perception, the interface between humans and computers as well as marketing topics. Combining more than two fields of research was necessary, as this study aims at analyzing individual's perception about data security in an online environment, more specifically focusing on e-Commerce. Besides academic journals, the research also relies on findings from previous research conducted by leading technology consulting companies focusing on data security in different industries as well as statistical data obtained by various organizations.

Based on the findings of the literature review, different variables and the operationalizing items for a survey were concluded combining findings from different fields.

Survey design

The survey included closed-end questions which could be answered in a multiple-choice setting. The survey was conducted in two languages (English and German) to increase the number of potential participants, yielding 303 useable datasets, with a population largely consisting out of students under the age of 34. As social media usage was identified as an important component to consider in this research, more details will be discussed in the literature review section, and adding the fact that the sample mainly consisted of students, it can be assumed, that a majority of our sample uses social media (Pempek, Yermolayeva, & Calvert, 2009).

Based on the literature, the survey aims at collecting information about the impact of the following variables on individual's perception of data security. First, the survey asks for each participant's proficiency regarding computer security as the belief in one's own ability to perform advanced tasks on a computer affects the extent to which people are willing to try out and use new software or services. Perceived ease of use, credibility and usefulness are dependent on one's belief in his or her individual skills in operating a computer (Wang, Wang, Lin, & Tang, 2003)

As the time when computers were the only devices which could access e-Commerce platforms lies long in the past, the increasing importance of mobile devices for using online shopping services must be respected (Stephen, 2016). As data which is being sent via mobile internet connections is usually not encrypted, barriers to prevent taping and unwanted storage of personal data are low and easily surpassed by cyber criminals. We therefore argue, that the number of transactions containing sensitive data (e.g. e-payments) made via a mobile device, like a smartphone or tablet, is an indication for perceived data security, as such a transaction implies a strong feeling of security while being online and consequently a lower degree of concern for data security.

Shrum (2002) argues, that presented information affect the accessibility of mental constructs used for judgments and that personal experiences have a much greater impact compared to presented information through media on the accessibility of mental constructs. This will be discussed further in the literature review. Because of this finding, an item asking for personal experiences with data breaches was introduced, followed by asking how such an experience has changed the consumer behavior of participants. So, the consumption of information via channels like digital, social or traditional media and potential experiences of participants form the second and third main variable.

Like physical marketplaces, digital marketplaces and online environments offer a variety of different products or services from many different vendors, those vendors typically are not identical, even if they sell the same product. These usually differ based on product or service quality, after-sales services, different warranty conditions

and their style of advertisement. If the individual features of a vendor are in line with the customer's expectations, it these features give the vendor a competitive advantage with respect to this specific customer. Peres, Shachar & Lovett (2013) found that brands and word-of-mouth generation are closely related and that there are differences between offline and online word-of-mouth. Especially in online environments, word-of-mouth about a brand can be influential on the brand's performance, as information gathered by social media has an effect on customer behavior depending on the level of the customer's social media self-efficacy, which affects the perceived trustworthiness of the respective information (Hocevar, Flanagin, & Metzger, 2014). In conclusion, the research investigates whether there are differences in the perceived trustworthiness of the ten most successful e-Commerce vendors in Germany. This investigation is in line with the study of Liu & Hung (2010) who showed that a customer's perception of a virtual environment affects customer loyalty.

Finally, with this study we aim to find out more about customer's willingness to share personal data to gain a benefit. The willingness to trade private information for a return is dependent on the level of trust a customer has in a specific e-Commerce platform. This pattern was shown in the banking and insurance industry. Interestingly, the same study revealed a large misconception on the customer side. Banks and insurances are subject of data breaches much more frequently compared to what their customers think (Rashid et al., 2017). Therefore, customer willingness to trade private data for a benefit is analyzed by proposing a set of different potential benefits and let participants indicate their individual probability of concluding the trade.

Statistical Model

The statistical model we applied is linear regression with multiple variables, as described above. The regression function denotes as followed:

$$Y = \beta_0 + \beta_1 Expt + \beta_2 InfoCon + \beta_3 Trust + \beta_4 Benf + \beta_5 Exp + u_o$$

Where β_0 is the regression model constant, β_1 to β_5 are the coefficients of each variable, *Expt* is the operationalization of the participant's expertise, *InfoCon* is the

operationalization of the participant's consumption of information about data security from different sources, Trust contains the operationalization of participant's perception of trustworthiness of the ten most successful online shops in Germany, *Benf* indicates the participant's willingness to trade personal data in exchange for a benefit, *Exp* shows whether a participant experiences a data breach or has been hacked and how this experience changed his or her online shopping behavior and u_o denotes an error term.

Based on the following literature review, the following hypothesis have been derived and tested.

> H1: The level of expertise a person has regarding computer security is negatively related to this person's perception of data security while being online.

> H2: The accumulated amount of information a person consumes about data security, affects his/her degree of perceived data security negatively.

> H3: The personal experience of having been hacked, lowers one's perceived data security.

> H4: The brand reputation of an e-Commerce platform influences one's perception of data security positively.

> H5: Customers are more willing to share personal data if they are offered a benefit.

The survey contained answer in text format, so the results needed to be coded and transformed into numbers. Inspired by Bloom, Sadun & Van Reenen (2010), Z-scores of the transformed survey results are used to ensure comparability among variables. The results of the regression are presented in the results section.

4. Literature review

To give an overview on the current state of research on the topic of perceived data security and online shopping, we will analyze existing literature in three large categories: trust, expertise and media consumption.

The role of Trust in e-Commerce

Trust and retail have always been closely related topics, and rightfully so. The concept of trust is something immensely important in a consumer-retailer relationship, especially in an online market environment (Huang & Tsui, 2016; Isbrucker, 2015; Oliveira et al., 2017). The first step in understanding the role of trust in e-Commerce, is understanding the concept of trust in general. In reality though, this task is easier said than done. The concept of trust is very abstract and hard to define precisely. Depending on the situation, the context and the people one asks, the factors defining trust change dramatically (Chen & Dhillon, 2003). So, it would be more appropriate to say, it is important to understand, how trust is defined as part of this research. Based on our literature review, a concept of trust based on three dimensions seems the most widely agreed on, in the context of a customer to online retailer relationship. Competence, Integrity and Benevolence combined into one concept yield in overall trust (Chen & Dhillon, 2003; Fang et al., 2014; Oliveira et al., 2017). Oliveira (2003) further describes the three dimensions as follows: Competence is a "companies' ability to fulfil promises made to the consumer", Integrity measures how "consistent, reliable and honest" a firm is and Benevolence is the level to which a retailer holds the consumers' interest above its own.

The next question is, why should trust be important at all? Where is the link to something measurable for an e-Commerce business? The answer is best divided into two steps: The intention to purchase and the intention to purchase again.

The first part of the answer is quite simple: the purchase intention. Without an intention to purchase a product, a consumer will not purchase that product, and without a purchase, there can be no revenue, without which, any shop will cease to exist. Trust, according to research, accounts for 57.5% of all online purchase intentions

(Oliveira et al., 2017), meaning it is incredibly important factor for creating revenue in the e-Commerce market.

This becomes even more evident, when considering one of today's most important concepts in e-Commerce is customer retention. A concept, tightly woven with any research into e-Commerce related topics, as the question how to convert a one-time shopper into a returning customer has occupied the minds of many researchers since the dawn of the online shopping age (Fang et al., 2014; Pavlou, 2002). According to a model by Willem Isbrucker (2015), trust is one of the three main influencers on a customer's intention to form a relationship with an e-Commerce business, the other two being perceived switching costs and satisfaction. The three are also interrelated, meaning high perceived switching costs influence satisfaction negatively, while increased satisfaction has a positive effect on trust and vice versa. In addition to satisfaction, perceived shopping risk and perceived relationship investment are described as the two main influencers on trust in this context. Isbrucker (2015) concludes, that in order to increase the chance of retaining customers, high levels of trust and satisfaction paired with a low level of switching costs is important.

Humans tend to be wary of whom they want to share information like their name, credit card number or home address with. For online retailing, this obviously poses a challenge, as any e-Commerce store needs their customers payment information, names, addresses and other personal data to process a transaction. In other words, in order to do business and produce a revenue, an e-Commerce website needs their potential customers trust (Flavián, Guinalíu, & Gurrea, 2006; Kim & Peterson, 2017; Rashid et al., 2017). In this sense, based on the literature review, we argue that trusting a company enough to hand them personal data, should also have an influence on the perception of data security. Or in other words, we believe, that the factor of trust has an impact on ones perceived data security when shopping online (López-Miguens & Vázquez, 2017).

Expertise

When analyzing factors influencing a person perceived data security, one must include the level of expertise that a person shows in the field of computer security. This is

especially true, when taking into consideration the lack of existing scientific research on the relation between expertise and perception of data security. Existing studies have shown, that with the level of expertise someone demonstrates in a certain field, that person's behavior towards that field changes. A complete novice usually has a different approach to a new situation than an expert (Bilalić, McLeod, & Gobet, 2008; Crespo-Almendros & Del Barrio-García, 2015). In the case of computer security, research indicates, that with an increase in expertise, the likelihood of using security software, like antivirus or firewall software, increases. More time spend on familiarizing oneself with digital threats, including threats on personal data security like phishing, trojans or keyloggers, will likely result in a higher awareness of the consequences these pose and result in a person actively engaging in counter measures. These include the usage of the before mentioned security software but also running security and software updates, should they be necessary (Holm, Sommestad, Ekstedt, & Honeth, 2014). A novice in the field of data security could be completely unaware, that threats like having credit card information stolen through a phishing e-mail or a trojan and personal passwords abstracted by a keylogger is even possible. Consequently, a novice would also be less likely to independently start using security software to protect his or her electronic devices from threats, as this person does not even know that they exist.

Based on these findings, we conclude that there is a difference in how a person perceives the security of his or her data when shopping online, based on that person's level of expertise in the field of computer security. We do expect this relation to be negative, meaning that an increase in expertise will result in a decrease of the level of perceived data security. Further, research indicates that increased awareness of security threats and the resulting increase in effort invested into protecting data could also result in an increase of concern for personal data (Barasch, Levine, & Schweitzer, 2016; Crespo-Almendros & Del Barrio-García, 2015; Holm et al., 2014). When being ignorant of digital security threats, a person might not feel as concerned for their personal data, as someone who knows the dangers to security and is actively trying to protect his or her data.

Media Consumption

Today, information in the form of digital media are omnipresent. At any time and place, one can find information about a place, service, product, company or event by using online services which also include traditional media like TV or newspaper, in the case they are not at hand. That means, people increasingly rely on online media, including digital forms of traditional media as well as social networks and other ways of digital communication. Digital communication is already an inherent part of billions of people's everyday lives and influences the way those people consume information and communicate with others. With special regards to e-Commerce, the trend of people relying on digital media changes their manner of judging about a product or a service and how consumers make decisions (Stephen, 2016).

Analyzing digital or online environments reveals, that the total amount of online information and services is both rapidly growing and becoming more accessible. Availability is improved through steady advances in the quality of mobile internet connection, new technology to access the internet by using electricity- instead of telecommunication-networks and new mobile devices, all being advertised by telecommunication providers. Combining these developments results in an exceedance of consumable information about a topic of interest related to the human capacity of information processing. Search engines, online version of traditional media but also new content generating formats, online retailers and social networks offer access to information about an almost unlimited range of topics. The reason for online media taking over traditional media is, that customers or users can interact and become an interactive part of media or even media creation by voting, posting, recommending, sharing, commenting or researching information. This behavior has two implications: online consumers or users aim at finding information which is consistent with their preferences while providers of online content or services are after increasing publicity. Also, referring to e-Commerce and customer's changed manners when buying a product or service, it is clear that customers can get a greater amount of suitable information about a product or service, using all functions of digital or online environments described above. On the other hand, the intense search for

information about a specific product or service delivers useful information to providers of online content and services, as they can use data of customer interactions for their recommender systems, algorithms and digital marketing (Stephen, 2016; Webster, 2010).

It is generally known, that not all information presented in online media, especially in social media, is true and of high quality. Therefore, customer interactions can be seen as part of a verifying process dependent on the relevance of accurate and true information for the individual about a specific product, service or topic. In this sense, we define "accurate and true information" as precise data that provides a detailed analysis of a product, service or topic, as well as the data being in line with the individual's preferences. Identifying backed information is necessary for customers to achieve the purpose of their activities in online media.

Sometimes such information might be obtained from sources which are perceived as untrustworthy or public opinion on social media goes against this information. Therefore, perceived trustworthiness of online information and the extent to which individuals are influenced by other's opinion are important aspects to consider (Agichtein, Castillo, Donato, Gionis, & Mishne, 2008; Hocevar et al., 2014).

Hocevar et al. (2014) in their study investigate the named aspects by using a modification of the self-efficacy-concept (Bandura, 1977). They define social media self-efficacy as "a person's beliefs about his or her capabilities to perform desired functions specifically in the social media environment" (Hocevar et al., 2014, p. 1). Their study is built upon the components of self-efficacy which are prior experience (influencing a person's confidence about finding true and accurate information), observations of other's performance (through comments, blogs or videos) and performance feedback, originally social persuasion (assuming that one has to create content in order to get feedback). Physiological and emotional states are left out as they are said to be not relevant in an online setting.

Findings show that users who use social media very actively, meaning users with high level a high level of prior experience, who are observing others and are creating

content which is responded by a high level of feedback, perceive information from social media as more trustworthy and are influenced stronger by the opinion of others.

Even though internet media seems to have taken over, Television (TV) managed to stay relevant in today's digital age. There are many different formats shown on TV, some of them informative and close to reality, other more fictitious and oriented towards entertaining the TV audience. We will now analyze, why TV has managed to stay relevant in an internet and social-media age.

Generally, TV can be described as people perceiving different impressions and linking these with reactions and emotions. This follows the overall logic of perception, meaning a stimulus generates a response which, in this case, is an information causing a judgement about it. These information are saved and re-used whenever an individual faces a situation which is similar to the underlying situation of the saved judgement, so humans tend to use heuristic processing (Stanovich & West, 2000). That means, whenever a judgement needs to be constructed, humans do not try to gather all relevant information from their memory, but only use a subset of quickly available information. This subset of information contains only the amount of data the individual considers to be sufficient for constructing a judgement. Additionally, the accessibility of information is also important when it comes to judging a situation. Only information which is remembered quick and easy can be processed and used for the construction of a judgement.

This is where TV comes into place, as it has a significant impact on the factors of information accessibility. Those are the frequencies of construct activation, its vividness and the relation to other closely related constructs. When a construct is reactivated often in a short period of time, it gets easier to access meaning that people watching similar programs on TV intensively, perceive a continuous series of stimuli for similar constructs, making these dominate soon. Very lucid information is remembered and retrieved easier than information requiring additional processing to form a judgement on. Most of the time, actions shown on TV are presented in a very entertaining or thrilling way as well as in the form of examples, what also holds for

news, so the stimulus perceived is strengthened. Given the continuous series of stimuli, constructs are linked together in the way they are presented on TV. Due to this linking behavior, there are many constructs activated, as soon as one construct within the linkage is activated leading to a series of responses to a particular stimulus. Theoretically, in the end the linkage can be seen as a script of how to react in a certain situation (Shrum, 2002).

Regarding the higher impact of examples or cases on judgements, Lichtenstein, Slovic, Fischhoff, Layman & Combs (1978) investigated the easiness to remember an accident. They asked participants to estimate the probability of death due to a stroke or an accident. The results showed that people overestimated the probability to die due to an accident enormously proving that accidents, which generally are presented in media or spoken about by persons of one's surrounding, are easier to remember and therefore lead to misjudgments.

Shrum (2002) argues that this phenomenon is also true for intense TV consumption. He explains that viewing TV influences the accessibility of constructs through the presentation of examples, which in consequence are retrieved easier and more often as a basis for judgements, although he limits this finding by stating that it only holds when the example presented on TV is not too far from reality.

Media consumption affects an individual's perception of information or any other form of stimulus, as well as changing the way the individual is responding to it. With respect to e-Commerce, information presented on TV or digital media might influence the perception of a specific product due to product tests and experience reports, a specific online shop when it is covered by media or the perceived security in an online environment when media present how secure or insecure specific actions can be.

5. Results

After carefully evaluating our findings from the before mentioned customer survey, we will now discuss the findings concerning the five hypotheses in detail. All results are shown in table 1. Before analyzing each hypothesis individually, it is important to put some of the general findings into context.

First of all, it is noteworthy, that there seems to be no significant relation between age and perceived data security (PDS) in any of the statistics. We found this to be caused by the simple fact, that over 97% of all participants were under 34 years old and 69,5% were between 18 and 24 years old. Due to this very condensed population, the age variable is insignificant in this context. The same applies to the variables education and employment. Here, 69,8% of all participants had a high school degree and 90,2% were students at the time of answering the survey (appendix 7). Like the relation of age and PDS, the sheer lack of diversion results in no significant effect of education and employment on PDS. Marital status also shows no significant relation to PDS. Since we received mixed answers to the question of current marital status, it seems that there is no significant effect on PDS, at least not in a population of mostly students (appendix 7). Interestingly, gender does have a significant effect on PDS in the context of all five hypotheses.

	Variable	Z-Score: Perceived Data Security				
		1	2	3	4	5
G	Gender	-0,301*	-0,365*	-0,532**	-0,170	-0,250**
		(0,113)	(0,107)	(0,262)	(0,120)	(0,109)
A	Age	0,037	0,043	0,264	0,051	0,075
		(0,119)	(0,112)	(0,262)	(0,113)	(0,116)
E	Education	0,011	-0,015	0,116	-0,037	-0,018
		(0,068)	(0,063)	(0,130)	(0,065)	(0,064)
M	Marital status	-0,124	-0,035	-0,271	-0,074	-0,119
		(0,118)	(0,111)	(0,266)	(0,113)	(0,113)
E	Employment	-0,127	-0,141***	-0,018	-0,141	-0,154***
		(0,082)	(0,056)	(0,165)	(0,080)	(0,079)
CO	Z-Score: Consumption		-0,294*			
			(0,056)			
PR	Z-Score: Proficiency	-0,041				
		(0,061)				
SC1	Z-Score: Security Certificate "Trusted Shop"	0,016				
		(0,070)				
SC2	Z-Score: Security Certificate "datenschutz cert"	-0,058				
		(0,064)				
SC3	Z-Score: Security Certificate "EHI Retail Institute"	-0,049				
		(0,065)				
SC4	Z-Score: Security Certificate "TÜV Süd Management Service"	0,070				
		(0,070)				
T1	Z-Score: perceived trustworthiness of Amazon.de				0,193*	
					(0,065)	
T2	Z-Score: perceived trustworthiness of Ebay.de				0,009	
					(0,077)	
T3	Z-Score: perceived trustworthiness of Ebay-Kleinanzeigen.de				-0,018	
					(0,078)	
T4	Z-Score: perceived trustworthiness of Otto.de				-0,167**	
					(0,075)	
T5	Z-Score: perceived trustworthiness of Mediamarkt.de				0,126	
					(0,101)	
T6	Z-Score: perceived trustworthiness of Zalando.de				0,210*	
					(0,073)	
T7	Z-Score: perceived trustworthiness of Thomann.de				-0,082	
					(0,065)	
T8	Z-Score: perceived trustworthiness of Lidl.de				0,107	
					(0,084)	
T9	Z-Score: perceived trustworthiness of Saturn.de				-0,131	
					(0,109)	
T10	Z-Score: perceived trustworthiness of Conrad.de				0,014	
					(0,074)	
B1	Z-Score: Benefit 1: small one-time coupon (15% off the next purchase)					-0,057
						(0,089)
B2	Z-Score: Benefit 2: large one-time coupon (50% off the next purchase)					0,226**
						(0,096)
B3	Z-Score: Benefit 3: personalized product recommendations					0,071
						(0,073)
B4	Z-Score: Benefit 4: newsletter offers					-0,139***
						(0,072)
B5	Z-Score: Benefit 5: permanent benefits (discounts for registered members)					-0,033
						(0,074)
B6	Z-Score: Benefit 6: monetary reward (50€ for ordering a VISA card)					-0,016
						(0,071)
B7	Z-Score: Benefit 7: free gifts (t-Shirts)					0,158**
						(0,078)
B8	Z-Score: Benefit 8: friend recommendations					0,012
						(0,071)
HA	Z-Score: Hacked			-0,877*		
				(0,288)		
HB	Z-Score: Behavior change after being hacked			0,285***		
				(0,145)		
	R²	0,048	0,120	0,347	0,147	0,121
	Observations	303	303	303	303	303

* significant at the 1% level; ** significant at the 5% level; *** significant at the 10% level

Table 1 Regression analysis of the survey findings

H1 Influence of Expertise on PDS

H1 states, that the level of expertise is negatively related to the level of perceived data security in the context of online shopping. The results seen in Table 1 Colum 1 seem to indicate, that there is some evidence to partly support H1, as the relation of PR, SC2 and SC3 to PDS is indeed negative. On the other hand, SC1 and SC4 are both positive and ultimately none of the variables proved to have a significant relation to PDS. In addition, the quality of the regression seems to be at a very low level, further supporting its' dismissal. Based on these results, H1 must ultimately be rejected.

H2 Effect of information consumption on PDS

The second hypotheses states, that with an increase in information a person consumes, PDS is negatively affected. The analysis, shown in Table 1 column 2, shows a significant negative coefficient for CO in relation to PDS. This indicates, that there is evidence to support H2 and we therefore accept the second hypothesis. The more often a person acquires information on data security issues, the lower that person's PDS will be. In the context of analyzing the effects of CO on PDS we can also observe a relatively large negative relation between gender and PDS.

H3 Being hacked lowers a person's PDS

The third hypothesis analytics in table 1 column 3, show that a hacker attack on a persons' electronic devices will negatively affect that persons PDS. In this case, the results strongly support H3. The relation between HA and PDS is both negative and significant. In addition, the quality of the regression as measured by R^2 is relatively high. Interestingly, there is some evidence, that a change in behavior after having experienced a hacker attack on a personal electronic device will lead to an increase in PDS. Based on this analysis, we accept H3 and can confidently say, that a hacker attack will lower a persons' PDS.

H4 Brand reputation is positively related to PDS

Our fourth hypothesis states, that an e-Commerce shop's brand reputation has a positive effect on PDS. The analysis took into account Germany's top 10 e-Commerce

platforms (Statista, 2016). The results show a significant positive relation between T1, T6 and PDS and a significant negative relation between T4 and PDS. Interestingly, the remaining results show no significant relation to PDS, indicating that a brands reputation only effects PDS at all, if the brand is both well-known and regarded as trustworthy. In the survey, Amazon (T1) was by far the most trusted online retailer, with 82% of our participants finding the shop trustworthy. Zalando (T6) comes in at number two, with 63% of the participants, who knew the brand, judging it as trustworthy (appendix 2 & 3). It does seem like there is a positive relation PDS and trust into T1 and T6. On the other hand, the results also indicate that a person who puts a lot of trust into Otto (T4) lowers his or her overall PDS, even though Otto is known to 81% of the participants and trusted by 55% of the ones that know the brand (appendix 4). Combining these findings, we cannot draw a decisive conclusion. Since the findings differ largely and, we conclude the effect of the variables T1 through T10 on PDS is not proven beyond doubt and could be caused by simultaneous causality bias, meaning someone with a lower PDS might just tend to trust T4 a lot, but trusting T4 will not result in a lower PDS. An effect of brand's reputation on PDS, measured through the perceived trustworthiness of a brand, is still very likely, but there is not enough evidence to accept H4 in this case. In conclusion, the results are too inconsistent and we reject the H4.

H5 Benefits are positively related to PDS

The last hypothesis is related to the question, how a benefit change ones' willingness to transfer data to an e-Commerce platform and consequently states, that a benefit positively influences PDS. The findings show, that the influence on PDS is highly dependent on the kind of benefit offered by the online store. B1, B3, B5, B6 and B8 did not produce significant results, showing that customer's PDS is not at all affected by them. B2 and B7 both do show significant positive relations to PDS, meaning larger coupons and gifts both seem to increase the customers PDS. On the other hand, we see some slightly significant indications, that B4 has an adverse effect on PDS. Newsletter offerings could end up decreasing PDS. Taking all findings into account, we can conclude, that while the findings do support H5, they also show that relevance is

highly dependent on the type of benefit offered by the e-Commerce platform. Not every benefit will increase customers PDS, but if an online shop chooses the right benefits, it can have a positive influence on PDS. Overall, we accept H5 but acknowledge that it is not universally true.

6. Conclusion

After going through all the findings step by step, we will now analyze, what they mean and what these results imply for the e-Commerce industry. First of all, the findings from our survey analysis mostly agree with existing literature, but differ in some important respects. We found, that a customer's perception of data security is highly influenced by that person's frequency of consuming information about data security issues on the one hand, and the experience of a hacker attack on the other. Proficiency in the field of data security on the other hand, proved to have no significant effect on the PDS of our population. This indicates, that gathering information on data security issues and having proficient knowledge in that field are essentially different factors and influence people's PDS in different ways. Meaning that collecting information does not necessarily relate to proficiency in the field and vice versa. This relation could be subject of further research. We highly encourage a study to investigate the relation of information gathering and expertise with regards to the topic of data security. Based on our findings, it is entirely possible, that without expertise, the raw information has a negative effect on a person's PDS, but combined with a certain level of proficiency, the information is processed differently and the effect on PDS could change.

Next, we will look at some indications for an actual online store, considering the relevant findings from H2, H3 and H5. With regards to H2, it should be obvious that an e-Commerce business cannot directly influence their customers media consumption behavior, but we do suggest that, in order to increase customers PDS, an online store should try not to make headlines through a media scandal. If the consumption of information on data security issues lowers PDS, it could consequently mean, that as an e-Commerce business, standing out negatively in terms of data security would influence that store's customer's PDS negatively. This should be avoided, if a store

wants to retain both their customers and their customer's trust (Fang et al., 2014; Flavián et al., 2006).

The second large influencer is the experience of being hacked, as described in H3. The results show a clear negative effect on PDS, meaning to increase PDS of their customers, an online store should implement sufficient data security measures and try to protect their customers as best as they can. Since we do not expect retailers to have direct access to their customers personal devices, we suggest educational efforts to protect their customers from a hacking attack. Since proficiency in the field of data security does not seem to have any effect on PDS, the effort of educating customers on data security should also not affect their PDS. Now, that makes it sound like educational efforts would be a waste of time and money. But, we argue that, as a consequence of educating people on data security issues and more importantly how to protect themselves against digital threats, could prevent a possible hacker attack and thereby also prevent the negative effect of that attack on a customer's PDS. Future research towards this direction is advised and could deliver scientific evidence to support this argument.

The lessons learned from looking at the analysis of H5 allow more decisive conclusions for e-Commerce businesses. If an online retailer wants to increase their customers PDS and make them more willing to transfer personal data, offering a benefit can be a good option, but only if the benefit is attractive enough. Badly received benefits like newsletters could even result in a decrease of customers PDS. It is therefore important for an online shop to choose the right benefits. In the context of PDS, the right benefit also does not necessarily mean the most attractive benefit. In our survey, the most attractive benefit was B5, which has no significant relation to PDS. On the other hand, B7 has a positive impact even though only 18% of our participants deem it attractive enough to trade personal data to obtain the benefit (appendix 1). For an online shop, this indicates, that before implementing a benefit with the goal of increasing customers PDS, research into the attractiveness, costs and the effect on PDS of a benefit should be conducted to ensure, that the planned benefit is well received,

reasonable from an economic point of view and has the desired impact on PDS. Without that research, there is a risk of causing no or even an adverse effect on PDS.

The last indication of the research shows, that trustworthiness alone is not enough to influence PDS. Only in special cases is a brand reputation strong enough to influence a customer's PDS. In most cases, e-Commerce businesses cannot rely on their reputation to influence their customers PDS, meaning a customer is not likely to give up personal information based on a brand's reputation alone, unless that brand is Amazon or Zalando.

Limitations and Future Research

The research we conducted was not without limitations, some of which were already briefly mentioned. The clear focus in our sample group is probably the largest limitation of this research and while it allows for a pretty accurate result for students under the age of 34, it is not possible to generalize the findings and draw conclusions, which hold true for other demographics. It would be highly beneficial, to conduct future research with a more diverse sample. It would also be interesting to analyze possible differences between generations and demographics. A future study could for example create archetypes for different demographics based on their differences in PDS. This could be useful to show, how the perception of data security changes depending on age, cultural and educational background.

Another fact is, that this research was limited to finding influencers on PDS, but cannot provide a clear link between PDS and a customer's decision to buy a product based on his or her perceived security in on an e-Commerce platform. This is why we suggest research into the relation between PDS and conversion rate, to analyze whether PDS could be a legitimate influencing factor on a customer's decision to buy from a certain online retailer (Heathman, 2014). This would add valuable insights into the concept of PDS ion general as well as giving e-Commerce businesses additional useful feedback on the effectiveness of increasing their customers PDS.

Additional limitations include a lack of insider knowledge. A research with the support an e-Commerce company could deliver different results.

Statutory Declaration

The Authors herewith formally declare that they have written the submitted dissertation independently. They did not use any outside support except for the quoted literature and other sources mentioned in the paper.

They clearly marked and separately listed all the literature and other sources which they employed when producing this academic work, either literally or in content.

Felix Balzer   Bastian Bollig

7. References

Accenture. (2011). *Welche der folgenden Aussagen zur Datensicherheit bei der Nutzung des Internets per Handy treffen auf Sie persönlich zu?* In Statista - Das Statistik-Portal. Retrieved from https://de.statista.com/statistik/daten/studie/76594/umfrage/aussagen-zur-datensicherheit-im-mobilen-internet/

Agichtein, E., Castillo, C., Donato, D., Gionis, A., & Mishne, G. (2008). Finding High-quality Content in Social Media. *International Conference on Web Search and Data Mining*, 183–193. https://doi.org/10.1145/1341531.1341557

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, *84*(2), 191–215.

Barasch, A., Levine, E. E., & Schweitzer, M. E. (2016). Bliss is ignorance: How the magnitude of expressed happiness influences perceived naiveté and interpersonal exploitation. *Organizational Behavior and Human Decision Processes*, *137*, 184–206. https://doi.org/10.1016/j.obhdp.2016.05.006

Bilalić, M., McLeod, P., & Gobet, F. (2008). Expert and "novice" problem solving strategies in chess: Sixty years of citing de Groot (1946). *Thinking & Reasoning*, *14*(4), 395–408. https://doi.org/10.1080/13546780802265547

Bloom, N., Sadun, R., & van Reenen, J. (2010). Does product market competition lead firms to decentralize? *American Economic Review*, *100*(2), 434–438. https://doi.org/10.1257/aer.100.2.434

Capgemini Consulting. (2017). *The Currency of Trust*. Retrieved from https://www.capgemini-consulting.com/resource-file-access/resource/pdf/privacy-and-cybersecurity-in-fs_dti-research-report.pdf

Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Q*, *36*(4), 1165–1188. Retrieved from http://dl.acm.org/citation.cfm?id=2481674.2481683

Chen, S. C., & Dhillon, G. S. (2003). Interpreting Dimensions of Consumer Trust in E-Commerce. *Information Technology and Management*, *4*(2), 303–318. https://doi.org/10.1023/A:1022962631249

Chircu, A. M., Davis, G. B., & and KAUFFMAN, R. J. (2000). *Trust, Expertise, and E-Commerce Intermediary Adoption*. AMCIS 2000 Proceedings. Retrieved from http://aisel.aisnet.org/amcis2000/405

Crespo-Almendros, E., & Del Barrio-García, S. (2015). Expert vs. novice users: Comparative analysis of the effectiveness of online discounts and gifts. *Revista Española de Investigación en Marketing ESIC*, *19*(1), 46–61. https://doi.org/10.1016/j.reimke.2014.12.001

Fang, Y., Qureshi, I., Sun, H., McCole, P., Ramsey, E., & Lim, K. H. (2014). TRUST, SATISFACTION, AND ONLINE REPURCHASE INTENTION: THE MODERATING ROLE OF PERCEIVED EFFECTIVENESS OF E-COMMERCE INSTITUTIONAL MECHANISMS. *MIS Q*, *38*(2), 407-A9.

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

Heathman, B. (2014). *Conversion marketing: Convert website visitors to buyers*. [s.l.]: Audioink Publishing.

Heng, Y. L., & Wei, T. H. (2010). Online store trustworthiness and customer loyalty: Moderating the effect of the customer's perception of the virtual environment. *African Journal of Business Management*.

Hocevar, K. P., Flanagin, A. J., & Metzger, M. J. (2014). Social media self-efficacy and information evaluation online. *Computers in Human Behavior*, *39*, 254–262. https://doi.org/10.1016/j.chb.2014.07.020

Holm, H., Sommestad, T., Ekstedt, M., & Honeth, N. (2014). Indicators of expert judgement and their significance: An empirical investigation in the area of cyber security. *Expert Systems*, *31*(4), 299–318. https://doi.org/10.1111/exsy.12039

Huang, E. Y., & Tsui, C.-j. (2016). Assessing customer retention in B2C electronic commerce: An empirical study. *Journal of Marketing Analytics*, *4*(4), 172–185. https://doi.org/10.1057/s41270-016-0007-x

IBM. (1981). *The birth of the IBM PC*. Retrieved from https://www-03.ibm.com/ibm/history/exhibits/pc25/pc25_birth.html

Initiative D21. (2017). *Empfohlene Gütesiegel Anbieter*. Retrieved from
http://internet-guetesiegel.de/

ISACA. (2017). *Which, if any, of the following have increased your concern about the privacy of your personal data?* In Statista - The Statistics Portal. Retrieved from
https://www.statista.com/statistics/374512/concerns-about-personal-data-privacy-uk/

Isbrucker, W. (2015). E-commerce Customer Retention – Factors and Their Interdependencies. Retrieved from http://www.willemisbrucker.com/business/e-commerce-customer-retention-factors-and-their-interdependencies/

Kim, Y., & Peterson, R. A. (2017). A Meta-analysis of Online Trust Relationships in E-commerce. *Journal of Interactive Marketing*, *38*, 44–54.
https://doi.org/10.1016/j.intmar.2017.01.001

L. J. Shrum. (2002). Media Consumption and Perceptions of Social Reality: Effects and Underlying Processes.

Lichtenstein, S., Slovic, P., Fischhoff, B., Layman, M., & Combs, B. (1978). Judged Frequency of Lethal Events. *Journal of Experimental Psychology: Human Learning and Memory*, *4*(6), 551–578.

Liu, H. Y., & Hung, W. T. (2010). Online store trustworthiness and customer loyalty: Moderating the effect of the customer's perception of the virtual environment. *African Journal of Business Management*, *4*(14), 2915–2920. Retrieved from http://search.proquest.com/openview/605bf9bb0fe1921c6ec4d71bacf70755/1?pq-origsite=gscholar

López-Miguens, M. J., & Vázquez, E. G. (2017). An integral model of e-loyalty from the consumer's perspective. *Computers in Human Behavior*, *72*, 397–411.
https://doi.org/10.1016/j.chb.2017.02.003

Oliveira, T., Alhinho, M., Rita, P., & Dhillon, G. (2017). Modelling and testing consumer trust dimensions in e-commerce. *Computers in Human Behavior*, *71*, 153–164. https://doi.org/10.1016/j.chb.2017.01.050

Pavlou, P. A. (2002). Institution-based trust in interorganizational exchange relationships: The role of online B2B marketplaces on trust formation. *The Journal*

of *Strategic Information Systems*, *11*(3-4), 215–243.
https://doi.org/10.1016/S0963-8687(02)00017-3

Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology*, *30*(3), 227–238. https://doi.org/10.1016/j.appdev.2008.12.010

Peres, R., Shachar, R., & Lovett, M. J. (2013). On Brands and Word-of-Mouth. *Journal of Marketing Research*, *50*(4), 427–444. https://doi.org/10.2139/ssrn.1968602

Rashid, M., Jiang, Z., Refalo, P.-L., Buvat, J., Kar, K., & KVJ, S. (2017). *The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure*: Capgemini Consulting.

Shah, M. H., Peikari, H. R., & Yasin, N. M. (2014). The determinants of individuals' perceived e-security: Evidence from Malaysia. *International Journal of Information Management*, *34*(1), 48–57. https://doi.org/10.1016/j.ijinfomgt.2013.10.001

Shrum, L. J. (2002). Media Consumption and Perceptions of Social Reality - Effects and underlying Processes. In J. Bryan & D. Zillmann (Eds.), *Media effects: Advances in theory and research* (2nd ed., pp. 69–95). Taylor & Francis.

Stanovich, K. E., & West, R. F. (2000). Individual Differences in Reasoning: Implications for the Rationality Debate? *The Behavioral and Brain Sciences*, *23*(5), 645-665; discussion 665-726. https://doi.org/10.1017/S0140525X00003435

Statista. (2016). *E-Commerce in Deutschland*. In Statista - Das Statistik-Portal (No. did-6387-1). de.statista.com. Retrieved from https://de.statista.com/statistik/studie/id/6387/dokument/e-commerce-statista-dossier/

Stephen, A. T. (2016). The Role of Digital and Social Media Marketing in Consumer Behavior. *Current Opinion in Psychology*, *10*, 17–21.

Symantec. (2015). *State of Privacy Report 2015*. de.statista.com: Symantec. Retrieved from https://de.statista.com/statistik/studie/id/26810/dokument/bericht-zum-datenschutz-von-verbrauchern-in-europa-2015/

Wang, Y., Wang, Y., Lin, H., & Tang, T. (2003). Determinants of user acceptance of Internet banking: An empirical study. *International Journal of Service Industry Management*, *14*(5), 501–519. https://doi.org/10.1108/09564230310500192

Webster, J. G. (2010). User information regimes: How social media shape patterns of consumption. *Northwestern University Law Review*, *104*(2), 593–612. https://doi.org/10.1525/sp.2007.54.1.23

8. Appendix

Ben1	Ben2	Ben3	Ben4	Ben5	Ben6	Ben7	Ben8	
123	62	187	207	58	118	111	129	very unlikely
74	51	64	60	43	72	72	64	unlikely
50	61	19	18	64	55	66	63	neutral
49	95	29	15	114	43	44	41	likely
7	34	4	3	24	15	10	6	very likely
18%	43%	11%	6%	46%	19%	18%	16%	% of Likely

Appendix 1

Name	0	1	2	3	4	5	
Amount	2	5	14	35	141	106	
Percent	1%	2%	5%	12%	47%	35%	
CusPerc		2%	5%	12%	47%	35%	
					Trust	**82%**	

Appendix 2 Trustworthiness of Amazon

Name	0	1	2	3	4	5	
Amount	39	6	19	73	110	56	
Percent	13%	2%	6%	24%	36%	18%	
CusPerc		2%	7%	28%	42%	21%	
					Trust	**63%**	

Appendix 3 Trustworthiness of Zalando

Name	0	1	2	3	4	5	
Amount	59	6	12	92	91	43	
Percent	19%	2%	4%	30%	30%	14%	
CusPerc		2%	5%	38%	37%	18%	
					Trust	**55%**	

Appendix 4 Trustworthiness of Otto

Appendix 5: Survey questions and sources

Has one of your personal electronic devices ever been hacked before? (L. J. Shrum, 2002)

Did the experience of having been hacked change you online shopping behavior? (Capgemini Consulting, 2017; L. J. Shrum, 2002)

How often do you get information on data security issues? (Hocevar et al., 2014)

Are you familiar with the following security certifications? Are they important to your decision, whether to trust an online retailer or not? (Initiative D21, 2017)

When it comes to general knowledge about data security, I would describe myself as… (Chircu, Davis, & and KAUFFMAN, 2000) NIH Proficiency Scale (2017)

In general, how secure do you feel your data is online? (Capgemini Consulting, 2017; Chen et al., 2012; Flavián et al., 2006)

On a scale from 1-10 how much do you trust eCommerce platforms? (Capgemini Consulting, 2017; Heng & Wei, 2010; Statista, 2016)

On a scale of 1-5, how likely is it that you will provide private information for one of the bellow mentioned benefits in eCommerce? (Capgemini Consulting, 2017; Chen et al., 2012)

On a scale from 1-5 how secure do feel while being online?(ISACA, 2017)

How often do you undertake sensitive transactions with your smartphone (e.g. Mobile Payments, Online Banking, Online Shopping etc.) (Accenture, 2011; Shah, Peikari, & Yasin, 2014; Symantec, 2015; Wang et al., 2003)

Appendix 6

Regression in SPSS. The full data set can be retrieved online at no costs under the following addresses:

https://felix.hs-furtwangen.de/url/HomeSite/2405728317/userfolder/0/path%3D~~public~~PDSRegression%2Esav/0

Appendix 7

The survey raw data in form of an Excel file, including every answer can be obtained via the link below.

https://felix.hs-furtwangen.de/url/HomeSite/2405728317/userfolder/0/path%3D~~public~~Data%20Security%20Project%5FTransformation%5Fraw%5Fdata%2Exlsx/0