UNIVERSITY OF VAASA

SCHOOL OF MANAGEMENT

Joakim Georgij Paljakka

THE IMPACT OF DATA BREACHES ON CONSUMERS' ATTITUDES AND BEHAVIORS

Master's Thesis in
International Business

VAASA 2019

TABLE OF CONTENTS **Page**

LIST OF TABLES AND FIGURES **Page**

UNIVERSITY OF VAASA
School of Management
Author: Joakim Georgij Paljakka
Topic of the thesis: The impact of data breaches on consumers' attitudes and behaviors
Degree: Master of Science in Economics and Business Administration
Master's Programme: International Business
Name of the supervisor: Vesa Suutari
Year of entering the university: 2012
Year of completing the thesis 2019
Number of pages: 76

ABSTRACT

There exists some amount of research regarding data breaches and how they affect consumers' attitudes and behaviors. However, the amount of studies in this context is still low and more research is required. The research has mainly concentrated on the breached companies' perspective and how the consumers' attitudes and behaviors have changed due to the breaches. This thesis investigates how the knowledge of data breaches affects consumers' attitudes and behaviors, and what kinds of attitudes and behaviors consumers have toward breached companies.

The study is qualitative in nature and uses semi-structured interviews to gather data from 10 Finnish interviewees. The consumers' attitudes and behaviors are affected by the knowledge of data breaches, especially due to concerns that the data breaches create. Furthermore, consumers' attitudes and behaviors towards companies that have experienced a data breach vary depending on different reasons. The results are mixed whether the consumers would do business with a breached company, or sign-in a service that has experienced a breach. The thesis provides more evidence on how consumers are affected by the data breaches and why companies should pay attention to consumers' data protection.

KEYWORDS: Data breach, consumer attitude and behavior

1. INTRODUCTION

This chapter includes the following topics: research background, research question and objectives, and research structure.

1.1. Research background

The internet and devices connected to it have rapidly developed over the last three decades, which has enabled different sized businesses to engage in the global market. At the same time, consumers have increased their digital activities. For example, in 2014, consumers spent $300 billion shopping online. Moreover, consumers have increased sharing their various private information online to different parties while, for example, using bank related services or filing tax returns. The different entities such as organizations or businesses trace consumers' activities and store their private information into databases. (Choong, Hutton, Richardson, & Rinaldo, 2017.)

While collecting customer data has advantages, the downside is that this data may be used for criminal intentions (Malhotra & Malhotra 2011; Choong et al. 2017). Hackers, hacktivists, and insiders are some of the actors who are involved in committing data breaches (Huq 2015). Motives for committing data breaches include financial, espionage, fun, grudge, and other motives. The largest amount of data breaches is motivated by financial gains. (Verizon 2018.) Additionally, data breaches are committed in increasing numbers and have significant impact on consumers and organizations (Sen & Borle 2015). The data breaches are disruptive for organizations and consumers. While organizations face consequences such as reputational damage, legal problems, and negative financial market impacts (Cashell, Jackson, Jickling & Webel 2004), the consumers may face short- and long-term consequences. For example, the consumer's identity (Wheatley, Maillart & Sornette 2016) or payment information may be stolen (Janakiraman, Lim & Rishika 2018).

As the consumers are connected to the Internet in increasing numbers while sharing their personal information to different parties, the cyber criminality evolves at the same time, and the potential for data breaches increases. There exists some evidence that breached information is going to increase from two to four billion items during the next five years. Therefore, the consumers should worry about privacy erosion, despite being involved

with trustworthy organizations. (Wheatley et al. 2016.) The information related to the data breaches often include personal information such as names, email addresses, account numbers, and transaction information (Chakraborty, Lee, Bagchi-Sen, Upadhyaya & Rao 2016). As consumers typically self-disclose in the online environment, online self-disclosure means how willing the individual is to share personal information to a company (Mothersbaugh, Foxx, Beatty & Wang 2012). Being involved in different online activities require self-disclosure, therefore the consumers may have concerns about how their personal information may be misused (Choi, Park & Jung 2018). The data breaches are related to privacy concerns, because the breaches cause potential misuse of personal information. Moreover, privacy concern means the beliefs about risks and negative consequences related to sharing information (Baruh, Secinti & Cemalcilar 2017).

There exist many studies related to privacy concerns (Baruh et al. 2017; Hoffmann, Lutz & Ranzini 2016). Privacy concern may be viewed as a predictor to privacy management. This means that the privacy concerns may affect the consumers' self-disclosure behavior. For example, how strictly the consumers share their personal information (Baruh et al. 2017). Moreover, researchers have studied "privacy paradox", which means that despite of privacy concerns, the consumers do not seem to change their privacy related behavior (Hoffmann et al. 2016), although the evidence in the context of privacy paradox seems to be mixed (Kokolakis 2017).

There exist several studies related to data breaches and their effects on consumer behavior and attitudes. The studies include data breach announcement effect on customer behavior (Janakiraman et al. 2018), data breach announcement and customer trust (Muzatko & Bansal 2018), data breach effect on user security management (Curtis, Carre & Jones 2018), intention to do business with a company that has experienced a data breach (Chakraborty et al. 2016), and scope of data breach effect on shopping intention (Chatterjee, Gao, Sarkar & Uzmanoglu 2019). Furthermore, the studies include the effect of publicized data breach on customer behavior (Lee & Lee 2012), and firm's recovery effort effects on customer behavior after a data breach (Choi, Sung & Jiang 2016; Goode, Hoehle, Venkatesh & Brown 2017). However, Choong et al. (2017) state in their study that there is only a small amount of marketing research available regarding data breach and its impact on consumers. This thesis aims to research further the consumers' attitudes and behaviors today.

1.2. Research question and objectives

Given that data breaches are committed in increasing numbers and affect companies and consumers, it is important to examine more closely how data breaches affect consumers' attitudes and behaviors today. Even though there exists research related to the data breaches and the effects they have on consumers, Choong et al. (2017) have stated that there exists only a small amount of marketing research related to the impact of data breaches on consumers. As the data breaches have become more frequent, it is important to provide more research on how the knowledge of data breaches affect the consumers, and what kinds of attitudes and behaviors the consumers have toward breached companies. While there is existing research related to companies that have experienced a data breach and how the consumers are affected by this, the study also aims to discover how the general knowledge of data breaches have affected the consumers' attitudes and behaviors. Moreover, this study includes only Finnish interviewees, so the data breaches are viewed from Finnish consumers' perspective. Additionally, this thesis mainly concentrates on the online aspect of data breaches and consumers' attitudes and behaviors.

The data breaches are a global phenomenon, and a company which is in one country may be breached from other countries. Additionally, the consumers do business with companies that are in other countries, and these companies may experience a data breach.

In order to understand the attitudes and behaviors related to data breaches, the thesis presents the relevant research related to data breaches, privacy concerns in online business, and consumers' perspective on these topics. The research question is:

How do data breaches affect consumers' attitudes and behaviors?

In order to answer the research question, two research objectives are presented:

(1) How does the knowledge of data breaches affect consumers' attitudes and behaviors?

(2) What are the consumers' attitudes and behaviors toward companies that have experienced a data breach?

1.3. Research structure

There are six chapters in this thesis including introduction, data breach, privacy concerns in online business, methodology, findings, and conclusion.

This chapter introduces the topic and provides information about it. Afterwards, the research question and objectives are provided. Finally, the research structure is presented.

In the second chapter, the data breaches are viewed from different angles, including general information regarding data breaches, the different kinds of data breaches that exist, the actors that are involved in these data breaches, and reasons for data breaches. Furthermore, the chapter includes legislation related to data breaches, data breaches' effects on organizations, and data breaches' effects on consumers.

In the third chapter, the literature section related to privacy concerns in online business provides a general overview on privacy, theory on privacy concerns, different perspectives on consumers' concern for online privacy, privacy concerns and privacy paradox, and (online) self-disclosure. Furthermore, a summary of the whole theory is presented in the end.

In the fourth chapter, the thesis presents the methodology of this study. The chapter includes research method, research approach, data collection and sample, and analysis of the data. Furthermore, the topics in this chapter include ethics related to the research, and reliability and validity of the study.

In the fifth chapter, the findings of the study are presented from the gathered data.

In the sixth chapter, the key findings are compared to the existing literature, practical implications are given, and limitations and suggestions for future research are presented.

2. DATA BREACH

This chapter views data breach from different aspects. The topics include general information regarding data breaches, data breach types, actors, and reasons for data breaches, and legislation regarding data breaches. Furthermore, the chapter discusses data breaches from organizations' and consumers' perspectives.

2.1. General information regarding data breaches

Data breaches are committed in increasing numbers and they have a significant impact on financial and legal implications for the organizations or individuals that are affected by the breach. For example, the average cost of a data breach for an organization in the United States was estimated to be approximately $5.9 million in 2014. The most significant impact of data breach on individuals is identity theft, which resulted in approximately $16 billion stolen from 12.7 million people in 2014. Data breach involves unauthorized access to private data, which may then be used in different ways. The private data is often related to personal health information, personally identifiable information (PII), trade secrets, intellectual property, and financial data. (Sen & Borle 2015.)

Data breaches are considered disruptive and costly cybersecurity events for organizations and consumers. Large breaches targeted at organizations have a potential for immediate financial consequences such as reduction of stock prices and reputational damage. Regarding individuals, not only do they face short term consequences, but additional after-effects such as identity fraud, because the stolen information may be sold in underground markets and used for criminal intentions. (Wheatley et al. 2016.)

Cyber risks are highly dynamic in the general context of the Internet. It is a difficult task for the IT security technology to keep up with the adaptive and evolving cyber-crime techniques, including social engineering attacks and abuse of "zero day" security vulnerabilities. Due to the increasing amount of confidential information stored in digital format and people using devices linked to the Internet, the potential for cyberattacks is increased. People who share their personal information with, for example, private and governmental organizations should not only worry about constant privacy erosion but expect that their personal information may be suddenly or progressively leaked to underground markets and other parties. (Wheatley et al. 2016.) The individual who has

stolen a victim's personal information may try to stay hidden and not reveal to the victim that his/her personal information has been stolen and is currently being misused. For example, while making purchases with the victim's payment card, the individual may forward the bills to another address rather than the victim's address. Therefore, the victim remains unaware of the whole event until the individual has caused severe damage to the victim's credit, reputation, or other assets. (Albrecht, Albrecht & Tzafrir 2011.)

Veltsos (2012) suggests that data breaches have increased due to the ease of collecting and stealing digital information. For example, three United States Department's contractors accessed Barack Obama's passport file in 2008 without proper authorization. Moreover, it was reported that 11 State Department employees accessed celebrities' and politicians' passport files for reasons such as curiosity. (Veltsos 2012.)

People often seem to imagine that threats aimed at personally identifiable information relate to large databases that hold the information, but this is not always the case. People usually give away small bits of information to multiple organizations and firms while using their services and this information is usually harmless. If the information is combined, it can be used for criminal intentions by an identity thief. By mining data to find similarities, the scattered information can be put together to provide an accurate profile. For example, the right amount of data may be used to open credit cards and transfer money from the victim's bank account. The personally identifiable information can be used for further purposes also, because it usually stays the same. (Veltsos 2012.)

Data breaches that affect different organizations and institutions have been committed in increasing numbers, although majority of them remain unreported. A large amount of confidential data regarding individuals and organizations is compromised. Moreover, the data includes, for example, personally identifiable information, financial information, log-in credentials, and payment card data. The news often report data breaches that have involved hacking or malware, but there are other methods such as insider attacks, and theft. People who commit data breaches include, for example, insiders, individual criminals, organized groups, and state-sponsored groups. Crimes that are committed with the stolen data include fraud, identity and intellectual property heft, espionage, revenge, blackmail, and extortion. (Huq 2015.)

Consumers have become increasingly desensitized to their data being compromised, because data breaches are very common today. Several factors contribute to the desensitization effect: Data breaches are reported more frequently on the news, stolen

data is not as tangible as a physical item, consequences of stolen data may not be felt instantly, and the lack of understanding what the results of a data theft may lead to. (Huq 2015.)

A data breach is a complex event, and the targets include any organizations, firms or individuals that store confidential data. Having a response plan for a data breach may not reduce the challenge of the event. Often the first questions that are asked after a data breach has been detected are: what data has been stolen, how long has it been since the data breach started, how did the attackers manage to bypass the defenses, and what is the level of penetration in the network. The breached target must respond quickly to combat the consequences that the breach has caused. Predicting the reason, method, and target of a data breach may be impossible, because the methods and targets vary a lot. Data breaches are often planned but may also be accidental. Some breaches go unnoticed for months or years, while others are detected in a matter of hours or days. (Huq 2015.)

Data breaches are often quickly reported on the media, but it is rarely disclosed what has happened to the stolen data. It is often difficult to follow what has happened to the stolen data due to various reasons. The data may be released to Deep Web marketplaces after a long period of time or not at all. The criminals may avoid unwanted attention by not advertising the data that is being sold as belonging to a specific breach, business, or organization. Victims of a breach may not want to reveal information that could make the data easier to identify. The Deep Web marketplaces have millions of records and the stolen data may be hard to track in this environment. Accessing stolen data requires purchasing it which is expensive and criminal. (Huq 2015.)

2.2. Data breach types, actors, and reasons for data breaches

Individuals and organizations are affected by data breaches every day. Some of the more common objectives of data breaches are to gain access to personally identifiable information, financial data, and credentials (Huq 2015). For example, data breaches that are targeted at online shopping systems commonly try to steal customers' credit card information and personal information (Peretti 2008). Afterwards, the customers become vulnerable to unapproved purchases. Cyber criminals can also exploit other information such as mailing addresses. These exploits are usually more difficult to detect (Chakraborty, et al. 2016).

Actions such as identity fraud, applying for loans or credit cards, selling to marketing firms, filing fraudulent tax returns, registering fake accounts, or spamming and phishing may be committed using personally identifiable information. Financial data may be used to create counterfeit credit cards, pay bills, make fraudulent online transactions, and transfer the victims' money out of their bank account. Credentials may be used to steal intellectual property, commit espionage, or to spam and phish. Other data, for example, stolen confidential data may be used in vengeance attacks and hacktivism, where the stolen data is held for ransom or the victims are blackmailed. Stolen data is often sold in Deep Web marketplaces. Payment methods that offer anonymity to the buyers and sellers are favored, such as bitcoins, WebMoney, and escrow accounts. (Huq 2015.) According to Verizon's data breach investigations report (2018), 58% of victims are categorized as small businesses, 24% of breaches affected healthcare organizations, 15% of breaches involved accommodation and food services, and 14% were breaches of public sector entities.

There are various ways for conducting data breaches (Ayyagari 2012). Next, some of the more common techniques are described briefly.

Unintended disclosure: Information that is considered sensitive is posted publicly on a website, mishandled, or sent to wrong address or people via email, fax or mail.

Hacking or malware: Electronic entry by an outside party, spyware and malware.

Payment card fraud: This fraud involves credit and debit cards and it is not accomplished by hacking. For example, skimming devices may be used at point-of-service terminals.

Insider: A person who has legitimate access intentionally commits a data breach. For example, an employee or a contractor.

Physical loss: Lost, discarded or stolen records that are not in electronic format. For example, paper documents.

Portable device: Lost, discarded or stolen smartphone, laptop, hard drive, CD, etc.

Stationary device: Lost, discarded or stolen stationary electronic device. For example, computers or servers that are not intended for mobility.

Various actors are involved in data breaches (Mills & Harclerode 2018). These actors are explained next. The whistleblower obtains data in the environment s/he is working in to reveal a misconduct. The United States congress has, for example, extended protection for whistleblowers who want to expose some type of corporate fraud. (Mills & Harclerode 2018.)

Data breach caused by the insider may involve a whistleblower or an employee who uses confidential data to harm the company or for a purpose that is unauthorized. Breaches that are conducted by insiders may additionally be unintended. Moreover, 25% of breaches in 2016 were caused by internal actors, and 14% of every breach in 2016 were caused by employee error. The belief that hackers are only responsible for data breaches is not very accurate. For example, an angry employee may be responsible for a data breach as well. (Mills & Harclerode 2018.) According to Huq (2015), the motivation for insiders to conduct data breaches may be difficult to understand. These insiders may be a part of an organization and proceed to act against it. They are motivated by, for example, money, ideology, coercion, and ego. Moreover, the insiders often have multiple motivations.

The hacker is involved in hacking systems. There exists a lot of different ways to hack databases. Some of these techniques are based on technical knowledge and some exploit human frailty. Criminal hackers use techniques such as point-of-sale (POS) hacks, physical theft, web-app attacks, crimeware, card skimmers, brute-force attacks on encryption, spear phishing, and cyber espionage. Hackers may prepare extensively and have a deep knowledge of the dark web. An example of hacking is that an employee downloads malware that is planted by a hacker which enables the hacker to gain entry to some data. Victims of the hacker may include consumers and companies. Most data breaches (62%) in 2016 involved a criminal hacker. The motivations of a hacker include harming a target, benefitting the hacker someway, and exposing a truth. In the context of corporate espionage, the hacker may benefit or harm a competitor. (Mills & Harclerode 2018.)

The hacker may be specified further to groups and individuals. Individual criminals usually refer to an individual or a group of two people that do business in the black market by stealing and selling private data. Hacktivists steal and release stolen data to reveal confidential information about an organization to cause harm or embarrassment. Organized groups are usually funded and run by crime syndicates. They often steal and monetize confidential data. Additionally, there exists hacktivist groups such as

Anonymous that usually operate for the same reasons as an individual hacktivist. Espionage, intelligence gathering, and competitive advantage are often the reason for data theft. There are two operational models for state-sponsored groups: the hacking team and its resources are controlled by the state or hacking activities are outsourced to third parties. (Huq 2015.)

The republisher is an entity that may inflict damage by publicly sharing data that has been leaked after a data breach. The republisher may be, for example, an individual on social media, a blogger, or a media outlet. After the hacker has gained access to some confidential data, s/he may forward the information to a republisher. The republisher may then publicly reveal the information to some audience, which may cause even more damage. Depending on the laws of a country, the republisher may have protection of free speech when revealing hacked or leaked data, although there are factors that may determine if the publication of information related to a data breach is legal. For example, the courts in the United States have allowed publication of information that was considered dangerous, intrusive, and illegally obtained. (Mills & Harclerode 2018.)

2.3. Legislation regarding data breaches

Different countries have different laws regarding data breach disclosure. In the next section, there is a brief comparison of laws between the United States of America and the European Union.

When a data breach occurs in the USA, the firms are obligated to inform affected individuals about the event due to the State and federal laws. The state breach law implemented in California was considered a success and lead to increased number of privacy breach reports from firms. Afterwards, other states started to implement similar laws. There are two prominent federal laws in addition to the state laws. “Health Insurance Portability and Accountability Act” mandates firms working in health care sector to notify about data breaches to individuals whose health information may be compromised, the Department of Health & Human Services, and in some cases the media. The “Gramm-Leach-Bliley Act” obliges firms in the financial sector to report data breaches to primary federal regulators, and under some circumstances to the individuals who have been affected by the breach. Some state and federal laws require firms to notify individuals only, and others require the firms to also report to the authorities. (Laube & Böhme 2016.)

According to Laube et al. (2016), EU Member States are affected by Union laws and national laws that mandate the firms to report data breaches. The authors reviewed all the enforced union breach notification laws and discovered that the firms must first report the data breaches to authorities. This is different from the US laws, where it is common to notify the individuals who have been affected by the breach. The objective is to create a union-wide transparency on data breaches. For example, the authorities may then offer guidance to the affected firms and individuals or inform unaffected firms and individuals about the ongoing attacks. Some Member States of the EU have made additional laws regarding data breach notification. General Data Protection Regulation (GDPR) and Network and Information Security Directive (NIS Directive) are newer additions that expand the EU data breach laws. (Laube et al. 2016.)

2.4. Data breaches from organizations' perspective

Companies have increased their reporting regarding data breaches on a global level. When companies announce data breaches, they frequently inform the customers that the security systems have been breached by individuals or groups who may abuse the customers' private information. The private information often includes payment and other personally identifiable information. (Janakiraman et al. 2018.)

The number of cyberattacks done to individuals and firms has been increasing over the years. Despite this, organizations often have a low budget on information security measures. The consequences of data breaches remain almost unnoticeable to the senior executives and board of directors in organizations. These consequences include increased consumer perception of risk and erosion of brand equity. Moreover, managers need to justify budgets. It is often difficult to calculate the costs of a system breach. Information breach costs include direct and enduring costs. A data breach does not only have an impact on downtime but also on loss of customers, brand equity, loyalty, and trust. (Choong et al. 2017.)

Firms are affected by two types of costs when a data breach happens: direct and indirect. An example of direct cost would be cleaning the systems of malware. Indirect costs refer to intangible costs such as reputation loss after public announcement of data breach. It is especially difficult to calculate how much the indirect costs are. (Laube et al. 2016.)

Cavusoglu, Mishra & Raghunathan (2004) have argued that after a data breach is announced publicly, the indirect costs exceed the direct costs.

According to Janakiraman et al. (2018), costs that have been associated with data breaches are often related to recovery costs such as hiring people to fix the problems caused by the data breach, paying fines, losing revenue, paying for credit monitoring services for customers, and spending money on public relations.

A large amount of data regarding data breaches is not available. Organizations do not always want to reveal information, because it could produce additional costs. A data breach announcement may create costs that take forms such as financial market impacts, reputation or confidence effects, litigation concerns, liability concerns, signal to attackers, and job security. The costs that follow a disclosure may be significant and could have an immediate impact after a data breach announcement. (Cashell et al. 2004.)

Data breaches have financial market impacts. A data breach announcement may cause the stock markets, credit markets, and bond rating firms to react in a negative way, which raises the cost of capital to reporting firms. Privately held firms that are not active in public securities markets may also be negatively affected if they are believed to be increasingly risky by banks and other lenders. (Cashell et al. 2004.) Studies in the field of information systems have investigated data breach announcement effects from the perspective of stock market reaction. One study found out, that on average, a public firm lost 2.1% of its market value within two days after announcing about the data breach (Cavusoglu et al. 2004).

The amount of trust a consumer has toward a brand can be eroded by negative news or crises. In addition, the brand image may suffer in the eyes of consumers by these factors (Dawar & Pillutla 2000). A data breach announcement may reduce the organization's reputation and damage the brand. Additionally, customers may have a less confident relationship with the organization. These effects may then cause the competitors to gain a competitive advantage. (Cashell et al. 2004.) Even though firms spend resources to build reputation and brand, a data security incident may have a large negative impact on the firm's reputation, customer relationships, and customer acquisition costs (Janakiraman et al. 2018).

Investors, customers, and other stakeholders may try to sue the breached company. An organization that has had previous data breaches may be facing larger risks in the court

due to negligence of cybersecurity. Additionally, officials of an organization may face severe sanctions. Data breach announcement may give a signal to potential attackers that the security systems have weak points, further increasing the risks for additional breaches. The employees taking care of IT systems may be unwilling to reveal a data breach for the sake of their employment. (Cashell et al. 2004.)

Having access to valuable data is important in business. Depending on the type of business, the valuable data may include information such as medical records, credit card numbers, trade secrets, and data stored on the cloud. The data may be compromised intentionally or unintentionally, disrupting the business and damaging its assets and reputation. Due to this reason, organizations should dedicate resources to protection from security incidents. For example, prevention of security incidents includes maintaining regular backups, keeping software up to date, and educating employees which may help in reducing potential errors. (Sarabi, Naghizadeh, Liu & Liu 2016.) Preventing cyberattacks is one of the most important elements, but due to evolving cybersecurity threats, marketing managers should be prepared in damage control if a cybersecurity threat occurred. Therefore, a data breach response plan is critical if a data breach occurs (Janakiraman et al. 2018.) Even though data breaches may be prevented to some degree, total protection from data breaches is not possible. Therefore, it is necessary to have damage control and recovery strategies regarding data breaches. These strategies help to protect the firm value after a data breach has occurred. (Gwebu, Wang & Wang 2018.)

Allocating resources to data protection may be a difficult task, because there are numerous attack methods. Several projects have collected information related to data breach incidents to analyze most common attacks. The reports may help organizations to invest in data protection in a more optimal way. It is important to notice that all businesses should not be treated the same when discussing about data breach attempts, because different businesses may be vulnerable to different types of data attacks. For example, a medical institution with a lot of workers may be more vulnerable to data loss caused by human error, while a company hosting a cloud server may be more vulnerable to denial of service attacks or hacking. (Sarabi et al. 2016)

A study focusing on voluntary risk factor disclosure as a damage control mechanism suggests that when the firm disclosed action-oriented security risk factor before the data breach occurred, the market audience reacted with less negativity when the data breach was announced (Wang, Kannan & Ulmer 2013). According to Choi et al. (2016), three types of justice perceptions, which include distributive, procedural, and interactional

justice. These together affect the following consumer's psychological responses: perceived breach and feelings of violation. Distributive justice refers to perceived fairness of outcome, procedural justice refers to perceived fairness of the procedure, and interactional justice refers to perceived fairness of the interpersonal treatment. The psychological responses were found to be important in post data breach behavior, which includes word of mouth and likelihood of switching. Therefore, the authors suggest that recovery actions should target the justice perceptions. (Choi et al. 2016.)

Bansal & Zahedi (2015) found that issuing an apology to the customers is a working technique after a data breach has happened. Denial may also work as a strategy depending on the situation and it is recommended over not taking any action (Bansal & Zahedi 2015). Gwebu et al. (2018) found in their study that firm reputation has importance in protecting firm value during a data breach. Firms with lower reputation suffer more negative returns after data breach disclosure compared to firms with superior reputation. A smaller amount of response strategies is effective in protecting firm value when applied by lower reputation firms, and response strategies matter less for firms with higher reputation. (Gwebu et al. 2018) Goode et al. (2017) found in their study that compensation is a valid recovery action for a data breach. The compensation has positive effects on continuance intention, perceived service quality, and repurchase intention. However, overcompensation may have a negative effect on customer outcomes.

Businesses frequently communicate privately by email with customers who have been affected by the data breach after it has been publicly announced. The emails usually include information on how the firm will respond to the incident. Additionally, the emails aim to notify the customers about the data breach and what the customers need to do next to minimize the harm the customers could experience due to the data breach. The customers' concerns regarding the breach and misuse of personal information may be amplified by this type of communication. Customers who open and read the emails related to the DBA incident may react strongly, because they may perceive an imminent threat to their personal information. Therefore, the sense of data vulnerability may be amplified by being exposed to emails from the firm after the data breach. (Janakiraman et al. 2018.)

If a multichannel retailer is breached in one channel, the retailer may emphasize this in its marketing communication while trying to reduce negative consequences of the data breach that could affect other channels. Some customers may stop doing business with the retailer, whereas other customers try different ways to do business with the retailer

while waiting for trust to be restored. It is then viable for these customers to shop from an alternative channel, if the channel has not been breached. (Janakiraman et al. 2018.)

It is important to reduce negative consequences associated with the data breach, but the company should additionally invest in building trust with consumers. Managers should pay attention to customers' perception of data vulnerability in order to influence the customers' responses to data breaches. Because the negative effects of data breach announcement decrease over time, it is implied that immediate actions should be taken in the early stage of the crisis. Furthermore, high-patronage customers are mainly providing traffic during the early stages of the data breach announcement, and therefore the retailers should initially try to maintain customer loyalty while dealing with the crisis. (Janakiraman et al. 2018.)

2.5. Data breaches from consumers' perspective

Consumers frequently share private information with retailers while using their services. There exists a psychological contract in this relationship. Therefore, the data breach announcement may be viewed as a breach of psychological contract and a violation of trust. (Malhotra & Malhotra 2011.) Purchasing a product from a retailer includes a tangible product and an augmented product. The augmented product includes all the other benefits a consumer receives from product purchase and consumption (Levitt 1981). Consumers expect that their personal information is kept safe by the retailers and this is thought to be part of the augmented product. Data breaches can be interpreted as a firm service failure. Also, when a data breach happens, customers will experience anxiety and data vulnerability, whether the data is abused or not. When a company announced a data breach, it reduced customers spending by 32.45%, decreased purchase trips by 20.28%, and decreased product purchases by customers by 22.31% over a period of seven months. (Janakiraman et al. 2018.)

According to Lee & Lee (2012), consumers start to use retreative behavior after an online store is breached. This retreative behavior includes avoiding the breached store, switching to another online store, and using offline stores. The negative effects related to the breach remain mostly in the online context, and the consumers may use the offline stores. According to Berezina, Cobanoglu, Miller & Kwansa (2012), security breaches had a significant negative impact on the following variables: satisfaction, likelihood of recommending a hotel, revisit intentions. These variables were affected negatively even

though the hotel guest's credit card was not misused. According to Chakraborty et al. (2016) trust is not the only predictor in consumers' online shopping behavior. Consumers purchase online even when the trust level is low. Other elements such as attitude toward online business may have an influence on customers' decisions in the context of online transactions. The authors found in their study which included older people and young adults that beliefs related to trust in online shopping services and attitude toward online business influence post data breach shopping intentions.

Retail patronage has been linked with favorable customer attitude toward firms. Customers having positive attitude toward a retailer may diminish the effects of negative information connected to the retailer. Additionally, customers with a stronger relationship with the retailer is often familiar with the retailer's products, prices, and customer service. Therefore, the switching costs may be higher (Janakiraman et al. 2018.) Moreover, negative news related to the retailer that are inconsistent with the customers' preferences may not be considered as relevant from the customers' perspective (Xiong & Bharadwaj 2013).

Curtis et al. (2018) find it interesting that while data breaches lower consumers' trust, the consumers do not change their security related behavior. Specifically, after a company experiences a data breach, the users of the company do not always tighten their security. This finding adds evidence to former studies that consumers do not feel responsible for their own security while using a company's website which requires confidential information. There are a few possible explanations for this lack of behavioral change. First, consumers may think that data security should be managed by the company which services are used. Second, data breaches are perceived to be rare and creating and remembering complex passwords takes a lot of effort. Third explanation is related to learned helplessness, which means in this context that data breaches are out of the consumers' control, and they cannot personally prevent attacks or data leaks. (Curtis et al. 2018.)

If there is a lack of transparency in the aftermath of a data breach may have a straining effect on the relationships between customers and shopping websites. The customers may learn that their personal information has been stolen or misused, for example, by checking their bank statements. Reports from the news media may also reveal possible data breaches (Chakraborty et al. 2016.) A study conducted by Muzatko & Bansal (2018) found that when companies delay their announcement of a data breach, they may suffer an increased drop of consumer trust compared to companies that announce the data breach

without delay. Moreover, companies that are willing to quickly disclose about the data breach when it is discovered may be in a better position to repair trust to pre-breach levels. The act of withholding information may be viewed as a sign of untrustworthiness from the customers perspective.

Perceiving a hacking incidence to be severe contributes to the customers' perceived online shopping risks. Moreover, perceiving the hacking incident to be severe affects the customers post breach shopping intentions. (Chakraborty et al. 2016) Scopes of the data breaches vary and may affect a few or many customers. Moreover, scope of the data breach affects repurchase intention in different ways depending on the consumers experienced emotion. The emotions that were studied in this study include fear and anger. If the experienced emotion is fear, it leads to feelings of less control and increased uncertainty related to the situation. Threat assessment of fearful consumers is significantly affected by the scope. For example, they may fear that what has happened to others may happen to them. Scope indirectly affects fearful consumers repurchase intention. If the experienced emotion is anger, it leads to feelings of control and less uncertainty about the situation. Angry consumers' threat assessment is not affected by the scope. Moreover, angry consumers repurchase intention is not affected by scope. (Chatterjee et al. 2019.)

3. PRIVACY CONCERNS IN ONLINE BUSINESS

This chapter discusses topics of general information regarding privacy, privacy concern, perspectives on consumers' concern for online privacy, privacy concern and privacy paradox, and (online) self-disclosure. In the end, the summary of theory is presented.

3.1. General information regarding privacy

Consumers, who are active online, usually measure the risks associated with online activity, especially matters concerning privacy misuse or reveal (Milne & Culnan 2004). The consumers are interested in how much they can trust the websites when sharing information (Schoenbachler & Gordon 2002). According to Wu, Huang, Yen & Popova (2012), multiple studies indicate that the consumers' concerns over privacy and trust are factors that slow down the e-commerce. The sales force is an important player when developing customer trust outside of e-commerce. However, in an e-commerce context where the trust assumes a crucial role, the sales force may not be available (Wu et al. 2012). It is anticipated that if customers' concerns regarding the risks associated with online activity can be addressed, increased e-commerce may be conducted (Odom, Kumar & Saunders 2002). Despite this, completing a transaction may be difficult or impossible without sharing personal data, even when the third party is trusted. The research suggests that the consumers' willingness to share personal information online is a major issue in e-commerce. Additionally, consumers' concern over trust and privacy may influence how successful e-businesses will be. (Wu et al. 2012.)

Privacy has been an important subject for a long time, even before computers started appearing in households. One definition for privacy is "the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude, and their behavior to others". (Wu et al. 2012.) Anonymity is another important concept related to privacy. The Internet has affected users by decreasing their ability to remain unidentified. (Wu et al. 2012.) While using the Internet, consumers leave detailed electronic footprints which include their behavior and preferences. These footprints may be obtained, used, or shared by other users or strangers. (Zviran 2008.) The Web technologies are developed rapidly, and this creates new ways for invading Internet users' privacy. Moreover, while the consumers are being active online and provide personal information in different ways, they have no control over their secondary use of this

information. For example, more than half of large US firms were monitoring their employees' e-mail activity in 2004. (Wu et al. 2012.)

The World Wide Web made it easier for companies to expand their businesses globally. For example, the businesses created online shops, online auctions, business to business and business to consumer platforms. E-commerce provides the opportunity for consumers to access online services, product information, and faster communication. However, large amounts of individual data about users is gathered and used by companies. This process happens through registration forms, order forms, tracking software, or cookies. This information allows businesses to analyze the users' online behavior and personal preferences. The information is utilized by the companies to identify the customers' demands, create more effective advertisements, and increase the sales of advertising space on their websites. (Wu et al. 2012.)

The more traditional ways of collecting data have been quite arduous, which has generally helped to protect consumers' privacy to a certain extent (Blanchette & Johnson 2002). However, the increased development of technology-based systems has affected the amount and the quality of information that can be gathered. Moreover, the information may be investigated and analyzed in progressively advanced ways. (O'Connor 2006.)

Privacy concerns influence individuals' online behavior. This means that the individuals are less willing to disclose information, less willing do online shopping, and staying off the Internet. The concern over privacy may have a limiting effect on the development of e-commerce. Furthermore, another outcome may be that the consumer database will not be complete or accurate enough, which means that the businesses will target potential customers inaccurately, waste their efforts, and frustrate their customers. (Wu et al. 2012.)

Numerous researchers view trust as being important in increasing the growth of the e-commerce. This may be particularly true for consumers who are not technically sophisticated (Grabner-Kraeuter 2002). A large factor to improve relationships between consumers and businesses is to build trust which reduces consumers' privacy concerns (Milne & Boza 2000). Consumers' willingness to share information is related to concerns over privacy. One way to reduce the consumers' concern over privacy and to increase trust is to create a privacy policy. For example, the privacy policies may explain the customers how their personal information will be used, what kind of security tools the website uses, and how the website is protected. (Wu et al. 2012.)

3.2. Privacy concern

The term online privacy means how personal information is gathered and utilized in the online context. Consumers often need to provide their personal information when using online companies' services. In addition, companies may use the consumers' personal information to improve customer relationship management. However, when the consumers are asked to provide personal information to these companies, this request may increase the consumers' privacy concerns. Consumers' privacy concern means that an individual has concern for personal information which may be misused, and this may lead to different negative outcomes. (Choi et al. 2018.) Jung (2017) states that individuals' privacy concern is triggered when they perceive that their privacy is violated by unauthorized parties or when the individuals lose control of their personal information. A definition for privacy concern is "individuals' beliefs about the risks and potential negative consequences associated with sharing information." (Baruh, et al. 2017). Privacy concern is often viewed as a predictor to privacy management, which includes activities such as sharing information online, utilizing privacy protective behaviors, use of online services, and use of social networking services (Baruh et al. 2017).

Since there is a possibility that the companies misuse the consumers' personal information, the consumers may avoid providing personal information whenever this option is available. If an individual has a high level of privacy concern, s/he may not provide personal information so easily to an online vendor. (Choi et al. 2018.) A few studies have suggested that privacy concern affects how willing individuals are to disclose personal information in different online contexts (Dinev & Hart 2006; Taddicken 2014).

The role of privacy concern and intention to disclose personal information as its outcome has been examined in many studies (Choi et al. 2018). However, there are various protective responses to privacy invasion that consumers can take other than the disclosure of personal information. For example, an individual who has a high level of privacy concern may refuse to use a company's services if the company is threatening the individual's privacy. Additionally, the individual may remove personal information from the company or complain to the company. (Son & Kim 2008.)

While some users may have coping behaviors when their privacy is threatened, some users do not respond at all. Disengagement means that the individual reduces his/her effort to deal with a stressor and even giving up achieving a goal because of the stressor. Furthermore, disengagement may finally lead to withdrawal from activities.

Disengagement in the context of online privacy means how much users reduce their efforts with coping behaviors when their privacy is threatened. This means, for example, that the individuals do not want to use coping behaviors, remove their personal information from a company, fake their personal information, spread negative information about the company, and complain to the company or a third-party organization. (Choi et al. 2018.)

Online consumers who value privacy will not provide their personal information to companies that are perceived to be a threat to the consumers' privacy. If the consumers' personal information is mishandled in some way and they find out about it, the consumers may take actions to reduce the threats. For example, the user may remove personal information or complain to the company. This may be explained by using the expectancy theory, which means that individuals try to minimize negative consequences and maximize positive consequences. People estimate expected outcomes by weighing costs and benefits of decisions. (Choi et al. 2018.) Similarly, consumers analyze whether it is worth to disclose information in the online context. This is also known as privacy calculus. (Dinev & Hart 2006.) When users have privacy concerns, they lead to coping behaviors when faced with privacy threats. Research suggests that users who are considered as having low privacy concern would be more likely to reduce their coping behaviors. (Son & Kim 2008.)

3.2.1. Perspectives on consumers' concern for online privacy

The following factors have been studied and found to influence consumers' overall privacy concerns: personal experiences related to the use of the Internet, socio-demographic factors, trust in other people and institutions, and political orientation and ideology. (Bergström 2015.)

Internet consumption practices and the reasons why consumers use the Internet affect the online privacy concerns while using digital media (Bergström 2015). When the user has more experience in using the Internet, s/he may perceive less risk while shopping online, fewer concerns related to system security, and possible fraud that may happen in the online environment. However, the user usually has more concerns regarding online privacy. (Miyazaki & Fernandez 2001.) Furthermore, there is no conclusive data on whether users are more concerned about privacy after experiencing a fraud (Jensen, Potts & Jensen 2005). Consumers may not be willing to adopt online banking because of

security risks. For example, consumers may view the risk of fraud or identity theft as reasons for not to use online banking. (Lee 2009.) Fogel & Nehmad (2009) found in their study that greater risk-taking attitudes are related to people who have profiles on social media. In comparison, those who do not have profiles on social media have a lesser risk-taking attitude.

Various demographic factors may have importance in the context of risk perception and concerns in digital media use (Bergström 2015). According to Fogel & Nehmad (2009), men have a greater risk-taking attitude compared to women. The study shows that women have more privacy concerns than men. Additionally, women disclosed less identity information than men. Jensen et al. (2005) reported in their study that women answered being more concerned about privacy than men, but women were under-represented in the study and therefore the result is not statistically significant. According to Baruh et al. (2017), there is only a limited amount of studies available related to the moderating role of gender, and these studies have provided conflicting results.

Age may influence online privacy perceptions, but the findings are not consistent in the research. A few studies have shown that the age has only a small or no impact on privacy concerns (Bergström 2015). However, study conducted by Blank, Bolsover & Dubois (2014) found that there is a negative relationship between age and privacy. The younger people in the study were more likely to manage their privacy protection compared to the older people. According to Elueze & Quan-Haase (2018), younger users participate in online activities despite privacy concerns. However, older adult users' privacy concerns are a factor that reduces their willingness to adopt and engage with digital media. Concern for online privacy and education level has been less researched (Bergström 2015). A study suggests that consumers who are less educated are less concerned of online privacy, and consumers who are highly educated are more likely to utilize privacy protection (Blank et al. 2014).

Metzger (2004) states in the study that trust does predict user disclosure behavior to a website. Moreover, privacy concerns are significantly affected by trust. Similarly, Chellappa & Sin (2005) found in their study that building trust is negatively related to privacy concerns. The authors suggest that online vendors should not only concentrate on users' privacy concerns but try to find ways to build trust. However, Okazaki, Li & Hirose (2009) found in their study related to mobile advertising that even though there is a modest link between privacy concern and trust, trust has only a small impact on perceived risk. According to Bergström (2015), the factor of trust has the same kind of inconsistency

in research as the demographic factors have. Nevertheless, Bergström (2015) found in her study that the higher the levels of trust individuals had in other people, the less concern they had for privacy issues.

Perceived online privacy may be additionally viewed from a political perspective (Bergström 2015). Yao, Rice & Wallis (2007) explain that privacy is deeply rooted in Western culture. Privacy concerns could be examined from a different perspective. Privacy is often viewed from a legal point of view rather than from the individual's perspective which consists of beliefs and values. People have different views on privacy rights. The individual's subjective view of right to privacy may include many areas of life, including the Internet. The study's result suggests that beliefs regarding right to privacy and desire for privacy are linked with online privacy concerns. The authors explain that an increased desire for privacy outside of the virtual context and stronger belief in the right to privacy are likely related to increased online privacy concerns. (Yao et al. 2007.)

Bergström (2015) explains that consumers' digital privacy concerns are more strongly related to personal applications such as debit cards and social media. For example, e-mailing or searching for information online do not cause the same type of concern. A possible explanation for this is that consumers are used to working with these tools, and they are considered necessary in working life and everyday life. The usefulness of these tools may surpass the potential privacy issues. According to Bergström (2015), there exists only a small amount of research related to political ideologies and privacy concerns and contributes to this context by finding in her study that individuals who are left-oriented are more concerned about privacy issues compared to right-oriented individuals.

3.2.2. Privacy concerns and privacy paradox

For a long time, privacy research has primarily concentrated on why individuals are willing to disclose information about themselves in the online context while being worried about privacy. The concept of privacy paradox was developed to explain differences of information sharing behavior between adults who have privacy concerns and teenagers who are willing to self-disclose. This concept has begun to include the conflict between individual attitudes and behavior in the online context of privacy. Privacy concern has been studied quite extensively and it has often been reported to have a weak effect on online self-disclosure and protective behavior (Hoffmann et al. 2016.)

Various researchers have attempted to explain privacy paradox and why individuals disclose personal information while having notable privacy concerns (Hoffmann et al. 2016). According to Lee, Park & Kim (2013), users disclose information by weighing benefits and risks. In the study, the results revealed that benefits and risks affected the users' intention to share information on social network services. However, it was notified that expected benefit had a stronger effect on the intention to share information compared to the expected risk. Hoffmann et al. (2016) state, that when making the decision to disclose personal information, the users use their own judgment on what is perceived as a threat to privacy.

The concept of user trust is another attempt to approach the issue of online self-disclosure despite privacy concerns (Hoffmann et al. 2016). Perceived control and trust in online social network provider reduce perceived risk of information disclosure. If the user feels that s/he is being in control, it also enhances trust in the online social network provider. (Krasnova, Spiekermann, Koroleva & Hildebrand 2010.) According to Jarvenpaa, Tractinsky & Vitale (2000) study's results, the amount of trust a consumer has toward an online store depends on the perceived size and reputation of the store. Moreover, the reputation had a greater effect on trust than perceived size. According to Hoffmann et al. (2016), even though users disclose personal information to the online services, there is only a small amount of evidence that the users would trust these services.

Lack of risk-awareness and not understanding how the individuals may cause harm to themselves when sharing information online is another explanation why individuals choose to provide personal information even though they might have notable privacy concerns. The explanation from this perspective is that a lot of users do not understand the privacy risks that are related to the online context. One reason for the users' lack of understanding of privacy risks in the online context may be because of not having proper digital skills. (Hoffmann et al. 2016.) Boyd & Hargittai (2010) found in their study that young users began to increasingly modify their privacy settings on Facebook between 2009 and 2010. This was at the time when there was a lot of discussion about Facebook's approach related to privacy. The authors found that how frequently the participants used Facebook, how they used Facebook, and Internet skills are correlated with privacy management.

Hargittai & Litt (2013) found in their study related to a diverse group of young adults that there are patterns related to online privacy management. The study found that these

patterns are related specifically to job search. The results imply that women, white people, and people with higher Internet privacy skills are more active in managing their online self-presentation. A study conducted by Park (2013) suggest that younger users are more skillful in privacy control compared to older users. In addition, the research discovered that privacy control behavior is strongly predicted by user knowledge. The three dimensions related to this user knowledge are technical familiarity, surveillance awareness, and policy understanding. According to Hoffmann et al. (2016) privacy or literacy skills may be better in predicting privacy behavior more accurately than privacy concerns. A study conducted by Bartsch & Dienlin (2016) found that experience with the Internet leads to increased online privacy literacy. Furthermore, this affects the users to behave more cautiously regarding privacy on social networking services.

Privacy concerns and privacy paradox has been approached in different ways, including Dienlin & Trepte (2015) study. In this study, the authors included a multidimensional approach to privacy in their study. The dimensions included informational, social, and psychological privacy. According to Young & Quan-Haase (2013) study, individuals have social privacy concerns. The social privacy concerns were managed by creating strategies to counter these social privacy concerns. On Facebook, the strategies included, for example, limiting the information on profile, or not accepting friend requests from strangers. However, only a small amount of concern was shown for institutional privacy. The individuals had no strategies to protect themselves from how the institutions might use their personal data. According to Hoffmann et al. (2016), users may perceive social privacy concerns to be accessible and understandable.

Although privacy paradox has been examined and confirmed in different studies, there exists some evidence that privacy concern has a statistically significant but weak effect on online behavior (Kokolakis 2017). Therefore, the evidence related to privacy paradox may be considered as mixed (Hoffmann et al. 2016). In a systematic review of the privacy paradox literature carried out by Kokolakis (2017), there was more evidence that the privacy paradox existed. Still, the evidence that supports paradox may weaken over time, as more variables are taken into consideration. After an increasing amount of new data and theory is added to the context of privacy concern studies, the discussion about the privacy paradox may stop in the future. (Hoffmann et al. 2016.)

Hoffmann et al. (2016) argue that when users have limited Internet literacy and skills, this affects the users by not allowing them to accurately calculate the benefits and potential costs of an online transaction. Hoffmann et al. (2016) continues by stating that even

though user trust may explain why users underrate institutional privacy risks, there does not exist enough evidence for users having an adequate level of trust in data intensive online services. Furthermore, large companies that provide Internet services, such as Facebook and Google, have questionable reputations. This could imply that people have institutional privacy concerns and mistrust for these types of companies. (Hoffmann et al. 2016.)

Even though there are several studies that have examined why privacy concerns do not necessarily reflect the privacy management choices made by users, there is a growing amount of studies reporting a noticeable relationship between privacy concerns and privacy management behavior. For example, in the context of e-commerce, privacy concerns are related to protective behaviors such as deleting cookies, removing personal information from commercial databases, and not disclosing information. (Baruh et al. 2017.)

Baruh et al. (2017) found in their meta-analysis that privacy concerns were associated with reduced intentions to use online services, although privacy concerns did not significantly affect the intention to use social networking services. The actual behavioral outcomes were similar. Users who had high privacy concerns did not often use online services, while no significant relationship between privacy concerns and utilization of social networking services was found. The intentions to share personal information by users who had higher privacy concerns were weaker, and their intentions to utilize privacy protection measures were greater. Similarly, the behavioral outcomes indicated that users who had higher privacy concerns shared smaller amount of personal information, and applied privacy protection measures more often. (Baruh et al. 2017.)

Baruh et al. (2017) state that even though the concept of privacy paradox suggests otherwise, privacy concerns seem to predict to some degree which individuals are willing to use online services and whether they utilize privacy management. Moreover, the effect typically seems to be small or moderate. However, privacy paradox seems not to apply for the use of social networking services. Privacy concerns were not significantly associated with the use of social networking services when examining from the perspective of intentions and behavioral outcomes. From the perspective of user motivations and risk-benefit analysis, one explanation for this may be that the social networking services fulfill the users' expressive needs in a better way when compared to other forms of online services. Thus, even though the users have privacy concerns, they may continue using the social networking service. (Baruh et al. 2017.)

3.3. (Online) self-disclosure

Andrade, Kaltcheva & Weitz (2002) define self-disclosure as "the quantity and quality of personal information that an individual provides to another". Masaviru (2016) defines self-disclosure as an act where the individual reveals personal information that is unlikely to be known without being shared. The information may touch upon topics that would not be shared with particular people (Masaviru 2016). According to Mothersbaugh, et al. (2012), self-disclosure means that an individual shares personal information to an entity and this information may include things such as name, preferences, and demographics. This information may also include things such as thoughts, feelings, and experiences (Bauer & Schiffinger 2015). It is argued whether all verbal or non-verbal that is connected to revealing information about self is self-disclosure. Not all self-disclosure has to be deep to be useful. Small talk may be considered as superficial self-disclosure and it is often used as a tool to initiate relationships, which may then lead to deeper levels of personal information sharing. (Masaviru 2016.)

What information individuals share about themselves depends on the context. For example, self-disclosure in dyads could serve to increase mutual understanding. Moreover, self-disclosure in groups may increase trust between group members, enhance group membership, and strengthen group membership. An individual may need to disclose personal information to authenticate their identity when dealing with an organization. On the other hand, organizations may request personal information from individuals for advertising or some other business-related reasons. Reciprocity is considered as an important aspect of self-disclosing behavior. Reciprocity in this context refers to the mutual exposure of communication partners. The reciprocity would happen in a situation where a disclosure of one partner would be followed by a disclosure by the other partner. (Bauer & Schiffinger 2015.)

The domain of human-computer interaction is interested in self-disclosure for multiple reasons. It is considered important for various web-based services that specifically target the individuals' preferences. Disclosing information to the organizations may show that the individual trusts the organization. Because there is a lack of face-to-face interaction online between organizations and customers, the organizations often have to rely on such feedback behavior. (Bauer & Schiffinger 2015.)

Mothersbaugh et al. (2012) define online self-disclosure as "individual's willingness to reveal personal information to a firm online". Self-disclosure that happens online may

take different forms such as sharing demographic related information or answering web surveys which measures customer attitudes and preferences. Additionally, online self-disclosure happens when an individual has to register and provide personal information to gain access to a website. This is type of online self-disclosure would be referring to an authentication process. Moreover, online self-disclosure is required while purchasing from an online shop if the user wants to make transactions using a credit card. Another example related to online self-disclosure during authentication would be while using online bank services. Online self-disclosure while using social media refers to what kind of information the users reveal of themselves to others. (Wakefield 2013.)

When observing self-disclosure from a commercial point of view, the theories suggest that consumers make assessments of the costs and benefits when deciding whether to disclose information. Companies use different approaches to modify the costs and benefits thinking style when interacting with consumers online. Specifically, the approaches aim to encourage the consumers to disclose information. (Shih, Hsu, Yen & Lin 2012.) The companies may offer rewards to consumers in exchange for self-disclosure, increasing subjective benefits, or offer better privacy protection to reduce the consumers' subjective costs for self-disclosure (Andrade et al. 2002). Some amount of data about customers may be collected without their permission or awareness, but data that could be used in customized marketing or advertising requires personal input that is collected usually by willing participants. This type of data is related to intentional self-disclosure, where the participant willingly provides some type of personal information to another. (Wakefield 2013.)

While self-disclosure is required in many processes, online users may not always be willing to provide some types of information in the Internet. For example, consumers understand that providing shipping and billing address while purchasing something is needed for receiving the item, but answering a survey related to past purchases on the same website may be perceived to be too private, personal, or risky to reveal. Likewise, when a website asks for the user's email address in exchange for content, some users may be hesitant to provide it because they are afraid of receiving spam email. This leads the user to search for the content from other sources. Online businesses require user data to provide better content and services while boosting sales, but customers may be unwilling to provide personal information in order not to suffer from unwanted consequences. (Wakefield 2013.)

Researchers have categorized negative consequences associated with disclosure into two categories. Moreover, these categories are defined as the loss of privacy and the loss of face. (White 2004.) Generally, embarrassment is related to concern for what other people think about us. Consumers may feel embarrassment in retail context if a purchase signals other people some undesirable information about the individual. The loss of privacy means concern for who has the personal information and how the personal information is used. Furthermore, the effect of loss of privacy may be reduced when the consumers perceive that they have control over who has the information and how it is going to be used. (Wakefield 2013.)

A possible cost or a risk may be that when the consumer gives information to a company, the information is used in a way that is detrimental to the consumer (Andrade et al. 2002). For example, a company may pass consumer's information to a third party that begins sending unwanted advertisements to the consumer (Shih et al. 2012). Because the online environment lacks social cues, this might promote dishonesty from the online users when asked to provide personal information. From the companies' perspective, it is important to detect the amount of false information that is provided by the users to improve their services. (Metzger 2004.)

Certain types of personal information requests from websites may affect consumers' risk and privacy perceptions differently (Wakefield 2013). People may be more willing to provide information regarding their interests, attitudes, opinions, and work-related information. In contrast, self-disclosure related to deep emotions, insecurities, or financial and health information are topics that people may be less willing to share. Consumers may be willing to discuss online about certain topics without difficulties, but these topics may be different on the Internet compared to face-to-face conversations. Furthermore, this behavior may occur because of the unique risks involved in e-commerce transactions and lack of social cues. (Shih et al. 2012.)

Information sensitivity has been discussed as a contributing factor to the level of uncertainty or risk that occurs with information disclosure (Angst & Agarwal 2009). Potential losses associated with self-disclosure include psychological, physical, or material aspects. For example, self-disclosure could cause embarrassment, loss of health, and loss of financial assets. (Mothersbaugh et al. 2012.) Research has also shown that information relevance significantly influences privacy beliefs (Wakefield 2013). If consumers are asked to disclose irrelevant information in a process or exchange, they are likely to perceive increased privacy risk and reduced privacy protection (Li, Sarathy &

Xu 2011). Consumers define costs related to the disclosure of personal information. Moreover, these costs vary depending on the personal information that is requested (Wakefield 2013).

3.4. Summary of theory section

The number of data breach attempts is on the rise and the impact of a data breach varies from minor to major damage depending on the situation. Both consumers and organizations suffer from the attacks. Data breaches may be considered a global threat or at least a threat to anyone who is connected online. There is a variety of ways how data breaches may be committed and the people who commit these breaches have different reasons for doing it, although it seems that hacking for financial reasons is the favored way of committing data breaches. The organizations have increased the reporting of data breaches, but still a large amount of data breach information is not released, because informing about data breaches may create additional costs, although there are laws that require the company to report about the data breaches. Additionally, many organizations do not know whether they are breached until much later. Similarly, the consumer may not know whether his/her personal information has been stolen and is currently being misused. If a company is breached, this generally affects consumers' attitude and behavior negatively including avoidance of the company, reduced trust, increased switching behavior, negative word-of-mouth, and reduced intention to do business with the company. The consumers' level of negative attitude and behavior may depend also on the breached company's actions during the breach and after the breach. The data breaches do not seem to affect consumers' security related behavior.

Privacy is an important factor for consumers. To use different online services or to buy something online, the user generally must disclose personal information. What consumers choose to disclose generally depends on the situation. For example, self-disclosure has been connected to weighing costs and benefits, and trust. Factors such as privacy concern and trust may affect the consumer's decision whether to do business with a company or use a service. Moreover, privacy concern may affect protective behavior, such as self-disclosure, in e-commerce context. Additionally, trust may also influence consumers' privacy concern by reducing it.

In the light of the background, this thesis aims to increase our understanding of consumers' attitudes and behavior related to data breaches.

4. METHODOLOGY

This chapter provides insight into the methodology used in the study. The topics include research method, research approach, data collection and sample, analysis of the data, ethics related to the research, and reliability and validity of the study.

4.1. Research method

Primary research methods may be quantitative or qualitative. Quantitative research goal is to quantify gathered data and applying various statistical analysis, while qualitative research includes providing insight and understanding the problem in a deeper way. (Chrysochou 2017: 412.)

Qualitative and quantitative methods differ from each other, and they are used for different purposes. While qualitative methods' purpose is to explore and understand a phenomenon deeply, quantitative methods' purpose is to test hypotheses, create predictions, and generalize results. The sample in qualitative methods is usually small and often involves unstructured data. In contrast, the sample in quantitative methods is large, may represent the population, and the data is usually structured. Additionally, qualitative methods are not aiming to generalize the results, while quantitative methods are more proper in generalizing the results. (Chrysochou 2017: 412.) Because this study aims to provide insight and in-depth understanding of consumers' attitude and behavior related to privacy and data breaches, the study is qualitative in nature.

Consumer behavior research is related to social and real-life phenomena, and this may be difficult or complex to explain and analyze. Research methods related to consumer behavior often aim to explain and provide reasoning behind a phenomenon, rather than only making accurate predictions. Moreover, predictions are involved with errors, and the purpose of a research method is to minimize these errors. Statistical significance should not be the researcher's only target, but s/he should focus on the significance of the effect and overall importance of the findings. (Chrysochou 2017: 426.)

This study is exploratory. Exploratory study is related to finding out what is happening, seeking out new insights, and asking questions to assess phenomena in a new way. If there is a need to clarify a problem, for example, what is the precise nature of the problem,

exploratory study may be useful. Other benefits that are related to exploratory research include flexibility and adaptability to change. Moreover, the focus may be broad in the beginning, and while the research progresses, it becomes narrower. Additionally, the study in this thesis is cross-sectional, which means that phenomena are studied at a particular time. (Saunders, Lewis & Thornhill 2009: 139-140, 155.)

4.2. Research approach

There are two general ways to approach a qualitative analysis. These commonly used approaches are called deductive and inductive approaches. Deductive approach means that existing theory is used to mold the approach towards the research process and to various aspects of analyzing data. On the contrast, inductive approach is used to create a theory from the collected data. It is mentioned that studies may mix both approaches, and this may even be likely to happen. While using an inductive approach, elements of deductive approach may be combined while seeking to develop a theoretical position. Then, the position's applicability may be tested using subsequent data collection and analysis. (Saunders et al. 2009: 489-490.) This study uses inductive and deductive approaches. This means, for example, that the existing theory related to data breaches and privacy was influencing the author while doing the interviews and analyzing the data. Saunders et al. (2009: 159) call this a hybrid approach, when, for example, an established theoretical construct helps the researcher to understand the findings.

4.3. Data collection and sample

The data was collected using semi-structured interviews. Semi-structured interviews include having a list of questions or themes that the researchers want to cover. The questions may vary between interviews. Some questions may be considered more important in one interview than others. Moreover, the researcher may change the order of the questions or add new questions depending on the how the discussions progress. Because of the nature of this type of interview, the discussions are recorded, and the researcher may take notes. (Saunders et al. 2009: 320.)

Semi-structured interviews give the researcher tools to probe for deeper answers. Specifically, the researcher may probe to gain deeper explanation for the interviewees' answers. Because the terms or ideas conveyed by the interviewees may be difficult to

understand, probing is a tool that helps the researcher to gain understanding about what the interviewees mean. Probing may lead the conversations to new areas, which the researcher might not have thought about before. These new areas may bring valuable information to the study. Interviews may also bring light to the interviewees' own understanding of how they think. Thus, the researcher may be able to gather a set of detailed data. (Saunders et al. 2009: 324.) As many of the interviewees who participated in this study used different ways to answer the questions, probing was a useful tool to gain deeper understanding into what they meant. Additionally, the interviewees may have answered shortly, but probing would help the interviewees to discuss further about the topic. For example, if the interviewee answered with a short yes or no, the interviewer would ask the participant to elaborate why. Furthermore, sometimes the participant would get lost while answering the questions and s/he would ask the interviewer to repeat the question or clarify the question.

The study uses semi-structured interviews to gather participants' opinions and behavior related to the research objectives. It involves exploring and understanding the phenomena, includes a small number of participants (10), verbal responses, aims to find patterns, features, and themes. The behavior may not be assessed in its natural environment in this study, but the participants' answers are interpreted. Chrysochou (2017: 426) states that personal judgment and experience is required while investigating a phenomenon, and there is a researcher bias involved with the results because of subjectivity. Therefore, this bias should also be considered while doing the research.

This study involves purposive sampling. This means that the researcher chooses the sample with specific requirements in mind (Panacek, Thompson 2007). The author chose this to have a varying sample of interviewees. The sample includes men, women, and interviewees representing different age groups. The purposive sampling was chosen to get a general overview of consumers' attitudes and behaviors related to data breaches. It is important to note that there could exist a bias in this way of sampling, because of the specific participant selection (Panacek et al. 2007). All the participants chosen for the study are Finnish, because nationality could be an additional factor that could affect the results of the study. Therefore, to eliminate this factor, all the chosen participants are Finnish. The interviews were conducted in Finnish.

The interviewees must have fulfilled some requirements before being accepted to the study. These requirements were that the interviewee must have used their personally identifiable information for online services, for example, bought something online or used

a social media account in the last 6 months. In addition, the interviewee must be at least a semi-active internet user, which means that the interviewee is not cut off from online activities. Because most of the interviewees were contacted using Facebook, they were accepted immediately. Two participants who were contacted by phone were asked if they fulfilled these requirements and they agreed. One participant was asked face to face if he would fulfill the requirements.

These interviews were conducted during October in 2019. The interviews were conducted using Facebook messenger, Skype, Discord, or phone. In addition, the interviews were conducted at suitable times for the participants. On average, an interview lasted approximately 25:11 minutes. The shortest recorded interview was 13:19 and the longest interview was 32:26. Next, the sample is presented.

Table 1. Sample

Gender	Age	Education	Position	Average daily Internet usage
Male	26	Secondary education	-	5-6 hours
Male	28	Secondary education	Demand planner	2 hours actively
Male	34	Bachelor of Culture and Arts	Product owner	5-6 hours
Male	42	Bachelor of Business Administration	B2B salesman	Work + 1½ hours out of work
Male	51	Bachelor of Business Administration	Security specialist	2 hours
Male	65	Bachelor of Science Degree in Chemistry Bachelor of Science Degree in Pharmacy	Retired	3 hours
Female	24	Secondary education	Trainee	2-3 hours
Female	27	Master of Science in Economics and Business Administration	Marketing manager	Work + 1-2 hours out of work
Female	37	Secondary education	Instructor (Practical nurse)	3-4 hours
Female	51	Secondary education	Executive assistant	Work + passively almost all the time

4.4. Analysis of the data

The data was analyzed using qualitative content analysis. This method is used to systematically and objectively describe and quantify a phenomenon. Moreover, theoretical issues may be tested to understand the data. The method allows the researcher to put words into content-related categories. Furthermore, it is assumed that the words and phrases share the same meaning after being classified into the categories. Content analysis offers replicability and validity and the purpose is to provide knowledge, insights, and facts. The method aims to attain condensed and broad description of a

phenomenon, and the results include concepts or categories describing the phenomenon. (Elo, Kyngäs 2008.)

After recording, transcribing, and printing the interviews, the author began to read through the transcriptions and color code different parts of the transcriptions. The author had decided to search for attitudes and behaviors related to the data breaches in the data. The color coding was done to match the interviewees' answers to the thesis' objectives. The colors were for the following categories: yellow – attitude, red – behavior, blue – explanations for an attitude or behavior. Because the attitudes and behaviors are quite general, the author began to find similarities in these categories and how many times they occurred in the data. Then these attitudes and behaviors were condensed into smaller categories that are revealed in the findings and results. Afterwards, the results were compared to the theory that is in the literature section.

4.5. Ethics related to the research

According to Saunders et al. (2009: 160), it is important to consider the ethics related to the collection of data. While collecting the data, the interviewees were notified what the interview includes, for example, what kind of topics are going to be discussed about. The participants were asked whether they would be fine with providing all the information and that it would be published in the thesis. This way the participants could choose whether they wanted to proceed with the interview. Additionally, the author told the interviewees that the data would be kept private, only the necessary information would be published.

4.6. Reliability and validity of the study

Reliability in the context of research means that whether the data collection techniques and analysis procedures will be able to produce the findings consistently. There exist four threats related to reliability including subject or participant error, subject or participant bias, observer error, and observer bias. Subject or participant error refers to whether the interview would bring different results depending, for example, on the mood of the participant. Subject or participant bias refers to that the participant may be telling what their boss might want them to answer. Observer error means that, for example, three researchers could use three different ways to ask a question, and observer bias means that

there would be three different ways to interpret the answers (Saunders et al. 2009: 156-157.)

There are some reliability issues regarding the use of semi-structured interviews. Two main biases include interviewer bias, and interviewee bias. Interviewer bias relates to how the interviewer asks the questions, including the tone, comments or non-verbal behavior. This may create a bias how the participant responds. The questions might be asked in a non-neutral way or there could be bias involved in the way the interviewer interprets the answers. There could also be a lack of trust between the interviewer and the interviewee, which could make the interviewee hesitant to give proper answers. Interviewee bias means that the interviewee might be participating, but not revealing all the necessary information. This may be, for example, because the participant is unwilling to discuss about sensitive information, or that the interviewer is seen as untrustworthy. The interview may also be seen as time-consuming, which could make some possible interviewees hesitant to apply for the interview, causing a bias to the sample. (Saunders et al. 2009: 326-327.)

Validity in qualitative research refers to how appropriate are the tools, processes, and data. Moreover, this includes appropriateness and validity in the relationship between the research question and the outcome, methodology and the research question, design and methodology, sampling and data analysis, and results & conclusion and sample & context. (Leung 2015.) Saunders et al. (2009: 157), state that validity refers to whether the findings are true.

There exist four logic steps related to validity. These are identification of the research population, data collection, data interpretation, and development of conclusions. Identification of the research population refers to whether the study's conclusions are generalizable to the whole population. For example, if the research is about the National Health Service, it would probably not be accurate to generalize the results to some software houses. Data collection refers to the validity of the collected data, whether the participants who apply for the study are appropriate for gathering proper data. Data interpretation refers to, for example, the appropriateness of the theory used in the study. The theory that is used in a study will shape the conclusions. Development of conclusions refers to whether the conclusions can withstand close examination. (Saunders et al. 2009: 158-159.)

Saunders et al. (2009: 326-327) have discussed about the validity of qualitative interviews. Generalizing the findings from qualitative interviews may be an issue. However, the validity of these kinds of studies is not an issue. Validity in semi-structured interviews is related to how much knowledge the interviewer gains from the interviewee, and how accurately the interviewer can interpret the interviewee's answers. To gain a high level of validity, the interviews must be conducted properly. For example, paying attention to clarifying the questions, using probing, and discussing the topics from different angles. The small sample related to semi-structured interviews will not be enough to make statistical generalizations. (Saunders et al. 2009: 327.) The results in this thesis are not aimed to be generalizable, but to gain increased understanding of consumers' attitudes and behaviors related to data breaches. The semi-structured interviews were conducted using many questions from different angles in the context of the study. Probing was used to gain further knowledge from the interviewee. The theoretical background in this thesis is chosen subjectively by the author, which may cause validity issues. Due to the interpretative nature of this study, there may be issues related to the accuracy of the interpretations.

The author notes that the interviews were done while the participants had spare time, which could make the participants more willing to give accurate answers. This means that the participants would be more relaxed. Some of the interviewees are working in companies involved with information technology, which might involve some bias, because these participants might think that they should know proper answers to the questions. Another bias may be related to the fact that the author knew many of the participants to some degree before the interview. They could give "socially appropriate" answers to the questions. This means that the participants may have answered differently, because of this relationship. On the other hand, the participants may have been more truthful with their answers, because the author is not a stranger. Another factor that could reduce the bias is that all the interviewees and the author are Finnish. This would reduce problems with the use of language, because the participants could answer in their mother tongue. Because the interviews were not conducted face-to-face, some elements could not be seen such as body language. However, the interviewees might also be more comfortable in giving answers being alone in a relaxed place.

5. FINDINGS

This chapter presents the key findings from the gathered data. First, this part of the thesis presents the findings related to how the knowledge of data breaches affect consumers' attitudes and behaviors. Afterwards, the findings related to the consumers' attitudes and behaviors towards companies that have experienced a data breach are reported.

5.1. Attitudes and behaviors related to knowledge of data breaches

This section includes attitudes and behavior related to the knowledge of data breaches. First, the section begins with describing reasons that cause concerns, and reasons that reduce concerns related to the knowledge of data breaches. Afterwards, other attitudes are reported. Finally, different behaviors related to the knowledge of data breaches are reported.

5.1.1. Attitudes related to knowledge of data breaches

The results indicate that there are various concerns caused by the knowledge of data breaches. The concerns relate to misuse of important personal information, unawareness of how the personal information is being used, being a data breach victim today, data security services, and future data security trends.

On a general level, most of the participants reported that there are concerns for the chance that the participants' personal information is misused. What is important personal information is subjectively decided, but it may include information such as payment information, and social security number. Other personal information that cause concern in this context include different account and password details related to online environment. The news has increased some participants' concerns in this context.

> *"I think that every time I give my credit card information somewhere… I would not have to read soon from the media that the company where I entered my information… that it would have been breached"* (Male, 42 years)

Similar to the previous theme, the data indicates that unawareness of what happens to the personal information causes concern for some of the participants, or if something has happened to the personal information. For example, a few participants explained that it is concerning that somebody could steal your identity without your knowledge, or you suddenly receive a bill to your house, and you do not even notice it. When the personal information has been shared knowingly or unknowingly, the participants may not have the knowledge if a data breach has happened.

> *"It causes anxiety that you do not necessarily even know that your information or identity has been stolen"* (Male, 34 years)

Many participants mentioned being concerned of being a data breach victim today. The concern levels range from slightly to quite concerned. This concern is related to increased awareness due to the knowledge of data breaches, doing business with foreign companies, and increased amount of services that require your personal information. Some participants' answers are more or less specific, but they imply concern for being a data breach victim today.

> (Answering whether the participant is concerned of experiencing a data breach today) *"Quite concerned… let's say this way that the understanding is increased all the time"* (Male, 34 years)

> *"I cannot say that I would be very concerned… there is an increasing amount of services that need the Internet and the more your information is in different places, the higher the chance (for data breaches)"* (Male, 51 years)

Another concern is related to security services. Knowledge about data breaches causes the concern due to understanding how different companies have been breached previously. The security services may be related also to personal use. Additionally, perceiving how easy it would be to gather the personal information by someone knowledgeable, if some hacker wants the information, s/he will get it.

> *"On some level, I should gain more trust for security services, I still do not trust them… if a hacker necessarily wants to get your information and the hacker has chosen you as a target, then unfortunately I have the belief that the hacker will dig the information and you cannot do anything about it"* (Male, 34 years)

The data breaches have affected a few participants' concerns about future security trends. This means that while everything is evolving technologically, including security systems, the criminals gain new ways to commit data breaches. Moreover, what is seen as safe today may be something else tomorrow. The answers are a bit different though, one participant views the trend as "depressing" while the other participant's answer implies stoic attitude.

> *"This is a competition between security measures and measures how the criminals try to get this information… it really is not black and white… what today is seen as safe may be tomorrow… you do not know"* (Male, 51 years)

The results indicate that there are various reasons that may reduce the concern for data breaches. These reasons are related to trusting "larger" or well-known companies and laws, believing there is only a small chance of being a victim, and believing that the consequences of a data breach are insignificant.

Many participants mention that they trust, or that you should be able to trust larger companies in managing the customers' personal information in a proper manner. For example, one participant always does shopping in larger firms or well-known brands that the participant believes to be trustworthy. Other participant mentions that the company will suffer severe consequences if it is revealed that the customer information is leaked from the company. Trusting that the companies follow the law was also mentioned. For example, the GDPR seems to increase this trust.

> *"I just trust that if the companies are large, they have these matters in order… it is important for them to keep the customers' information safe, because otherwise the whole garbage will fall down, if it would be revealed that the information has been leaked from there"* (Female, 51 years)

> (Answering whether the participant is concerned whether an online company or service provider can keep the personal information safe) *"I am not concerned, because this new data security protection law (GDPR) was implemented, it is quite strict"* (Female, 37 years)

One reason for reduced concerns is believing that there is only a small chance of being a data breach victim. This includes the belief that it would not be possible to experience

something like this, not wanting to worry about a chance that is extremely small, believing it is very unlikely to experience a data breach, or believing that the data breach is a "distant" possibility.

> *"I do not want to worry about everything… unnecessarily about an extremely small chance"* (Female, 51 years)

Other reason that may reduce concerns for data breaches is believing that the consequences of a data breach are insignificant. Some participants who have experienced a data breach describe that only small amount of damage was done due to the data breach, such as when they lost their payment information and it was used to buy something online. The participants were provided compensation. For example, the bank contacted one participant and the payments were compensated. One participant mentions that even though there are increasingly more services that require your personal information, the personal information is often very general, so the damage that could be done is very minor.

> *"My credit card was used to do shopping, and this was revealed to me when the bank contacted me… called me and the card was cancelled… nothing serious really happened because I was compensated"* (Female, 27 years)

Outside the context of concerns, the attitudes include being personally responsible for security, being careful, and being sceptic. The attitude of indifference is discussed in the end.

The results indicate that the knowledge of data breaches has affected some of the participants in being personally responsible for security. Some reasons for this attitude is that the news have affected to behave much more carefully and that the participant is responsible for his own security, understanding that sharing personal information in a "stupid" way may cause troubles, or considering if it is smart to disclose important personal information when some party asks for it. Somewhat similar to the previously mentioned attitude, many participants answered being more careful due to the knowledge of data breaches. For example, one participant mentions being more carefree years ago. Other answers include, for example, being more careful due to the news, and being careful where to share personal information.

> *"I am aware in a sense that I must act more carefully… that you yourself are quite responsible for your own security"* (Male, 28 years)

> (Answering whether the news about data breaches has affected the participant's online behavior) *"It has slightly increased carefulness after reading"* (Male, 26)

Finally, a few participants mentioned being more sceptic as a result of the knowledge of data breaches. For example, the news has affected one participant to be more sceptic, whether the participant dares to share the information. Other participant mentioned that while being abroad, the participant needs to be more sceptic while paying, an attitude which may be related to her previous data breach experience.

> *"(The news) have increased skepticism… do I dare to share the information"* (Male, 42 years)

The data indicates some level of indifference to the data breaches. However, it is not clear whether the indifferent attitude is caused due to the knowledge of data breaches, or if the attitude exists despite the knowledge. Some level of indifferent attitude was implied in many of the participants' answers, even though at the same time they may have attitudinal or behavioral changes. The indifferent attitude is revealed, for example, that some of the participants are not really concerned about data breaches, it is not a daily concern, or there are so much more concerning things in daily life. This some level of indifferent attitude may also be related to perceiving that there is a small chance of experiencing a data breach. For example, the interviewees may believe the data breach to be a "distant" event. The indifferent attitude is revealed in other ways also. Many participants answered that they have not been in contact with a company that has experienced a data breach. Moreover, many of these participants were contacted for the interview using Facebook, and this company has experienced data breaches. An explanation for this may be that the participants know or believe that they have not been personally involved in the data breach, so their answers may reflect this. The level of indifference does not generally seem to be high, but some of the answers imply indifferent attitude.

> (Answering if the participant is concerned today about being a victim of a data breach) *"I am not really concerned… I do not really think about this in daily life… I have a lot of other things in daily life"* (Female, 37 years)

(Answering has the knowledge of data breaches from the news affected the participant's behavior) *"It does not affect… if something happens then there is nothing you can do about it"* (Female, 51 years)

5.1.2. Behaviors related to knowledge of data breaches

The behavioral changes due to the knowledge of data breaches are related to what to self-disclose, where to self-disclose, password management, and payment behavior.

Most participants answered that their self-disclosure behavior has been influenced due to the knowledge of data breaches. Due to the knowledge of data breaches, many of the participants have chosen to share only the necessary information while interacting with companies, purchasing something, or using social media. Some specific answers include deleting payment information after purchasing something, not sharing important personal information to places where it does not belong, ignoring optional fields when filling forms, reduced use of Facebook. Furthermore, the behavioral change includes chatting more carefully online, for example, not discussing about personally important information. Additionally, some participants answered observing generally how they share their personal information while being online.

"I try to share only the necessary information, nothing additional. If some field is optional, then I leave it unfilled" (Male, 28 years)

"I discuss more carefully… I generally do not discuss about personal information over there (WhatsApp)" (Male, 34 years)

Similarly, the participants are more attentive on where to disclose their personal information. This includes behavior such as investigating the company before doing business with it, for example, by visiting message boards to find other users experiences with the company, using Google to search information about the company, or asking friends if the company is trustworthy. One participant mentioned that she investigates whether the competitions on Facebook are fake, before participating in them. Some of the participants' answers imply that while purchasing something online, they choose to purchase from a company that they personally believe to be trustworthy.

> *"I search background information of the company and if I find some issues from some message board etc. then I at least have to be more careful"* (Male, 51 years)

Some participants answered changing their password management due to the knowledge of data breaches. It is important to note, that these participants have previously experienced a data breach, which may affect this behavior, although one participant answered that the news have also affected this behavior. The passwords are created differently to each service, password generators are used, and the passwords have been changed after a company notifies about a data breach.

> (Answering whether the news about data breaches has affected the participant's online behavior) *"It has in a sense that I pay much more attention on passwords and different services… the passwords are very different in different services as they should be"* (Male, 28 years)

A few participants mentioned being more careful with payment information. For example, the participants may choose to use other payment method than credit card while purchasing something.

> (Describing credit card purchases) *"If there is some other way, I try to use it"* (Male, 42 years)

5.2. Attitudes and behaviors toward a breached company

This section includes attitudes and behaviors related to companies that have experienced a data breach. The section begins with whether a participant would or would not do business with a company because of a data breach, and whether a participant has stopped doing business with a breached company. It continues with whether a participant would sign in or not in a service that has been breached recently. It should be noted that the participants' answers included mixed answers. For example, the participant would generally do business with a company, but if X happens, s/he would not do business.

Reasons for doing business with a company include getting a specific product or service that is not available elsewhere, believing that the breach may not be the company's fault, and believing that the consequences of a data breach are insignificant for the participant.

Furthermore, some of the interviewees mentioned that their intention to do business with a breached company requires deep consideration.

The results show that if a company can offer a service or product that is only available in this specific company, most participants would do business with the company. Some of the reasons include that if the product or service is a "must-have" or vital, then this would encourage the participant to do business with a breached company. The participants' answers imply hesitance, but if it would be necessary, they would do it. In this case, one participant noted paying extra attention on the payment method. Some of the participants would generally not want to do business with a breached company, but in this case they would or consider it.

> *"If the situation was normalized, managed, protected, and it would be something that would be necessary… For example, to get a password or an identification document or something using the internet… It would be necessary to do then."* (Female, 51 years)

> *"If I really need the product and I cannot get it elsewhere… I think it would be necessary then… but if I have any other option to be without the product, I would be."* (Male, 42 years)

The results indicate that before doing business with a breached company, the participants would deeply consider whether continuing or beginning to do business with the company. Some of the participants' answers include "requiring serious consideration" or "reconsidering". Additionally, the participants would investigate the company or try to get convincing answers from the company. Moreover, the participants' answers imply that they do personal "risk analysis" or weighing cons and pros, whether doing business with the breached company would be worth it.

> *"This is kind of related to risk analysis… I could take the risk… I think this depends on the risk level"* (Male, 65 years)

Believing that the company is not responsible for the data breach may be a reason for doing business with the company. A few participants argue that the company might not be responsible of the breach. If the company has done necessary security management and a data breach happens, the participants consider it as not a significant reason for them to stop doing business with the company.

> *"If the company has worked with the information that is available today… and despite this, a data breach has happened… I do not see a problem in this case"* (Male, 51 years)

Believing that the consequences of a data breach are insignificant seem to convince some of the participants to do business with a breached company. This may be related to earlier experiences with data breaches, where the participants noted that there have only been minor consequences. The answers imply that if the attitude may be different in the future, depending on whether the data breaches are personally more significant.

> *"I do not believe that I would quit doing business… Sometimes this can happen, but there have not been any serious consequences at least for now."* (Female, 27 years)

The results show some reasons for not doing business with a company, including trust issues, company's indifferent attitude to the possibility of a data breach, and because of concerns for possible misuse of personal information. The results indicate that some of the participants have trust issues after a company experiences a data breach. These trust issues may convince the participant not to do business with the company. Because the security has been breached, it reduces the trust.

> *"I would not do business if the company has experienced a breach… I believe that quite possibly I would stop doing business with the company… because the trust would be gone"* (Male, 42 years)

Earlier it was shown that a data breach may not be the company's fault and due to this the participants will do business with the breached company. On the contrast, if the company has had an indifferent or sloppy attitude to the possibility of data breaches, some of the participants may not want to do business with the company.

> *"If it appears that the company has clearly had an indifferent attitude toward consumers, it tells me that I do not want to do business with the company"* (Male, 51 years)

Another reason for not doing business with a breached company is related to concerns about misuse of important personal information. The answers imply that due to the data

breach, the participant would be worried of losing personal information to wrong hands. One participant noted that if he had previously used a payment card with the company, he would consider not doing business with the company.

> *"I would quit doing business if I got that information… I do not want to do business with that kind of company… I would be afraid that my information would be misused"* (Male, 65 years)

The results show that only one participant answered having stopped doing business with two companies due to his accounts being breached that were connected to the companies. Many of the participants have not stopped doing business with a breached company due to not having experience with a breached company, or not knowing whether a company has experienced a data breach. However, the author wants to notify here most of the participants who answered like this were interviewed using Facebook, which has experienced data breaches. The reasons why other participants who perhaps know about a breached company and have not stopped doing business with it include believing that it is not necessarily the company's fault, and because of insignificant consequences.

In a more specific context related to companies and their services, the results indicate that few participants would sign-in a service that has been breached lately, although the participants would wait until they believe it is safe to use the service or they are given the information that it is safe to use.

> *"I would possibly stay safe for many days and not sign-in… until the specific company would show green light that the service is usable… I would kind of passively wait until there is more understanding about the situation"* (Male, 28 years)

A few others answered that they would sign-in and often the companies ask the users to at least change their passwords. It is important though, that the data breach has been fixed before signing in.

> *"Some service may have notified me that they have experienced a data breach and it has not really affected how I use the service… I may have changed my passwords in case of if I have been one of the persons whose information has leaked somewhere"* (Female, 27 years)

The results showed two main reasons not to sign-in in a service that has been breached lately: Trust issues because of the breach and concern for misuse of personal information. One participant notifies that it depends on services, but if the service is “shady” or “smaller”, the participant would have less trust to them and making the participant less hesitant to sign-in.

> *“I would try to avoid it because of its trustworthiness… I cannot trust that my information would not leak from there… so they would not experience a data breach again”* (Female, 37 years)

6. CONCLUSION

This chapter presents key findings, practical implications, and limitations and suggestions for future research.

6.1. Key findings

In the beginning of this thesis, the research question was presented. The research question in this thesis is:

How do data breaches affect consumers' attitudes and behaviors?

The results suggest that the data breaches affect consumers' attitudes and behaviors in many ways. The knowledge of data breaches causes concerned attitude. These concerns include concerns for misuse of personal information, concerns for being unaware how the consumers' personal information may be used, concerns for being a data breach victim today, concerns for data security services, and concerns for future security trends. Reasons that reduced the concerned attitude include trusting the companies and laws, believing there is only a small chance of experiencing a data breach, and believing that the consequences of data breaches are personally insignificant. Other attitudes related to the knowledge of data breaches include being personally responsible for security, being careful, being sceptic and being indifferent. Furthermore, knowledge of data breaches affects self-disclosure, password management, and payment behavior.

The data breaches affect the intention of doing business with a company that has experienced a data breach. The intention to do business with a company that has experienced a data breach relates to getting a specific product or service that is not available elsewhere, believing that the company may not be responsible for the data breach, believing the consequences of a data breach to be personally insignificant, and believing that deep consideration has to be done before doing business with this company. The intention not to do business with a company relates to trust issues, believing that the company has been indifferent towards customers, and having concerns for misuse of personal information. The data breaches affect the intentions to signing-in a service that has been breached. The reasons to sign-in include waiting until it is believed to be safe to

sign-in and believing there is a need to change the password. Reason not to sign-in a service is related to reduced trust and concerns for misuse of personal information.

Next, the results are discussed in detail. The first objective of the thesis is how the knowledge of data breaches affects consumers' attitudes and behaviors. Many interviewees answered that they have concerns for misuse of personal information. According to Jung (2017), losing control of personal information and perceiving that information is being accessed without permission activates privacy concerns. Similarly, the results in this thesis indicate that the interviewees generally have concerns for the misuse of their personal information, due to the knowledge of data breaches. Data breaches mean that unauthorized parties have access to confidential information and in this context the consumers are not in control of their information. For example, reading the news related to data breaches has caused this concern for some of the interviewees, and the concern for misuse of personal information is often related to information such as payment information and social security number.

Some of the interviewees answered that being unaware of what is happening to their personal information causes concerns. Albrecht et al. (2011) have stated that the victim of a data breach may be unaware that his/her personal information has been stolen and is currently being misused. The results in this thesis indicate that the interviewees seem to be concerned, because they do not know if their information is currently being misused and whether the personal information has been stolen. For example, the explanations included that the interviewee might suddenly receive a bill because someone misused his credit card and he would not even notice the misuse, or someone might be misusing the interviewee's identity today and s/he would not know about it.

The interviewees concerns included having concerns for being a data breach victim today, data security services, and future data security trends. Wheatley et al. (2016) have stated that IT security has difficulties in keeping up with the evolving cyber-crime techniques and that people should worry about constant privacy erosion. The results in this thesis indicate that many interviewees are indeed concerned for experiencing a data breach today due to the knowledge of data breaches. A few interviewees showed concern for the current data security services that are being used and whether these security services can keep their information safe. Similarly, a few of the interviewees are concerned about the future security trends. Furthermore, these interviewees stated that they are concerned about the increasing amount of data breach techniques and if the data protection technology can keep up with the criminals.

However, the results in this thesis indicate that some attitudes seem to reduce these concerns related to the knowledge of data breach. Many of the interviewees answered that trust is important while doing online business. Milne & Boza (2000) have reported that building trust between consumers and businesses reduce privacy concerns, and Metzger (2004) has stated that trust is a major factor influencing privacy concerns. The results in this thesis show that the reason for reduced privacy concern is connected to trust, especially trusting large companies or companies with "good image", and laws. The interviewees trust these "larger companies", which reduces their concerns related to the knowledge of data breaches. Some interviewees reported that these kinds of companies increase trustworthiness, and that the repercussions of a data breach would be very problematic for the companies. Therefore, the interviewees believe that the companies will do a lot to ensure that their data security would be working properly. As the laws related to data breaches have increased, the interviewees believe to be safer from data breaches. For example, GDPR was mentioned by some participants as reducing concerns. Due to the laws, the companies must have a stricter data security protection.

Some of the interviewees answered that they have less concerns because they believe data breaches are rare or their consequences are insignificant. Curtis et al. (2018) have explained that consumers may perceive data breaches to be rare. The results in this thesis indicate that some of the interviewees reported having reduced concerns related to the knowledge of data breaches, because they believe there is only a small chance of being a victim. Nevertheless, some of the interviewees who stated that they believe that there is only small chance of being a victim of a data breach had also previously experienced a data breach. Goode et al. (2017) have stated in their study related to data breaches that compensation may be used as an effective tool to positively influence customers' continuance intention and service quality perceptions. In this thesis, some of the interviewees thought that the consequences of data breaches were insignificant, and this would reduce their concerns related to the knowledge of data breaches. Furthermore, this seems to be related to their previous experiences with data breaches. For example, while some of the participants' payment information has been misused, they were compensated, and the process was reported to be rather easy. Therefore, believing that the data breaches cause insignificant consequences is related to the compensation.

Other reported attitudes include being personally responsible for security, being careful, being sceptic, and being indifferent. Curtis et al. (2018) have stated that after a company experiences a data breach, the users do not tighten their security or feel responsible for

their security. The results in this thesis show, while not strictly related to Curtis et al. (2018) reported context, that the knowledge of data breaches has enhanced some of the interviewees' responsibility for security. Likewise, the interviewees reported as being more careful due to the knowledge of data breaches. Specifically, being more aware of their privacy behavior. Some of the interviewees also mentioned being more sceptic, meaning a doubting attitude if it is safe to share personal information. Curtis et al. (2018) have explained that the data breaches may be perceived to be out of the consumers' control, and they cannot prevent the attacks and data leaks. Similarly, while the indifferent attitude was not strongly brought up in the results of this thesis, many of the interviewees' answers implied this. For example, it was explained that if something happens, then there is nothing you can do about it.

Most of the participants have changed their behavior due to the knowledge of data breaches. This includes self-disclosure behavior, password management, and payment method behavior. Baruh et al. (2017) have stated that privacy concerns are related to privacy management, which includes self-disclosure and protective behavior. Similarly, the results in this thesis suggest that due to the knowledge of data breaches and the privacy concerns that they have created, the interviewees have changed their information sharing and protective behavior. Furthermore, this provides evidence against the privacy paradox (Baruh et al. 2017). Many of the interviewees in this thesis informed that their self-disclosure behavior is stricter, for example, sharing only the necessary information and investigating the companies before doing business with them. Similarly, a few interviewees stated that choosing a suitable payment method instead of just relying on paying with a credit card, because of concerns related to misuse of the credit card. Curtis et al. (2018) have discussed how users do not change their security behavior after data breaches, but the results in this thesis imply otherwise. If the interviewee has noticed or has been notified about a data breach, the interviewee has at least changed the password related to the service.

The second objective in this thesis is related to the consumers' attitudes and behaviors towards companies that have experienced a data breach. First, the discussion begins with the intention to do business with a breached company. While many interviewees would not necessarily want to do business with a breached company, they would still deeply consider it depending on the circumstances. Other reasons for the intention to do business with a breached company include getting a specific product or service and believing that the consequences of a data breach are insignificant. Choi et al. (2018) have stated that individuals estimate outcomes by weighing costs and benefits when dealing with

companies, especially when considering privacy. The results in this thesis imply that both getting a specific product that is not available elsewhere and deep consideration are related to weighing costs and benefits of decisions. If the interviewee considers the product or service to be very important, then the interviewee is more willing to do business with the company and share the personal information. Some interviewees believe that the data breaches' consequences are insignificant, which would make them willing to do business. This is related to the interviewees' previous experience with the data breaches and compensation, as was stated earlier in the results.

A few interviewees stated that the company might not be responsible for the breach. Chakraborty et al. (2016) have stated that if the customer perceives a hacking incidence to be severe, it affects the customer's post breach shopping intention negatively. The results in this thesis show that believing that the company may not be responsible for the data breach increases some of the interviewees' willingness to do business with a breached company. This means that the company might have proper security, but it is still breached despite the efforts to protect the data. If some of the interviewees do not see the hacking incidence as severe, the interviewee may do business with the company.

The intention not to do business with a breached company is discussed next. Some interviewees mentioned that there are trust issues related to the intention to do business with a breached company. Chakraborty et al. (2016) have stated that trust related to online shopping affects significantly post data breach shopping intentions. The interviewees in this thesis stated that the trust would be gone due to the earlier data breach. Therefore, they would not want to do business with a breached company.

Some interviewees mentioned that if the company has had an indifferent attitude towards customers, they would not want to do business with the company. Chakraborty et al. (2016) have stated that if the consumers perceive the breached company's hacking incidence to be severe, their intentions to do business with the company is reduced. In this thesis some of the interviewees answered that if the company has had an indifferent attitude towards the customers, for example, ignoring customers' data protection, they would see this as a reason not to do business with the company. The interviewees would perceive the hacking incidence to be severe in this context, which reduces their shopping intention.

The results in this thesis show that concerns for misuse of personal information is related to the intention not to do business with a breached company. Consumers may not want to

disclose personal information or use online services, because of the privacy concerns (Baruh et al. 2017). In this thesis, many participants would not want to do business with a company that has been breached because of concerns related to the misuse of personal information. The breached company causes concerns, and because the interviewee must disclose information to the company to gain something, s/he would choose not to do it. However, most of the participants have not stopped doing business with a company, because they answered having not been involved with a company that has experienced a data breach.

A few interviewees stated that they would sign-in a service that has been breached. Curtis et al. (2018) have stated that consumers do not feel responsible for their security or tighten it. The results in this thesis show that a few of the interviewees would wait until it is safe to proceed or change passwords immediately. This means that the interviewees take care of their security by managing their passwords and paying attention on whether it is safe to sign-in. However, many interviewees would not sign-in a service that has been breached due to trust issues or believing that the interviewees' information may be misused. These two reasons were mentioned also in the context of intention to do business with a breached company. Malhotra & Malhotra (2011) have stated that data breach announcement causes a violation of trust, and Baruh et al. (2017) have stated that consumers may not want to use online services due to privacy concerns. In this thesis, many of the participants reported that their trust would be gone, and they would not sign-in. The data breach increases the privacy concerns and make the interviewee hesitant to sign-in. Similarly, the concern for misuse of personal information was expressed by some of the interviewees. They have concerns that their personal information would be leaked or stolen. This belief affects negatively the intention to sign-in a service that has been breached.

6.2. Practical implications

The results suggest various practical implications. The companies should pay special attention on customers' data protection, because many of the interviewees reported being concerned about misuse of personal information due to the data breaches. This may affect the consumers' self-disclosure behavior and make them less willing to do business with the company. Additionally, if the company experiences a data breach and the consumers believe that the company has had a proper data protection, they may have a forgiving attitude towards the company. If the consumers notice that the data breach has been

caused by having an insufficient data protection, the consumers may not want to do business over there. Despite this, many interviewees reported having reduced intentions to do business with a company that has experienced a data breach. Therefore, it is important to prevent the data breach in the first place. Additionally, it could be advisable to provide a reasonable compensation for those who have been involved in the data breach, although this depends on the scope of the data breach.

Some of the interviewees stated that they are concerned about how their personal information might be misused or not knowing whether their personal information has been misused. The companies should also pay constant attention to the data security systems for possible breaches. If the company provides services that require the user to sign-in and the service has been breached, it would be advisable that the company provides proper communication to the users about password management and whether it is safe to log-in. Additionally, the results provide resources for companies to consider what aspects of data breaches are most relevant for consumers. For example, some of the interviewees stated being concerned about misuse of personal information such as credit card and that these interviewees would choose other payment method instead. It would be advisable then to provide multiple payment methods for the consumers.

6.3. Limitations and suggestions for future research

There are various limitations in this study. The sample consisted of people with different backgrounds with the intention to have a varying overview on consumers' attitudes and behaviors related to data breaches, but the sample size is small. Even though the study included people from various age groups, there were no participants who are under twenty years old. This study only consisted of Finnish interviewees, so there might be differences with other nationalities. Because the interviewees' answers were translated from Finnish into English, there might exist accuracy issues with the author's interpretation. Also, the theoretical background and the results were subjectively chosen and interpreted by the author. This study provides a snapshot of the current attitudes and behavior related to data breaches. However, the attitudes and behaviors related to data breaches may change in the long run. Also, Saunders et al. (2009: 327) have stated that this kind of study cannot be used to make statistical generalization about the entire population.

Contrary to Curtis et al. (2018) findings, this study found that data breaches affected many of the interviewees by making them personally more responsible for security. Despite

this, the sample in this study was quite small and the results are not so generalizable. Also, this study did not specifically concentrate only on the privacy management. Nevertheless, this topic could be researched further. Some of the participants implied indifferent attitude in this study while at the same time having their attitudes and behavior affected by the data breaches. The indifferent attitude seemed to be slight, but still visible. The research could investigate this further, whether the consumers are truly indifferent. Specifically, if the consumers have an indifferent attitude, why and how the consumers are indifferent toward data breaches.

Because there are consumers who have experienced a data breach, future research could investigate how the attitude and behaviors of consumers who have experienced a data breach differ from those consumers who have not. Some of the interviewees in this study had personally experienced a data breach and it might have affected their attitudes and behavior compared to those who have not experienced a data breach. Many of the participants mentioned not having stopped doing business with a company, because they have not been involved with one. Future research could investigate consumers who have stopped doing business with a company because it has experienced a data breach, and why did they stop doing business with it. Additionally, this study only consisted of Finnish participants. Future research could compare people with different nationalities and their attitudes and behavior related to the data breaches.

REFERENCES

Albrecht, C., C. Albrecht & S. Tzafrir (2011). How to protect and minimize consumer risk to identity theft. *Journal of Financial Crime*, 18:4, 405-414.

Andrade, E. B., V. Kaltcheva & B. Weitz (2002). Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. *Advances in Consumer Research*, 29, 350-353.

Angst, C. & R. Agarwal (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33:2, 339-370.

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security*, 8:2, 33-56.

Bansal, G. & F. M. Zahedi (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, 71, 62-77.

Bauer, C. & M. Schiffinger (2015). *Self-disclosure in online interaction: A meta-analysis* [online]. 48th Hawaii International Conference on System Sciences [cited 26 August 2019]. Available from the Internet: <https://www.researchgate.net/profile/Christine_Bauer/publication/270593076_Self-Disclosure_in_Online_Interaction_A_Meta-Analysis/links/557cc84508aeea18b776a9f5/Self-Disclosure-in-Online-Interaction-A-Meta-Analysis.pdf>

Bartsch, M. & T. Dienlin (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, 56, 147-154.

Baruh, L., E. Secinti & Z. Cemalcilar (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67, 26-53.

Berezina, K., C. Cobanoglu, B. L. Miller & F. A. Kwansa (2012). The impact of information security breach on hotel guest perception of service quality,

satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, 24:7, 991-1010.

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, 55, 419-426.

Blanchette, J. & D. G. Johnson (2002). Data retention and the panoptic society: The social benefits of forgetfulness. *The Information Society*, 18:1, 33-45.

Blank, G., G. Bolsover & E. Dubois (2014). *A new privacy paradox: Young people and privacy on social network sites* [online]. Prepared for the Annual Meeting of the American Sociological Association, 16-19 August 2014, San Francisco, California [cited 26 August 2019]. Available from the Internet: <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/A%20New%20Privacy%20Paradox%20April%202014.pdf>

Boyd, D. & E. Hargittai (2010). Facebook privacy settings: Who cares? *First Monday*, 15:8-2.

Cavusoglu, H., B. Mishra & S. Raghunathan (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce*, 9:1, 69–104.

Cashell, B., W. D. Jackson, M. Jickling & B. Webel (2004). The economic impact of cyber-attacks. *Congressional Research Service*, 1-41.

Chakraborty, R., J. Lee, S. Bagchi-Sen, S. Upadhyaya & H. R. Rao (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.

Chatterjee, S., X. Gao, S. Sarkar & C. Uzmanoglu (2019). Reacting to the scope of a data breach: The differential role of fear and anger. *Journal of Business Research*, 101, 183-193.

Chellappa, R. K. & R. G. Sin (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6, 181-202.

Choi, B. C. F., S. K. Sung & Z. Jiang (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems*, 33:3, 904-933.

Choi, H., J. Park & Y. Jung (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42-51.

Choong, P., E. Hutton, P. S. Richardson & V. Rinaldo (2017). Protecting the brand: Evaluating the cost of security breach from a marketer's perspective. *American Journal of Management*, 11:1

Chrysochou, P. (2017). Consumer behavior research methods. In: Consumer Perception of Product Risks and Benefits, 409-428. Ed. Emilien, G., R. Weitkunat , F. Lüdicke. Cham: Springer. ISBN 978-3-319-50530-5

Curtis, S. R., J. R. Carre & D. N. Jones (2018). Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal*, 33:4, 425-435.

Dawar, N. & M. M. Pillutla (2000). Impact of product-harm crises on brand equity: The moderating role of consumer expectations. *Journal of Marketing Research*, 37:2, 215–26.

Dienlin, T. & S. Trepte (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology,* 45, 285-297.

Dinev, T. & P. Hart (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17:1, 61-80.

Elo, S. & H. Kyngäs (2008). The qualitative content analysis process. *Leading Global Nursing Research*, 62:1, 107-115.

Elueze, I. & A. Quan-Haase (2018). Privacy attitudes and concerns in the digital lives of older adults: Westin's privacy atittude typology revisited. *American Behavioral Scientist*, 62:10, 1372-1391.

Fogel, J. & E. Nehmad (2009). Internet social network communities: Risk raking, trust, and privacy concerns. *Computers in Human Behavior*, 25:1, 153-160.

Goode, S., H. Hoehle, V. Venkatesh & S. Brown (2017). User compensation as a data breach recovery action: An investigation of the Sony Playstation network breach. *MIS Quarterly*, 41:3, 703-727.

Grabner-Kraeuter, S. (2002). The role of consumers' trust in online shopping. *Journal of Business Ethics*, 39:1, 43-50.

Gwebu, K., J. Wang & L. Wang (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, 35:2, 683-714.

Hargittai, E. & E. Litt (2013). New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security & Privacy*, 3, 38-45.

Hoffmann, C. P., C. Lutz & G. Ranzini (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10:4.

Huq, N. (2015). *Follow the data: Dissecting data breaches and debunking myths* [online]. Trend Micro analysis of privacy rights Clearinghouse 2005-2015 data breach records. Trend Micro, 5-50. [cited 26 August 2019]. Available from the Internet: <https://documents.trendmicro.com/assets/wp/wp-follow-the-data.pdf>

Janakiraman, R., J. H. Lim. & R. Rishika (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, 82:2, 85–105.

Jarvenpaa, S. L., N. Tractinsky & M. Vitale (2000). Consumer trust in an internet store. *Information Technology and Management*, 1:1-2, 45-71.

Jensen, C., C. Potts & C. Jensen (2005). Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63:1-2, 203-227.

Jung, A-R. (2017). The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern. *Computers in Human Behavior*, 70, 303-309.

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computer & Security*, 64, 122-134.

Krasnova, H., S. Spiekermann, K. Koroleva & T. Hildebrand (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25, 109-125.

Laube, S. & R. Böhme (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, 2:1, 29-41.

Lee, M. C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, 8:3, 130-141.

Lee, M. & J. Lee (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. *Information Systems Frontiers*, 14:2, 375–393.

Lee, H., H. Park & J. Kim (2013). Why do people share their context information on social network services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, 71, 826-877.

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, 4:3, 324-327.

Levitt, T. M. (1981). Marketing intangible products and product intangibles. *Harvard Business Review*, 59:3, 94–102.

Li, H., R. Sarathy & H. Xu (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, 51:3, 434-445.

Malhotra, A. & C. K. Malhotra (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, 14:1, 44–59.

Masaviru, M. (2016). Self-disclosure: Theories and model review. *Journal of Culture, Society and Development*, 18, 43-47.

Metzger. M. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Meditated Communication*, 9, 1-24.

Mills, J. L. & K. Harclerode (2018). Privacy, mass intrusion and the modern data breach. *Florida Law Review*, 69:3, 771-830.

Milne, G. & M. Boza (2000). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Direct Marketing*, 13:1, 5-24.

Milne, G. & M. Culnan (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive marketing*, 18:3, 15-29.

Miyazaki, A. D. & A. Fernandez (2001). Consumer privacy concerns and preference for degree of regulatory control. *Journal of Advertising*, 38:4, 63-77.

Mothersbaugh, D. L., W. K. Foxx II, S. E. Beatty & S. Wang (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research*, 15:1, 76-98.

Muzatko, S. & G. Bansal (2018). *Timing of data breach announcement and e-commerce trust* [online]. MWAIS 2018 Proceedings, 7. [cited 26 August 2019]. Available from the Internet:<https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1006&context=mwais2018>

O'Connor, P. (2006). An international comparison of approaches to online privacy protection: Implications for the hotels sector. *Journal of Services Research*, 6.

Odom, M., A. Kumar & L. Saunders (2002). Web assurance seals: How and why they influence consumers' decisions. *Journal of Information Systems*, 16:2, 231-250.

Okazaki, S., H. Li & M. Hirose (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of advertising*, 38:4, 63-77.

Panacek, E. A. & C. B. Thompson (2007). Sampling methods: Selecting your subjects. *Air Medical Journal*, 26:2, 75-78.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, 40, 215-236.

Peretti, K. K. (2008). Data breaches: What the underground world of carding reveals. *Santa Clara Computer High Technology Law Journal*, 25:2, 375-413.

Sarabi, A., P. Naghizadeh, Y. Liu & M. Liu (2016). Risky business: Fine-grained data breach prediction using business profiles. *Journal of Cybersecurity*, 2:1, 15-28.

Saunders, M., P. Lewis & A. Thornhill (2009). Research methods for business students. 5th edition. Essex: Pearson Education Limited. ISBN 978-0273716860

Schoenbachler, D. & G. Gordon (2002). Trust and consumer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing*, 16:3, 2-16.

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

Shih, D-H., S-F. Hsu, D. C. Yen & C-C Lin (2012). Exploring the individual's behavior on self-disclosure online. *International Journal of Human-Computer Interaction*, 28, 627-645.

Son, J. Y. & S. S. Kim (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 32:3, 503-529.

Taddicken, M. (2014). The 'Privacy Paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-mediated Communication*, 19:2, 248-273.

Veltsos, J. R. (2012). An Analysis of data breach notifications as negative news. *Business Communication Quarterly*, 75:2, 192-207.

Verizon (2018). *2018 Data breach investigations report* [online] [cited 16 December 2019]. Available from Internet: <https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf>

Wakefield, R. (2013). The influence of user affect in online information disclosure. *Journal of Strategic Information Systems*, 22:2, 157-174.

Wang, T., K. N. Kannan & J. R. Ulmer (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, 24:2, 201-218.

Wheatley, S., T. Maillart & D. Sornette (2016). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, 89:7, 1-12

White, T. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology*, 14:1-2, 41-51.

Wu, K-W., S. Y. Huang, D. C. Yen & I. Popova (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, 28:3, 889-897.

Xiong, G. & S. Bharadwaj (2013). Asymmetric roles of advertising and marketing capability in financial returns to news: Turning bad into good and good into great. *Journal of Marketing Research*, 50:6, 706–24.

Yao, M. Z., R. E. Rice & K. Wallis (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, 58:5, 710-722.

Young, A. & A. Quan-Haase (2013). Privacy protection strategies on Facebook: The internet privacy paradox revisited. *Information, Communication & Society*, 16, 479-500.

Zviran, M. (2008). User's perspectives on privacy in web-based applications. *Journal of Computer Information Systems*, 48:4, 97-105.

APPENDIX 1. Interview questions

-Milloin olet aloittanut Internetin käytön?
-Paljonko käytät aikaasi Internetissä päivittäin?
-Mihin tarkoituksiin käytät Internettiä?
-Miten huolestuneeksi yksityisyydestäsi kuvailet olevasi, kun olet yhteydessä verkkoon?
-Oletko tänä päivänä huolestuneempi yksityisyydestäsi verkossa kuin vuosi sitten?
-Onko huolesi yksityisyydestäsi muuttanut tapaasi jakaa henkilökohtaista tietoa verkossa?
-Mistä tai minkälaisesta henkilökohtaisesta tiedosta olet eniten huolissasi?
-Oletko huolestunut siitä pystyykö verkossa toimiva yritys tai palveluntarjoaja pitämään henkilökohtaisen tietosi turvassa?
-Oletko halukas jakamaan henkilökohtaisia tietoja verkossa toimiville yrityksille ja palveluntarjoajille?
-Oletko päättänyt olla käyttämättä jotain verkossa olevaa palvelua tai jättänyt ostamatta jotain turvallisuushuoliesi vuoksi?
-Onko mitään tekoja mitä yritys voisi tehdä vähentääkseen turvallisuuteen liittyviä huoliasi?
-Tiedätkö mikä tietomurto on?
-Oletko kuullut tai lukenut tietomurroista jostain lähteestä?
-Onko tietomurtojen uhka lisännyt huolia, että henkilökohtaisia tietojasi käytettäisiin väärin?
-Oletko tietoinen jostain tietomurrosta, jossa olet ollut uhri ja johon on liittynyt henkilökohtaisia tietojasi? (Kyllä, kysymykset 1. 2. Ei, kysymys 3.)
1. Kuinka huolestunut olit, että olisit tietomurron kohde ennen kuin tietomurto tapahtui?
2. Kuinka huolestunut olet tänä päivänä, että joutuisit uudestaan tietomurron kohteeksi?
3. Kuinka huolissasi olet tänä päivänä, että olisit osallinen tietomurron kohteena?
-Lopettaisitko asioimasta lähiaikoina tietomurron kohteeksi joutuneen yrityksen kanssa?
-Oletko lopettanut jonkin yrityksen kanssa asioimisen siitä syystä, että se on ollut tietomurron kohteena?
-Voisitko kirjautua verkossa olevaan palveluun tai sovellukseen, jos se olisi lähiaikoina joutunut tietomurron kohteeksi?
-Jakaisitko henkilökohtaisia tietoja verkkokauppaan, jos se olisi viime aikoina joutunut tietomurron kohteeksi ja tämä yritys olisi ainoa tapa hankkia jokin tuote tai palvelu?
-Ovatko tietomurrot vaikuttaneet tapaasi hallita henkilökohtaisia tietojasi verkossa?
-Oletko muuttanut tapaasi käyttää sosiaalista mediaa tietomurtojen vuoksi?

-Onko mitään tekoja mitä yritys voisi tehdä tietomurron jälkeen, jotka vakuuttaisivat sinut jatkamaan tai aloittamaan yrityksen palvelujen käytön?
-Olisitko halukas maksamaan yrityksille paremmasta turvallisuudesta liittyen henkilökohtaisiin tietoihisi? Jos kyllä, miten paljon?