Noora Etelä

COPING WITH PERSONAL DATA BREACHES IN HEALTHCARE

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Etelä, Noora
Coping with personal data breaches in healthcare
Jyväskylä: Jyväskylän yliopisto, 2021, 69 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaajat: Soliman, Wael; Siponen, Mikko

Nykyinen tietoyhteiskunta pitää dataa arvokkaana resurssina. Valitettavasti tämä tarkoittaa, että myös laiton datan hyväksikäyttö on kohtuuttoman yleistä. Verkkorikolliset pitävät terveystietoja arvokkaimpina, ja siksi tietomurrot koskevat suhteettomasti terveydenhuoltoa. Tutkittaessa tietomurtotapausten vaikutuksia, nykyinen kyberturvallisuustutkimus priorisoi usein organisaation näkökulman yksittäisen uhrin näkökulman sijaan. Tämä tutkimus pyrkii kuitenkin tukemaan potilaan näkökulmaa terveydenhuollon tietorikkomuksen uhrina tutkimalla potilaan selviytymisprosessia.

Tutkielman tarkoituksena on tutkia potilaan selviytymistä terveydenhuollon tietomurroista. Ymmärtämällä paremmin, miten terveydenhuollon tietomurtojen uhrit reagoivat ja selviytyvät kyseisistä tapahtumista, on mahdollista suunnitella yleisiä käytäntöjä, joilla säännellään toimintaa tietomurtojen jälkeen ottamaan potilas uhrina paremmin huomioon.

Tämä tutkimus koostuu kirjallisuuskatsauksesta sekä empiirisestä tutkimuksesta. Tutkimuksen empiirinen osuus toteutettiin kvalitatiivisin menetelmin, ja empiirinen data kerättiin temaattisten haastattelujen sekä fiktiivisen vinjetin avulla, edustaen terveydenhuollon tietomurron olosuhteita. Kerätty tieto analysoitiin käyttäen abduktiivista sisällönanalyysiä.

Tutkimustulokset osoittivat, että potilaiden selviytymisprosessi henkilökohtaisen terveydenhuollon tietomurron jälkeen seuraa selviytymisprosessia, joka määritellään selviytymisteoriassa. Potilaan selviytymisprosessi alkaa tietomurtotapahtuman ensisijaisesta arvioinnista, joka aiheuttaa potilaalle erilaisia negatiivisia kokemuksia, minkä jälkeen seuraa tapahtuman toissijainen arviointi sekä potilaan näkemys tilanteen hallittavuudesta, mitkä vaikuttavat valittuun selviytymisstrategiaan ja selviytymistoimintoihin, joita potilas käyttää kokemansa ahdingon lievittämiseen.

Asiasanat: *tietomurto, kyberrikollisuus, selviytymisteoria, selviytymisstrategiat, terveydenhuolto*

ABSTRACT

Etelä, Noora
Coping with personal data breaches in healthcare
Jyväskylä: University of Jyväskylä, 2021, 69 p.
Cyber Security, Master's Thesis
Supervisors: Soliman, Wael; Siponen, Mikko

Today's information age considers data as a valuable resource. Alas, this means that illegal data-related activity is also rampant and data breach events are unfortunately common. Medical information is considered the most lucrative by cyber criminals, and therefore data breach events disproportionately damage the healthcare industry. However, when investigating the effects of data breach incidents, extant cyber security and data breach research often prioritizes the organizational point of view over the individual victim's perspective. By examining the patient's coping process, this thesis intends to support the patient's perspective as a victim of a healthcare data breach.

The purpose of this thesis is to study patient coping with a healthcare data breach involving confidential medical information. By better understanding how victims of healthcare breaches react and cope with the negative event, it will be possible to design a general code of conduct and improve policy regulating conduct following a breach that takes the patient as a victim better into account.

This thesis consists of a literature review on data breaches and coping theory as well as an empirical investigation on how patients cope with a healthcare data breach. The studies empirical component was carried out utilizing a qualitative approach, with primary data collected via virtual thematic interviews supplemented with a fictitious vignette to provide research participants with space. The collected data was examined using abductive content analysis.

The study found that patients coping with a personal health care data breach follows the coping process defined by coping theory, beginning with the primary appraisal of the stressor event resulting in various negative outcomes, followed by and the secondary appraisal of the event and the patient perception of control ability, that influence the chosen coping strategy and coping activities employed to alleviate they're distressed experienced by the patient.

Keywords: *data breach, cybercrime, coping theory, coping strategies, healthcare*

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

A data breach incident is a security violation where sensitive, protected, and/or confidential data is accessed by an unauthorized entity. It is one of the most common types of cyber incidents and as the value of data increases and its generation turns ubiquitous, stealing data presents an ever more attractive opportunity for cybercriminals. The topic of data breaches is one of interest in the cyber security research community, but the body of the extant research is often heavily skewed towards a capitalistic perspective. According to Sen and Borle (2015), the existing research regarding computer security incidents generally focuses on examining what kind of financial impacts does disclosing an incident publicly have on the victim organization. The humane view, which considers the effects of a breach on the victim individuals, is much less perused. This is unfortunate, since both information technology and cyber security contain an inherent social issue in the form of the people who use and design IT.

Research, which approaches data breaches from an organizational point of view, routinely prioritizes profitability and organizational performance over the people who ultimately fall victim to the breach. This presents a moral dilemma. A data breach event has significant consequences to the individuals, whose data has been compromised, as well as the affected organization (Sen & Borle, 2015). Individual people are the indirect victims who may bear significant financial, social, or psychological effects in their personal lives caused by a data breach event. This humane problem of data breaches is recognized in the existing literature, yet it has been overshadowed in representation by the organizational point of view. Ablon, Heaton, Lavery and Romanosky (2016) maintain that little research examining individual consumer sentiments towards data breaches exists, compared to the several studies conducted to examine organizational attitudes, reactions, and costs as a result of data breaches.

Some judiciaries have begun to develop a harsher stance on supporting consumer rights regarding the protection of data, such as in the form of GDPR in the EU. The impact of data breaches on individual people may at times be intangible and vague and overshadowed by the economic impact, but it

nevertheless must be taken seriously, since ignoring the harm inevitably causes ineffective deterrence of cybercrime (Solove & Citron, 2018). It is beneficial to the cyber security community to diversify the research literature on data breaches with perspectives that challenge the business centric foundation of the extant literature, in order to create a more holistic and robust understanding of the effects of a data breach incident.

According to Seh et al. (2020), out of all known data breach events in the United States between years 2005 and 2019, the healthcare industry has had the largest number of data breaches of any sector. As the most susceptible sector with extremely sensitive patient information considered highly compelling by cyber criminals (Chernyshev, Zeadally & Baig, 2019), the victimization of patients in data breach incidents must be taken into account in the data breach discussion. Based on the need for further research from a diverging perspective, in this pro gradu -thesis, with Lazarus and Folkman's (1984) theory of stress and coping and the transactional model of coping as the theoretical framework, I will study how patients subjected to a healthcare data breach cope with the event.

To define the research topic further, this study will focus on patient coping with personal data breach events in a healthcare context that compromise sensitive personal information, also referred to as personal data breaches. Review of the general concept of a data breach and the narrower idea of a personal data breach is necessary, as data breaches reach all different types of information. In the context of this thesis, as stated above, I will focus on personal data breach events that expose sensitive health information of individual people. This type of breach may have serious psychological, social, and financial consequences on the victims (Solove & Citron, 2018), but it should be noted that personal health records are not the only kind of information susceptible to unauthorized disclosure and breach within the healthcare industry. Consider for example unauthorized access to software of automated medical devices which could endanger ongoing treatment due to interference with devices connected to the internet. Thus, the repercussions suffered by individual victims of healthcare data breaches vary, but the intangible distress caused by the exposure of personal health information should not be overlooked in the data breach debate.

The topic of this study was prompted and can be motivated by timeliness of recent events in Finland. In October of 2020, a private Finnish healthcare company Vastaamo disclosed publicly that the company had suffered a personal data breach and that the confidentiality of an undisclosed number of highly sensitive psychotherapy patient records had been compromised (Heikkilä & Hevonoja, 2020). The following public reaction to the breach was very prominent and exhibited collective anger, which prompted the first draft of the research topic that would be refined to the final version.

The research objective of this study is to explore patient coping with an invasive personal data breach event in healthcare. Considering the timeliness of the topic, the Vastaamo data breach provides my thesis a research question:

How do patients cope with personal data breaches that happen in healthcare? The study is guided by the idea that the stress and cognitive effects of a data breach incident on the individual victim must be recognized in order to improve both proactive and reactive conduct in response to data breach events. Only by understanding how the individual victims react to and try to overcome the stressor can the response to data breach incidents evolve to better safeguard trust in society.

The possible effects of a data breach on the healthcare provider organization are not in the scope of the study. The outcome of the patient's coping process, whether coping was successful or not, is not considered either, as the coping process and coping outcome are separate concepts. The goal of this thesis is to investigate patients' coping process in the aftermath of a personal data breach, following Lazarus and Folkman's (1984) theory of coping as a transactional process. Lazarus and Folkman (1984, p. 142) define coping as a process, attempting to manage stressful demands in dynamic situational conditions throughout a period of time. The interaction between the person and the environment is transactional, with both parties influencing each other dynamically (Lazarus & Folkman, 1984, p. 142). The patient coping process and coping activities are explored from via the two most examined coping strategies considered in extant research literature on coping, problem-focused and emotion-focused coping (Lazarus & Folkman, 1984), as most coping activities can be divided between methods aimed at confronting the problem and methods oriented toward avoiding dealing directly with the problem (Roth & Cohen, 1986).

When studying data breaches, much of the empirical research literature surrounding the topic follows a quantitative methodology. Carre, Curtis and Jones (2018) conducted a quantitative questionnaire to study consumer reactions to security breaches to minimize reputational damage and thus protect firm value. Janakiraman, Lim and Rishika (2018) conducted a statistical study to study the impact of data breach announcements on customer behavior to develop ways for managers to engage with customers post breach to protect firm value. Chang, Gao and Lee (2020) studied the effects of a data breach event on organization's value through a quantitative event study. However, as the goal of this study is to explore subjective patient coping, qualitative research's inherent subjectivity may provide holistic insights of the patients' experience (Hirsjärvi & Hurme, 2008, p. 22).

The study was conducted as a qualitative semi-structured interview study. Each interview was complemented with a fictional vignette to simulate a realistic scenario to learn more about the interview participants' thoughts and beliefs in specific circumstances (Gourlay et al., 2014). The discretionary sample, consisting of seven interview participants aged 25 to 35, was not limited to only victims of major personal data breaches. All research participants had been exposed to data breach news and public communications in the year leading up to their interview date. The vignette presented the participants with a news article and an email about a healthcare data breach event, modeled after public

communications following the Vastaamo data breach, informing the research participant that the confidentiality of their health information had been compromised. Interviews were conducted thematically, with three natural themes arising from Lazarus and Folkman's (1984) coping theory: primary appraisal, secondary appraisal, and coping strategy and activities. After data collection, abductive content analysis was used to analyze the interview data.

The findings suggest that patient's coping process in response to a healthcare data breach follows Lazarus and Folkman's (1984) theory, progressing from a primary appraisal resulting in experiences of injustice, negative emotions, and a changing view of the healthcare provider, to a secondary appraisal, which is influenced by the patient's perception of control. The secondary appraisal influences the patient's choice of coping strategy and coping activities. A positive perception of control, interview participants reported employment of problem-focused coping in the form of gathering information and managing financial risk, while a negative sense of control was followed by emotion-focused coping, which included distancing, acceptance, social support, and transferring responsibility. The findings suggest that patient coping in response to a healthcare data breach is dynamic and can change depending on the rationale and reappraisal of the incident. Some participants wished to disengage to wait for the scenario to develop for to allow problem-focused coping later. Instead of actively seeking information, passive waiting implies a coping attempt that involves emotion-focused activities in the hopes of subsequent problem-solving actions.

This study contributes to data breach discourse in cyber security research by considering and emphasizing the experience of the individual victim. The results of this study can benefit business in practice by providing valuable insights to communication with victims and business continuity planning. The findings can also be used as justification for changes in data breach policies and the protection and aid of data breach victims.

The research is organized as follows: chapter two introduces the concept of data breaches, relevant law, and data breaches in healthcare, followed by a literary review of coping theory, its origins and development in chapter three. Chapter four describes the used research methods, followed by research results and their analysis in chapter five. Chapter six includes discussion of the findings, practical contributions, and limitations of the study, followed by conclusion in chapter seven.

2 DATA BREACH

Data breaches are a complex concept, reaching into the domains of criminology, cyber security, economics, psychology, and sociology. Thus, in order to get a generalized view of the topic, this chapter begins with an overview of context, key terms and concepts, followed by summary of existing literature and looking into why and how data breaches happen, and at what cost. Legislation in the European Union that provides regulation regarding data privacy and data breaches is also considered, as well as allocation of responsibility over a data breach incident. Existing literature on healthcare data breaches is analyzed, and the chapter is concluded with table 1 summarizing all reviewed research literature on the subject.

As society has developed towards increasing data dependency and the possibilities of exploiting data for financial gain have evolved with new emerging technologies, it is expectable that the value of information assets increases in a linear manner. Comparison between 10 of the world's largest companies by market capitalization in 2010 (Financial Times, 2010) and 2020 reveals that organizations capitalizing on high volumes of data, such as Microsoft, Apple, Amazon, Alphabet, Facebook, and Alibaba (Statista Research Department, 2020) have benefitted from the information revolution in ways that surpass any expectation. The ability to decipher meaningful information from data creates value and thus provides a competitive angle in business. This visible shift in market valuation demonstrates how valuable data is as a new type of raw material and as an enabler of profit. However, the value of data is neither overlooked by actors operating outside of the rule of law. Stealing, aggregating, and monetizing stolen data is a profitable avenue of criminal activity.

A general definition of a data breach is described as the unauthorized disclosure or use of information (Seh, Zarour, Alenezi, Sarkar, Agrawal, Kumar & Khan, 2020). Sen and Borle (2015) define data breaches more categorically as follows:

> A data breach incident involves unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of

> confidentiality, integrity and availability of the affected data. Sensitive, protected, or confidential data may include personal health information, personal identifiable information, trade secrets or intellectual property, and/or personal financial data. (Sen & Borle, 2015, p. 315)

According to the definition above, a data breach may compromise many types of confidential data. However, according to the Office of the Data Protection Ombudsman in Finland, a personal data breach is a narrower definition referring only to "events leading to the destruction, loss, alteration or unauthorized disclosure of, or access to, personal data" (Tietosuojavaltuutetun toimisto, n. a.), meaning that the concept of a personal data breach is a subcategory below the general definition of data breaches.

The apparent criminal market values data quality over quantity. Regardless of attempts of prevention, laws and regulations, the occurrence of data breach incidents is unfortunately common in a global setting. Annual reports of data breach incidents describe a volatile reality regarding frequency and scale. Edwards, Hofmeyr and Forrest (2016) analyzed a Privacy Rights Clearinghouse (PRC) data set on data breaches and discovered that between 2005 and 2015 there was no statistically significant increase in frequency or scale of data breaches in the USA. However, Bisogni and Asghari (2020) depict a clear growing trend in data breach incidents in the USA from 2005 to 2017. In Europe, longitudinal data on data breaches is scarce, with a plotting of data breach events in Ireland between 2009 and 2019 being one of the only public statistics regarding data breach events in an EU member state before and after the application of the General Data Protection Regulation (GDPR). The application of the GDPR was followed by an increase of over 100% in reported data breach incidents in Ireland. It is evident that the growing numbers of data breaches are not necessarily only attributable to more frequent incidents but could also be explained due to simple increased reporting. (Bisogni & Asghari, 2020)

Edwards et al. (2016) point out in their study that it is no consolation if data breaches appear stable in scale and occurrence: along with the progression of technological advancement, the knowledge on monetizing personal information grows. This, combined with the availability of discrete methods of transferring money online may cause an increase in the financial consequences and effects of data breaches in the future (Edwards et al., 2016). The improvement in monetization of personal information acts as an additional incentive for criminals to commit data breaches (Bisogni & Asghari, 2020).

Incidents where confidential data is breached by an unauthorized actor happen due to various reasons. According to Seh et al. (2020), data breach incidents are often categorized based on whether they are caused by external or internal factors. Incidents that occur with the assistance of an internal agent are classified as internal data breaches. Examples of internal causes of a data breach are privilege abuse, improper data disposal, or loss and theft. Contrastingly, data breaches caused by an external agent or source are referred to as external

data breaches, such as hacking incidents including malware and ransomware attacks, phishing, and fraud in the form of stolen credit cards. (Seh et al., 2020)

The most prominent narrative in media is to attribute breaches to malicious hacking attacks and while such attacks are undoubtedly a serious cause of data breach incidents, they do not account for all (Trendmicro, 2015). Other prominent causes of data breaches include insider attacks, theft or loss, and unintended disclosures (Trendmicro, 2015). In an observational study in a Malaysian financial service company, Abidin, Nawawi and Salin (2019) discovered that employees often do not take sufficient precautions to protect customer data despite mandates assigned in organizational privacy policies. Abidin et al. argue that this irresponsible behavior may be attributed to ignorance of the responsibility to protect confidential customer data (Abidin et al., 2019).

Much of the existing literature on data breaches study the association between data breach incidents and financial firm outcomes. Makridis and Dean (2018) documented a negative association, where a 10% increase in breached records was associated with a 0,2% decline in firm outcome, a 1,1% outcome decline in case of the breached records being health and human services data. Gwebu, Wang and Wang (2018) confirmed previous findings that the stock market reacts to public disclosure of data breaches in a statistically significant negative manner, and Chang et al. (2020) examined the effects of a breach incident on an organization's short and long-term value, discovering negative influence on both, with the breach scale affecting the negative return on the company market value positively.

Solove and Citron (2018) approach data breaches from a legal standpoint, criticizing the judicial system of the USA for being too rigid and failing to validate the harm experienced by the individual victims of personal data breaches. This study explores perceptions towards data breaches in Finland, a European Union member state liable under the GDPR, but for the sake of thorough perusal of existing literature, the legal environment of the USA is also briefly considered. According to Solove and Citron (2018) the risk for stolen data being abused long after the incident itself can never be fully absolved and such abuse may cause great harm. Thus, the causal connection between a data breach and obvious harm experienced by the breach victims is not always easy to prove (Bisogni & Asghari, 2020).

Solove and Citron (2018) emphasize, that law should not overlook the victims' experienced feelings of anxiety generated by the heightened risk of harm as notable harm to the individual victims. The breach victims experience anxiety post breach as a result from the awareness that their personal information is outside of their control and can be misused at the victim's cost. In cases of breaches involving reputation-damaging information, such as the Ashley Madison breach of 2015, victims evidently experience heightened emotional distress. (Solove & Citron, 2018)

Additionally, in cases of breaches involving potentially embarrassing or reputation-damaging data, victims may find it difficult to legitimately claim

appropriate recognition of their experienced harm and trauma as a result of the crime committed against them (Cross, Parker & Sansom, 2019). An unfortunate but notable example of such victim blaming and gate keeping mentality is, again, the Ashley Madison breach of 2015. Cross et al. (2019) note that the shame experienced by victims of the Ashley Madison breach directly influenced the feelings of isolation and humiliation experienced by the victims, thus indirectly failing to prevent further crime, such as extortion and blackmail, derived from the breach.

Still, a data breach concerning seemingly not embarrassing or less harmful personal data should not be seen as less important, as accumulation of data to larger sets that reveal sensitive information is no longer a difficult task (Solove & Citron, 2018). Thus, the ease at which stolen information can be monetized, poses acute problems especially to individual citizens (Edwards et al., 2016; Bisogni & Asghari, 2020). Dion and Smith (2019) remind us of the victim's difficulty of proving quantifiable and speculative damages. Even if stolen data is not misused to result in financial loss to the individual victim, knowing that one's personal information is completely outside of the victim's control may cause psychological distress and anxiety for the victim for years to come in anticipation of potential misuse in the future (Ferrick, 2018), as there is generally nothing to be done to secure the stolen information. The electronic aspect of a data breach unfortunately ensures that once the information is compromised, it is permanently available for illegal activity, making it possible for victims to suffer ongoing and lasting psychological damage. (Dion & Smith, 2019).

Martin, Borah and Palmatier (2017) studied the fundamental customer perceptions of companies simply having access to their personal data and their perceptions of potential harm from such access, finding that after a breach incident, customers experience amplified feelings of violation and diminishing trust towards the organization. Martin et al. (2017) suggest that clients feeling vulnerable creates negative consequences in companies regardless of whether a breach instance is perceived to be malicious or not: even a benign data access vulnerability is still seen as concerning and damaging to the reputation of the company. The findings of Bansal and Zadehi (2015) counter this sentiment, proposing that the customers' experienced violation of trust post breach is moderated by attributes of the breach incident. Following attribution theory and organizational justice theory, Bansal and Zadehi reason that a case, where a breach incident can be categorized as organization's unauthorized sharing of customers' private information to generate profit, is different from a breach resulting from malicious hacking due to the former being an internal, stable, and controllable event whereas the latter may be considered an unpredictable and external event. The authors argue that this distinction separates the two violation types regarding the trust violation experienced by customers. (Bansal and Zadehi, 2015)

2.1 Legal views and GDPR

As mentioned above, this study is conducted in Finland under the EU's GDPR 2016/679, applied on May 25th, 2018, which inevitably influences the definitions and legal views of this thesis. However, as the topic of data breaches is ubiquitous and not containable to certain geographic locations, different legal environment presented in the review literature is also summarized.

As a regulation, the GDPR applies to every entity within the scope of EU law and overruns national legislation of each member state, its purpose being standardizing regulation across the Union. Additionally, the GDPR includes an enforcement mechanism for regulation violations, which allows regulators to impose considerable fines to victim organizations (Bisogni & Asghari, 2020). The regulatory enforcement of financial consequences for neglecting adequate data protection works as an encouragement for organizations in the scope of EU law to elevate their data protection practices.

Bisogni and Asghari (2020) found that firms operating in Europe generally don't fear reputational damage from obliging to notify supervisory authorities, as the regulation does not necessitate such notifications to be made public. The GDPR Article 59 regulates that annual reports from each supervisory authority may include a list of notified infringements, but the article does not compel this, thus rendering the publication of such lists optional. Dion and Smith (2019) present arguments for ensuring individuals have the right to take legal action against the data keeper in case of breach. This is to ensure adequate data protection from the data holder, which in turn encourages growth of online commerce (Dion & Smith, 2019). However, the GDPR does not necessitate public disclosure of all personal data breach events but the decision of disclosing such a breach event publicly or even to the individual victims is up to interpretation based on the presumable risk posed to the data subjects (Tietosuojavaltuutetun toimisto, n. a.). Bisogni and Asghari (2020) note that due to there not necessarily being reputational ramifications due to public disclosure, organizations are incentivized to notifying authorities as cautionary action. This may explain some of the growth in data breach statistics in the EU.

2.2 Allocation of responsibility

Views regarding who is responsible and accountable for a data breach incident are as many as there are actors in the complicated matrix of security breaches. It is challenging to decide to whom to ascribe responsibility for certain actions and whom to assign accountability over consequences (Kayes et al., 2020). While hackers who illegally access confidential data bear responsibility for their actions, how much responsibility should be allocated on businesses for protecting their customers' data is not as simple (Bentley, Oostman & Shah, 2018). The findings of Carre, Curtis and Jones (2018a) support the widely

accepted notion that consumers do not feel responsible for their online security activities when using electronic services, even if they were to exhibit poor security behavior such as using an unsafe password. This consumer perception seems illogical and irrational, as such security behavior exhibited by a consumer may contribute to the firm's vulnerability to data breaches, yet consumers attribute the responsibility of data protection entirely to the organization. However, even as a breach event lowers consumer trust, consumer security behavior is not affected. (Carre et al., 2018a)

The same sentiment is echoed in the results of Carre, Curtis and Jones's (2018b) questionnaire, indicating that consumers view firms as more responsible for data protection as well as more responsible for the data breach compared to consumers. The conclusion supports the theory that customers experience decreased trust post data breach due to a breach of their psychological contract. (Carre et al., 2018b)

The concept of a psychological contract was pioneered by Professor Denise Rousseau to refer to the beliefs of an individual regarding a mutual agreement between the individual and another party (Rousseau, 1989). In the domain of data breaches, consumers may consider a data breach incident to be a breach of the psychological contract between the individual victim and victim organization. Rousseau (1989) specifies that the psychological contract stands upon the individual's belief that a commitment between the parties was made, binding said parties to some obligations. The violation of the psychological contract only explains the decrease in the individual's trust in the organization post data breach to the extent to which the individual ascribes responsibility for the protection of their data to the organization in the psychological contract (Carre et al., 2018b).

Janakiraman et al. (2018) have studied the impact of data breach announcements on customer behavior based on the type of breach, following Coombs and Holladay's crisis categorization. Coombs and Holladay (2002) divide different crisis types into three distinct clusters: the victim crises, where damage to the organization and its stakeholders is inflicted by an external entity; the accidental crises, where the crisis is caused by unintended accidental actions of the organization associated with the operations; and the preventable crises, where the organization intentionally puts its stakeholders at risk. Janakiraman et al. (2018) expand on the categorization by describing them in terms of the attribution theory: a victim crisis has a weak attribution to responsibility, accidental crisis has a minimal attribution to responsibility and an intentional crisis, which involves no preventative action to prevent accidents and human errors as well as violation of laws and is defined by the highest attribution of responsibility (Janakiraman et al., 2018).

2.3 Data breach incidents in healthcare

As noted by Seh et al. (2020), internet connectivity, smart medical devices, cloud computing, and other web-based technologies have enabled the healthcare sector to transition from paper-based systems to electronic health record systems (EHR), transforming healthcare data to a digital form. However, Chernyshev et al. (2019) point out that health data is regarded as the most compelling type of data for cyber criminals. Regardless of the advantages presented by these electronic systems, such as immediate availability of patient data, enhancement of patient care and cost-effectiveness, such systems also open up the attack surface of health services to potential security breaches (Seh et al., 2020).

A data breach in healthcare context is often broadly described as "illegitimate access or disclosure of the protected health information that compromises the privacy and security of it." (Seh et al., 2020). A broad definition of health information, sometimes used interchangeably with terms "health records" and "medical records", is considered to be relevant to any and all aspects of personal health, related to encounters with healthcare professionals, in physical or digital form, handled and stored by various organizations and often linked to personally identifiable information (PII) (Chernyshev et al., 2019).

Kamoun and Nicho (2014) note that a personal health record (PHR) may reveal plenty of sensitive information including PII such as names and social security numbers, employment details, financial information as well as information regarding diagnoses, medications, and treatments. This information is considered extremely critical since its manipulation may cause inaccurate treatment, which in the worst-case scenario may result in permanent injuries or have fatal consequences for patients (Seh et al., 2020) and its unauthorized disclosure may impact the patient's wellbeing by causing financial, psychological, and social distress.

Seh et al. (2020) have analyzed a Privacy Rights Clearinghouse's data breach data set detailing all reported data breaches in the USA during a 15-year period from January 2005 to October 2019. Analysis of the data set reveals that the healthcare sector has faced the most data breach incidents out of all, 61.55% of all recorded data breaches in total. In the last four years of the examined data set (2015–2019), 76.59% of all incidents were recorded in the healthcare industry in the USA. According to the data, the healthcare sector has been specifically and persistently attacked, eclipsing any other sector as the subject of data breaches. Hacking attacks, unauthorized internal access, theft or loss, and inappropriate data disposal were the most common forms of disclosure of protected healthcare information discovered in the data set, accounting for almost 97% of all recorded breach incidents. (Seh et al., 2020)

Seh et al.'s (2020) review of the entire PCR data collection revealed that during the full timeframe of the data set, healthcare documents were exposed by both internal and external threats, including hacking, theft/loss,

unauthenticated internal disclosure, and improper disposal of confidential data. The analysis of Seh et al. (2020) found an increase of hacking incidents in the data set, where 81.85% of all recorded hacking incidents happened during the last four years, 32.23% in the 2019 alone. In opposition, theft/loss and improper disposal of data show a clear decrease from 2015 to 2019. (Seh et al., 2020) A possible explanation for these distinct changes may be that criminal actors have found hacking to be either the most or one of the most lucrative ways to commit data theft in terms of cost-to-benefit ratio. Similarly, analyzing published data breach records in healthcare, Chernyshev et al. (2019) found ransomware to be the most commonly used malware type used in hacking scenarios.

Neame (2012) brings ethical significance to the conversation by pointing out that personal autonomy as an ethical concept declares that people have the right to manage and control everything regarding their own bodies, including their personal health records. Kamoun and Nicho (2014) build on this, arguing that personal autonomy transforms into a public expectation that healthcare providers must keep patient information and health records safe and confidential. Ablon et al. (2016) conclude that, unsurprisingly, data breaches in all sectors have weakened the United States' public's confidence in these organizations' ability to protect their personal data. Pivoting this argument to seek similar sentiments in a European context would be an interesting additional research topic. Concluding this chapter, Table 1 presents an overview of the reviewed literature on data breaches.

TABLE 1 Summary of reviewed articles on data breaches

Author(s)	**Context**
Makridis, C. A. & Dean, B. (2018).	Effects of data breaches on public and private organizations
Chatterjee, S., Gao, X., Sarkar, S. & Uzmanoglu, C. (2019).	Consumer reactions to data breaches
Carre, J. R., Curtis, S. R. & Jones, D. N. (2018a).	Effect of security statements on online consumer perceptions
Gwebu, K. L., Wang, J. & Wang, L. (2018).	Organizational response to a data breach
Chen, H. S. & Jai, T-M. (2019).	Customer perceptions of data breaches in the service industry
Carre, J. R., Curtis, S. R. & Jones, D. N. (2018b).	Consumer reactions to security breaches and minimizing reputational damage
Janakiraman, R., Lim, J. H. & Rishika, R. (2018).	Impact of data breach announcements on customer behavior
Chang, K.-C., Gao, Y.-K. & Lee, S.-C. (2020).	Effect of a data breach on an organization's value
Solove, D. J. & Citron, D. K. (2018).	Legal positions on the potential harm from a data breach to consumers
Abidin, M. A. Z., Nawawi, A. & Salin, A. S. A. P. (2019).	Customer data theft inside of an organization
Sen, R. & Borle, S. (2015).	The risk of data breach of a firm in the context of its primary industry, geographical location and

	previous breaches
Dion, J. H. & Smith, N. M. (2019).	Privacy, data breaches and identity theft from a legal standpoint
Cross, C., Parker, M. & Sansom, D. (2019).	Victim blaming discourse and challenging the 'ideal victim' in the Ashley Madison data breach
Martin, K.D., Borah, A., & Palmatier, R.W. (2017).	The influence of customer perceptions of vulnerability to harm due to firm data practices
Bentley, J. M., Oostman, K. R. & Shah, S. F. A. (2018).	Organizational crisis management responses to data breach events
Bisogni, F. & Asghari, H. (2020).	Relationship between data breaches, identity theft and data breach notification laws
Kayes, A., Hammoudeh, M., Badsha, S., Watters, P. A., Ng, A., Mohammed, F. & Islam, M. (2020).	Responsibility attribution post breach
Edwards, B., Hofmeyr, S. & Forrest, S. (2016).	Data breaches in ten years, 2006-2016
Coombs, W. T., & Holladay, S. J. (2002).	13 crisis types in three distinct categories
Ablon, L., Heaton, P., Lavery, D., & Romanosky, S. (2016).	Consumer reactions to data breaches
Chernyshev, M., Zeadally, S. & Baig, Z. (2019).	Data breaches and digital forensics in healthcare
Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020).	Data breaches in healthcare
Kamoun, F., & Nicho, M. (2014).	Possible causes contributing to healthcare data breaches
Neame, R. (2012).	Prevention of health information abuse

3 COPING WITH AVERSIVE EVENTS

This chapter inspects scientific literature and theory on how people react to stressful and aversive external demands. We begin with an introducing coping and emotions as closely related concepts, after which we take a look at coping theory which makes up the theoretical framing of the thesis. This is followed by a look into the general dichotomy of coping strategies, problem-focused and emotion-focused coping, after which the chapter is concluded with some negative emotions associated with data breach events and how they affect the coping process.

In a negative and aversive event where a person holds little control over circumstances, such as a personal data breach, the person's cognitive expectations and wants are at discord with the environment, prompting coping responses from the individual. Lazarus and Folkman (1984) define coping as cognitive and behavioral efforts that are meant to resolve a discrepancy between the situation and the individual's desires. Successful coping relieves stress experienced by the individual and it is determined by a cognitive appraisal of the circumstances (Lazarus & Folkman, 1984).

Previous research has established that emotions are a mediating mechanism decoupling stimulus and response (Scherer, 1982). Emotions are closely related to the cognitive appraisals of circumstances: a person appraises an event cognitively which cues an emotion (Smith & Ellsworth, 1985). They are experienced in response to particular objects of consciousness or thought (Rustin, 2009, p. 21), such as an experienced stressful event and the interpretation of it (Smith & Ellsworth, 1985). According to Brosch, Scherer, Grandjean and Sander (2013), psychological and neuroscientific research argues that emotion and cognition influence each other bidirectionally, as cognitive processing elicits emotional reactions in response to stimulus and emotional responses modulate cognition by creating latency time between the stimulus and response to allow humans to adapt their response to the environmental stimulus.

In their analysis of literature on emotions, stress and coping, Yih, Kirby, Spitzer and Smith (2020) synthesize that the majority of empirical research

argues that the process of adapting to situations flows from appraisal to coping to emotions, ignoring the direct role of appraisal in emotion generation supported by the appraisal theory. However, Lazarus (1991a, p. 113) argues that while coping does result from emotion and is mostly used for mitigation of emotional distress, coping is also preceded by situational appraisal and may alter subsequent reappraisals, therefore influencing future emotions. Emotions and coping mediate each other, and as according to Folkman and Lazarus (1988), coping may be prompted by emotions, yet it also influences following emotions, facilitating a cyclical link between the concepts. The adaptational coping process can therefore be considered as an iterative sequence of cognitive processes that influence each other (Yih et a., 2020).

3.1 The transactional model of stress and coping

Research on coping is vast, with numerous historical approaches to how humans cope with stressful situations. A consensus within many approaches to coping theory is that coping requires psychological stress to act as a catalyst for subsequent coping activities (Folkman, Lazarus, Gruen & DeLongis, 1986). Perlin and Schooler (1978) define coping as the actions people take in order to escape from being harmed by strenuous events and this definition rests on a fundamental assumption that humans take active and conscious actions in response to external stressful forces that affect them. Perlin and Schooler's (1978) definition of active responsiveness to external powers illustrate this definition as one derived from psychoanalytic ego psychology, which is one of two traditional theoretical approaches to coping (Lazarus & Folkman, 1984, p. 118). According to Lazarus and Folkman (1984, p. 118), the other traditional approach, the animal experimentation model of coping, is widely regarded as superficial and devoid of the cognitive emotional richness and nuance that is a necessary element to human functioning. The emphasis on ways of perception and reasoning of a person's interaction with their environment is the key distinction between coping in the psychoanalytic ego psychology and coping in the animal paradigm, as the animal experimentation model bypasses cognition while focusing mainly on behavior (Lazarus & Folkman, 1984, p. 118).

Lazarus and Folkman have argued that neither of the traditional approaches to coping decouple coping from an automatic human response as effortful (Lazarus & Folkman, 1984, p. 130). The deployment of any coping activity is not an automatic response to an aversive situation, but rather depends on the person's assessment of the event (Mikulincer, 1994, p. 241-242). On top of this, the traditional approaches do not differentiate coping from successful adaptation to circumstance, which according to Lazarus and Folkman (1984, p. 133) blends the two distinct concepts of coping activities and coping outcome together. Lazarus and Folkman (1984, p. 133) argue that coping activities should be considered separate from their outcome, and this argument is supported by Thoits's (1995) literary review findings, which state that the

relationship between personality traits, coping strategy preference, and coping outcome effectiveness is highly complex and inconsistent.

There is a consensus within modern coping research that Lazarus and Folkman's (1984, p. 142) definition of coping as a process of attempting to manage stressful demands in dynamic situational circumstances over a period of time is a salient approach to coping theory. In order to study coping, the particular environmental and situational conditions must be understood, since coping thoughts and behaviors are not static, but are targeted to a specific context (Lazarus & Folkman, 1984, p. 142). The process approach to coping is transactional, supporting the understanding that the individual and their environment are seen as being in an ongoing mutual relationship, with each dynamically influencing and being influenced by the other, shifting and changing the person-environment relationship as a result of continuous appraisal and reappraisal of the circumstances (Lazarus & Folkman, 1984, p. 142; Folkman & Lazarus, 1980). Thus, as the stressful situation progresses, an individual may dynamically transition between any coping activities, be it problem-solving attempts aimed at changing the aversive conditions or emotion-focused coping directed inward seeking to change the person's sense of the event to manage emotional distress (Lazarus & Folkman, 1984, p. 142-143). The changed person-environment relationship induces re-evaluation and re-appraisal of the relationship, feeding into the bidirectional dynamic of the coping process between the individual and the environment. (Folkman & Lazarus, 1980; Lazarus & Folkman, 1984, p. 142-143)

Folkman, Lazarus, Dunkel-Schetter, DeLongis and Gruen (1986) draw distinctions between the coping process approach and another school of thought regarding coping, the trait-oriented approach, which regards coping styles as personality traits, with differences in the aversive situation having little effect to coping activities. The transactional process-oriented approach opposes this consideration, construing great importance to the context as coping is seen as a solution to the psychological and environmental demands of context specific stressful events over static features of personality (Folkman et al., 1986). No single coping mechanism or strategy is universally applicable regardless of situation, and the outcome of coping activities is highly dependent on situational elements (Thoits, 1995).

Cognitive appraisals and coping activities are the two central components of the coping process (Folkman & Lazarus, 1980; Nach & Lejeune, 2010; Folkman, Lazarus, Gruen & DeLongis, 1986). Cognitive appraisal, according to Folkman, Lazarus, Gruen and DeLongis (1986), is the mechanism by which an individual assesses whether a particular situation is influential to their well-being. The cognitive appraisal an unconscious cognitive process (Lazarus, 1991b), divided into two parts: primary and secondary appraisal. The cognitive process of assessing the stressful situation in terms of risk of harm or benefit is referred to as primary appraisal (Folkman & Lazarus, 1980; Folkman, Lazarus, Gruen & DeLongis, 1986). The primary appraisal produces an emotional reaction (Folkman and Lazarus, 1988) and its definition is influenced by

personality traits such as values and beliefs (Folkman, Lazarus, Gruen & DeLongis, 1986). The primary appraisal and its accompanying emotions influence the secondary appraisal (Folkman & Lazarus, 1988), which identifies what can be done to manage the potential harm or benefit and what is needed in order to cope with the situation (Folkman & Lazarus, 1980). The secondary appraisal is followed by various coping actions, cognitive and behavioral efforts to manage external and internal demands meant to restore the strained person-environment relationship (Folkman & Lazarus, 1980; Nach & Lejeune, 2010). The adjusted person environment relationship is examined once again as primary appraisal, creating a feedback loop for the coping process to begin again (Folkman & Lazarus, 1988). Figure 1 depicts a simplified design of the flow of the coping process.

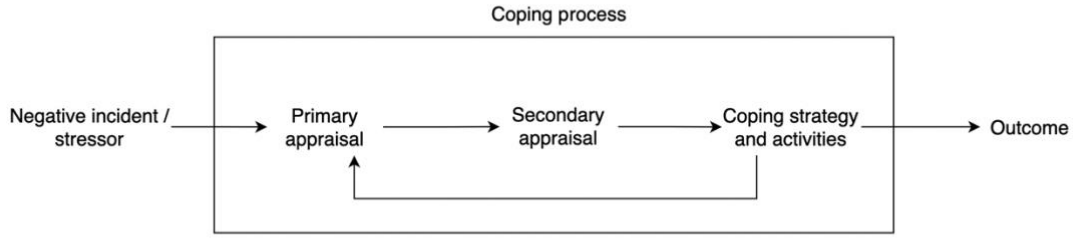

FIGURE 1 A high level summary of the coping process and its relations, modified from Salo, Makkonen & Hekkala, 2020.

Coping is commonly thought to serve two main functions: constructive management of the problem causing distress and emotional regulation (Folkman, Lazarus, Gruen & DeLongis, 1986). These functions support the common dichotomy of coping strategies between problem-focused coping and emotion-focused coping due to their differing goals (Carver & Scheier, 1994). Problem-focused coping is defined by the attempt to manage or adjust the stressful circumstances (Folkman & Lazarus, 1980). Emotion-focused coping, as described by Smith and Lazarus (1990, p. 628), consists of handling distressing feelings that occur in an event when the situation's conditions are not adjustable with a problem-solving coping approach. Even though these two coping strategies are theoretically easily distinguishable, in reality they often overlap (Carver & Scheier, 1994).

3.1.1 Emotion-focused coping

It is now generally established that emotion-focused ways of coping include cognitive processes such as avoidance, minimization, distancing, escapism, selective attention, seeking social support, positive comparisons and finding positive meaning from stressful events, all of which have a common goal of lessening emotional distress (Lazarus & Folkman, 1984, p. 150; Folkman, Lazarus, Gruen & DeLongis, 1986). According to previous research, this type of coping is likely to occur when the individual determines that little can be done to manage stressful external conditions (Lazarus & Folkman, 1984, p. 150).

Some of the forms of coping listed above are reappraisal methods, which have the potential of modifying how the stressful experience is perceived without objectively altering the situation (Lazarus & Folkman, 1984, p. 150). However, Lazarus and Folkman (1984, p. 150-151) note that such coping processes that have the potential of altering the meaning of a stressful transaction also run the risk of falling into the domain of self-deception and distortion of reality.

3.1.2 Problem-focused coping

The concept of problem solving implies an analytical approach to an external problem, but according to Lazarus and Folkman (1984, p. 152-153), problem-focused coping also involves strategies oriented inward, such as making motivational and cognitive improvements including refocusing aspiration levels or reducing the presence of ego. These internal coping activities can be considered reappraisal strategies within the realm of problem-focused coping (Lazarus & Folkman, 1984, p. 152-153). Aggressive interpersonal attempts to change the situation, as well as rational and planned efforts to solve the external problem are ways of problem-focused coping directed to the environmental factors causing stress (Folkman, Lazarus, Gruen & DeLongis, 1986).

Both problem- and emotion-focused coping can, in theory, help and hinder each other in the coping process (Lazarus & Folkman, 1984, p. 153). Folkman et al. (1986) present an example of the two distinct coping strategies being deployed together, when a person determines that the best way to relieve anxiety is to tackle the task that is causing the anxiety, thus using problem-based coping to control emotion (Folkman et al., 1986)

3.2 Emotional reactions to data breach events

As previously stated, the secondary appraisal that determines coping strategy and activities in response to a stressor is influenced by the primary appraisal and its accompanying emotions (Folkman & Lazarus, 1988). The coping activities following the secondary appraisal alter the person-environment

relationship, which is then reappraised and accompanied by new experienced emotions (Folkman & Lazarus, 1988). This implies that emotions and coping exist in a bidirectional relationship (Folkman & Lazarus, 1988), with emotions acting as a decoupler between stressor and reaction (Scherer, 1982) and the coping process mediating subsequent emotions (Folkman & Lazarus, 1988). Thus, in the context of this thesis, negative emotions are experienced after a person learns of a personal healthcare data breach and appraises the situation to have influence over their life. A motive consistent primary appraisal supports and verifies the individual's current beliefs, evoking positive emotions, whereas motive inconsistent primary appraisals destabilize current beliefs, thus eliciting negative emotions (Roseman et al., 1996). A primary appraisal that determines a situation to be harmful to the individual generates negative emotions which mediate subsequent coping activity, thus supporting the notion that cognitive appraisal, emotions and coping all relate to each other (Yih et al., 2020).

Chatterjee, Gao, Sarkar and Uzmanoglu (2019) reported that a data breach announcement may elicit a variety of emotional reactions in the breach victims, including surprise, frustration, anxiety, anger and fear. Negative emotions such as dislike, anger and contempt are evoked by other people (Roseman et al., 1996) and assuming that patients believe that a healthcare data breach event was caused due to actions of others, it is reasonable to expect the emotional reactions to be negative and driven by external agency.

Negative events and wrongful conduct reduce trust (Bansal & Zadehi, 2015) and it can be assumed that in the event of a healthcare data breach, the patient is likely to believe that their trust toward the organization has been violated. However, the subjective and complex nature of emotional responses means that different people view the seriousness of privacy violations very differently (Bansal & Zadehi, 2015). Bansal and Zadehi (2015) suggest that there is a negative association between the perceived seriousness of violation and the violated trust, moderated by the type of privacy violation in question. Bansal and Zadehi (2015) suggest that the individual determines subjectively whether the violation was caused internally or externally, whether it was preventable and whether the event is likely to reoccur. The individual's judgement on these attributes defines the violation type which moderates the negative association between the perceived scale of the data breach event and individual's violated trust (Bansal & Zadehi, 2015). However, one limitation with the perception of potential risk of reoccurrence is that it's inherently subjective and prone to bias. According to Fischhoff, Gonzalez, Lerner and Small (2005), it is true that events are more likely to occur in the future when they have been regularly encountered or witnessed in the past. Yet, this idea of incident availability can be deceitful if such incidents are given overwhelming visibility for example in news media, constituting a sampling bias that may not be obvious for the regular person (Fischhoff et al., 2005). This raises the question of whether and how past media coverage of data breach incidents affects patient response and coping with a healthcare data breach containing confidential health information.

Roseman et al. (1996) observe that the extent to which a person perceives themselves capable of controlling an event's motive-inconsistent aspects and successfully employing a problem-focused coping strategy differentiates between experiencing contending emotions (e.g., frustration or anger) or accommodative emotions such as sadness. Roseman et al. (1996) draw on Wortman and Brehm's (1975) review and synthesis on uncontrollable events, which argues that that if a person thinks they can still maintain control over uncontrollable circumstances, they will experience frustration or anger-like responses, while if control is assumed to be out of reach, the person will experience learned helplessness.

Table 2 concludes this section with a summary of the examined coping literature, creating the theoretical framework that serves as the research's foundation, guiding the data analysis performed later on.

TABLE 2 Summary of reviewed articles on coping

Author(s)	**Context**
Lazarus, R. & Folkman, S. (1984).	The concept of coping and coping process, alternative to traditional formulations
Perlin, L. I. & Schooler, C. (1978).	Theorizing coping
Folkman, S. & Lazarus, R. S. (1980).	Theorizing coping in a specific age sample
Folkman, S., Lazarus, R. S., Dunkel-Schetter, C., DeLongis, A. & Gruen, R. J. (1986).	Subjective coping processes across a range of stressful situations
Folkman, S. & Lazarus, R. S. (1988).	The relationship of coping and emotions in stressful encounters
Carver, C. S. & Scheier, M. F. (1994).	Situational coping throughout the phases of the event
Smith, C. A. & Lazarus, R. S. (1990).	Influence of emotions on adaptation
Thoits, P. A. (1995).	Review of existing literature on stress, coping resources, coping strategies and social support processes
Compas, B. E., Banez, G. A., Malcarne, V. & Worsham, N. (1991).	Perceptions of control and coping strategies used by children when dealing with stress
Endler, N. S., Speer, R. L., Johnson, J. M. & Flett, G. L. (2000).	Task and emotion coping strategies association with the presence of two types of situational control (objective and perceived)
Valentiner, D. P., Holahan, C. J. & Moos, R. H. (1994).	The influence of parental support on young adults coping with uncontrollable and controllable stressors
Liang, H., Xue, Y., Pinsonneault, A. & Wu, Y. (2019).	Coping strategies in response to IT security threats
Garnefski, N., Kraaij, V. & Spinhoven, P. (2001).	Cross-referencing emotion regulation and coping

4 RESEARCH METHOD

This chapter begins with a description of the research problem and design, followed by the objective of the study, description of the methods of research and analysis and their implementation, finally concluding in contemplations of the study's quality and ethics.

Despite the concept of coping being one of considerable interest in psychology and social sciences, research literature on data breaches is not very saturated regarding an individual's coping with data breach events in any service domain, especially in terms of research considering coping theory. Thus, after consideration and examination of the research topic and general research surrounding it, the research problem of the thesis was specified further with coping theory. Here, the guiding theoretical framework is Lazarus and Folkman's (1984) transactional model of stress and coping, presented in Figure 1. The purpose of this study is to research how patients react to personal data breaches in healthcare, with the objective of exploring patients' coping process in response to their confidential health information being compromised. The research question describing the foundation of the study is: *How do patients cope with personal data breaches that happen in healthcare?*

In the case of a personal data breach in healthcare, the sensitivity of the subject matter makes it reasonable to expect that those involved in the data breach will have strong reactions and will use coping mechanisms to try to regain some sense of stability in their lives amidst the chaos brought on by a traumatic event. Therefore, it is important and necessary to research the coping process within such circumstances to understand how patients respond and cope that policies may be established that better regard the victim of the breach.

This study takes a situation-oriented coping process approach, exploring how people cope with specific negative circumstances within the healthcare service sector, as to the scope of the research topic is limited to personal data breaches in the healthcare context. Coping activities are categorized depending on their function, such as gathering additional information and seeking social support (Folkman & Lazarus, 1980). The situation-oriented research methodology allows for a more detailed explanation of coping within

boundaries of the specific situation, but it has flaws, one of which is the findings' poor generalizability due to the approach's situation-specific nature, which does not prioritize cross-situational analysis (Folkman & Lazarus, 1980).

Much of the research on coping with specific situational stressors seek to understand the full coping process including the coping outcomes (Carver & Scheier, 1994). However, as the objective of this study is to understand how patients', whose personal health information is exposed in a healthcare data, coping process proceeds from initial reaction to coping activities, coping outcomes are eliminated from the research design, concentrating instead on the coping process within the domain of a data breach incident in healthcare.

Instead of seeking to make statistical generalizations, qualitative research aims to describe a phenomenon, comprehend a specific behavior, or provide a potentially meaningful understanding of a phenomenon (Tuomi & Sarajärvi, 2018, p. 98). As the goal of this study is to analyze patient coping with an invasive healthcare data breach, a qualitative research method is appropriate for the purpose. This decision to employ a qualitative method for the thesis can be justified by the differences in ontological assumptions between quantitative and qualitative research. According to Hirsjärvi and Hurme (2008, p. 22), a qualitative methodology views reality as subjective, whereas quantitative research approaches reality from an objective and consistent position. As the purpose of this study is to explore coping of individual patients, which have an inherently subjective quality to them, the integral subjectivity that is facilitated by qualitative research allows for deeper and more substantial understanding of the patients' experience.

4.1 Data collection method

The empirical data was collected using semi-structured interviews as the predominant data collection method. The flexible and situation-specific nature of interviews is often seen as their greatest advantage, as interviews allow for a broader interpretation of answers than for example a structured questionnaire (Hirsjärvi, Remes & Sajavaara, 2016, p. 204–205). As noted by Gillham (2000, p. 12), a questionnaire would suffice if the questions were to be simple and had well defined responses, as questionnaires are great when dealing with factual and binary issues but aren't always appropriate for topics that require depth, such as is the topic of this thesis. Complex human experiences are generally not easily discussed in an inherently clear and structured manner (Gillham, 2000, p. 16). The most valuable feature of interviews as a data collection method is the depth and vividness of the information that may be uncovered with it, possibly facilitating deep discovery of what the data truly reflects (Gillham, 2000, p. 10).

According to Hirsjärvi and Hurme (2008), the major advantage of interviews is that there is a direct linguistic contact between the interviewer and the respondent, providing an opportunity for ad-hoc in-depth examination and, if needed, for redirection of the interview. On the other hand, this creates some

disadvantages to be considered, as interviews can become lengthy and potentially be inaccurate, as unstructured and semi-structured interviews generate high volumes of unrelated information. (Hirsjärvi & Hurme, 2008, p. 34–35)

Due to the potential sensitivity of the subject, interview participants were not limited based on whether or not they had firsthand experience with invasive data breaches in healthcare. This meant that the interviewees may not have had past experience on which to base their comments and responses, and instead relied solely on their beliefs and assumptions. Folkman and Lazarus (1980) point out that what people think they would do and what they actually do in real situations don't generally correlate well with each other and that the most effective way to learn about situational demands and how people cope with them is to study how people cope in real stressful situations. To accommodate this objection, the study's data collection method, the semi-structured thematic interview, was supplemented with a vignette that served as the foundation of the interviews.

Vignettes are short stories about hypothetical events and fictional people that are told to the research participants and are meant to represent circumstances that the research participant can relate to, with the goal of learning more about the participant's beliefs and perceptions (Gourlay et al., 2014). According to Hughes (1998), a vignette allows the participants to provide a logical perception of the hypothetical story within the framework of a vignette since it provides them with distance and space. The vignette approach was applied to the data collection method by introducing the same fictional vignette to each research participant at the beginning of each interview. The interview participants were presented and advised to read a fictional news article of a personal data breach suffered by a private healthcare provider and a subsequent fictional email that was sent to the subject of the vignette, informing them that the participant had fallen victim to the personal data breach and that the compromised data included their personalized health information. The interviewees were asked to answer the interview questions from the perspective of the data breach victim. The vignette approach is a decently common method within psychological and sociological research, but within the domain of cyber security research it is very rare. Even so, the vignette approach allows for a novel approach to data breach research by imitating the specific circumstances that are under investigation, without subjecting the interview participants to potential traumatic experiences.

Semi-structured thematic interviews follow certain premeditated themes that are central to the research problem and provide a loose structure to the interviews (Hirsjärvi & Hurme, 2008 p. 48). The three themes guiding the interviews were *1. Patient reaction to personal data breach in healthcare and primary appraisal*; *2. Perception of controllability and secondary appraisal;* and *3. Coping strategy and coping activities.* The interviews were conducted as individual interviews, due to the potential sensitivity of the subject matter and the inexperience of the researcher. The discretionary sample consisted of local

Finnish adults, ensuring the accessibility of the interviews (Gillham, 2000, p. 12). Individuals were not excluded from the discretionary sample based on their own data breach experiences, nor were personal prior experiences a requirement for participation in the study. The number of participants was determined by what was feasible within the limits set by resources and scheduling requirements. According to Tuomi and Sarajärvi (2018, p. 99), 6-8 interviewees are sufficient for a thesis, keeping the workload manageable. The final number of research interviews was seven. Table 3 presents some of the final interview participants' demographic information. The interviews were carried out in Finnish to make self-expression as easy as possible for the respondents. This was done in order to ensure the linguistic benefits of the interviews as the chosen data collection method.

TABLE 3 Interview participants

Interview participant	**Age, gender**
Participant A	25, female
Participant B	25, male
Participant C	25, female
Participant D	27, male
Participant E	28, female
Participant F	30, male
Participant G	35, female

To ensure adherence to research ethics, prior to each interview, each participant was briefed on the purpose of the study, the confidentiality, storing and disposal of the material and was then asked to fill out a consent form (Hirsjärvi & Hurme, 2008, p. 20; Gillham, 2000, p. 15). The participants were informed that they were free to terminate their participation in the study at any time. The participants were reassured that the purpose of the interviews and the vignette is to explore coping based on hypothetical events and that at no point were the participants expected to share any information regarding their personal health information or potential past experiences. The purpose of the vignette method was to allow the respondents to address the fictional events from a non-personal experience, diffusing the potential distress brough on by the topic (Hughes, 1998).

4.2 Vignette

The vignette consisted of a fictional news article and a fictional email addressed to the interview participant. Both materials were written in Finnish and the

news article was constructed to contain information similar to the first news articles surrounding the Vastaamo data breach of 2020. This was done in order to create a realistic scenario to aid the interview participants' immersion. The news article described information of a patient information system data breach in a fictional healthcare facility Halla that had compromised the medical information of thousands of Halla's patients. Little additional information was given in the news article. After reading the news article, the interview participants were presented a subsequent fictional email from Halla the healthcare facility, informing the interview participant of the compromise of their medical information's confidentiality. The purpose of the vignette was to inform the interview participant of a data breach event in healthcare that affects them, in sufficient detail to foster a clear reaction and trigger the coping process, but generally enough that the application of the study is not limited to only specific types of data breach events in terms of how and why the breach happened.

4.3 Interviews

An interview's goal is to obtain information from which reliable conclusions regarding the topic under investigation can be reached (Hirsjärvi & Hurme, 2008, p. 66). An additional advantage presented by a half-structured interview format is the transparency of the questions, enabling the emergence of wide-ranging experiences. As a necessary element of a semi-structured interview, the interview frame containing the pre-meditated question themes was tested in pilot interviews, after which the interview frame was further modified and developed. Pilot interviews are necessary with thematic interviews to test the validity and aptitude of the predetermined themes (Hirsjärvi & Hurme, 2008, p. 71). The pilot interview participants were chosen from the researcher's social contacts so that the study's time schedule would not be disrupted. After two pilot interview iterations, the final thematic interview frame, containing the three question themes defined in chapter *4.1 Data collection method*, was reached, and was later employed in the research interviews. The interview themes followed the major phases of the coping process, divided into primary appraisal, secondary appraisal, and coping methods.

As a precaution to the ongoing COVID-19 pandemic, all interviews were conducted remotely via videocall services Zoom and FaceTime. The interviews were recorded as audio recordings with the permission of each interview participant. All interviews took place in May 2021 and ranged from 15-30 minutes in length.

At the beginning of each interview, the purpose of the study was expressed to the participants once more. The participants were then asked to familiarize themselves with the study vignette and after the interviewee signaled having had finished familiarizing themselves with the vignette, the participants were informed of the interviewer beginning the audio recording.

Some static demographic questions and a question regarding exposure to data breach news was asked of each participant first, after which the interviewer progressed to the first interview theme.

Theme 1, patient reaction to personal data breach in healthcare and primary appraisal, was used to explore the participant's primary appraisal of the breach event presented in the vignette and what emotions the interviewee believed they would experience in the situation.

Theme 2, perception of controllability and secondary appraisal, explored the participant's secondary appraisal by inquiring whether or not they felt in control and capable of taking steps to alleviate the situation.

Theme 3, coping strategy and coping activities, was intertwined with theme two in the sense that the interview participants often described their chosen coping strategies and activities while answering to questions about theme 2. Detailing follow-up questions were asked regarding theme 3 to investigate individual coping activities further. Finally, each participant was asked for final thoughts regarding the topic. This concluded the interview.

During the interviews, there were times where the interviewer noticed that the respondent lost touch of the vignette scenario and was not considering situational factors provided in the vignette. When this happened, the interviewer indirectly reminded the participant of the event presented in the vignette while asking a detailing follow-up question.

4.4 Data extraction and method of analysis

Data extraction began with transcription. Each audio recording of an interview was listened to and transcribed into Microsoft Excel in Finnish following the general practices of basic transcription, retaining all the features of speech containing information that is considered central to the problem being analyzed (Braun & Clarke, 2006). To protect the participants' anonymity and to prevent the research data from creating a personal register, the interview data was anonymized and coded from P1 to P7 (Ruusuvuori & Nikander, 2017, p. 438). The transcriptions were then translated into English while best preserving the true nature of the interviewee statements. Hirsjärvi and Hurme (2008, p. 20) question how well literal transcriptions follow interview participants' oral statements and to address this critique, the transcription and translation of participants' statements were transformed into written material while respecting linguistic nuance and meaning.

The interview material was analyzed with qualitative content analysis, a method used to examine content that has been written, heard, or seen (Tuomi & Sarajärvi, 2018, p. 103). Qualitative content analysis is often divided into two main categories based on which reasoning logic typical to qualitative research is used to draw conclusions (Tuomi & Sarajärvi, 2018, p. 103; 107). These categories are content-driven inductive reasoning and theory-driven deductive reasoning. There is, however, a third scientific reasoning logic called abductive

reasoning, which exists somewhere in between the two traditional reasoning rationales, and possible only if observation is guided by an existing theory (Tuomi & Sarajärvi, 2018, p. 107). Abductive reasoning in qualitative data analysis is considered to initially follow data-driven inductive reasoning, while connecting the findings to existing theory later in the analysis process (Tuomi & Sarajärvi, 2018, p. 110–111).

In this study, data analysis was performed with theory guided abductive content analysis, with initial codes arising from the interview data, which were later connected to existing coping theory and Lazarus and Folkman's (1984) coping process. The abductive data analysis process was conducted according to guidance of Tuomi and Sarajärvi (2018, p. 123) and Braun and Clarke (2006). The procedure began with getting acquainted with the data, which was followed by the reduction of interview data and the creation of initial codes. One theme at a time, the interview material was condensed and coded. Afterwards, there was a search for commonalities as the initial codes were reviewed, followed by thematization of codes into higher categories. This process was conducted iteratively with the interview data and its interpretation influencing each other until the higher categories could be connected to coping theory and Lazarus and Folkman's transactional coping model.

Reduction and coding of the interview data were conducted in Microsoft Excel. Material deemed irrelevant to the research problem was first removed from the data, after which the entire remaining data was reduced to simplified codes regarding each interview theme (Tuomi & Sarajärvi, p. 123). The initial codes were data-driven, identifying simplified basic elements and points of interest from the data (Braun & Clarke, 2006). Table 4 presents an example of initial reduction and coding of theme 1 interviewee statements.

TABLE 4 Example reduction of theme 1 interview data

Original research participant statement	**Reduced statement**
"I'm not afraid of things like that. Maybe I don't know enough, but I feel like there wouldn't be anything so personal there that it wouldn't bother me."	The event holds no influence
"I would immediately like more information as to what information has been compromised."	Need for more information
"I'd feel despair because I assume I have the right to decide who reads and processes this information."	Deprived right to decide Despair
"As part a bigger group of victims, I don't feel as much in danger as an individual."	Disappearing among the victims

Following Tuomi and Sarajärvi (2018, p. 124), the next phase of content analysis involved analyzing similarities and differences from the coded expressions. Concepts describing similar phenomena were grouped and clustered into classes, which were analyzed for upper and main categories, connecting the

data-driven analysis to existing theory (Tuomi & Sarajärvi, 2018, p. 124; Braun & Clarke, 2006).

Finally, the analyzed codes and classes were reviewed, refined, and conceptualized into a main category, connecting the abductive analysis to coping theory (Tuomi & Sarajärvi, 2018, p. 125, 132; Braun & Clarke, 2006). However, as mentioned before, content analysis is a continuous back-and-forth movement between the unprocessed data set, the coded material, and the generated analysis (Braun & Clarke, 2006). Keeping this in mind, the analysis was revisited and refined during reporting of the results with new ideas and contributions.

4.5 Quality of the study

Good and credible scientific research considers certain factors throughout the research process, such as the validity of the study, its reliability, and how research ethics are followed within that specific study. The terms validity and reliability most often refer to quantitative research, but even so, the same concepts should still be evaluated within qualitative research (Hirsjärvi et al., 2016, p. 231).

Research validity refers to a study's capacity to measure accurately and precisely what is to be measured. Reliability, on the other hand, refers to the consistency and reproducibility of the results, meaning that the study must be conducted and reported in a way that facilitates its potential recreation. The reliability of a research study can be emphasized by a detailed description of the implementation of the research process, including what was done, how it was done and how the results were reached. (Hirsjärvi et al., 2016, p. 231–232)

The quality and reliability of this thesis were emphasized by considering the validity of the methods throughout each step of the study to prohibit randomness of the results and by writing the report in sufficient detail and in a way that allows the repeatability of the research. According to Hirsjärvi et al. (2016, p. 232) the accuracy mandated by good reliability is to be taken into consideration at each phase of the research: the conditions under which the research material was produced must be detailed, and the fundamental task of creating classifications must be described transparently in the content analysis process. While interpreting the results, the reader must be informed of the reasons for the researcher's interpretations (Hirsjärvi et al., 2016, p. 232–233).

The validity of the research methods was supported by the applicability of qualitative research to a highly subjective and experience-oriented, sensitive research topic and by triangulating the data collection method with thematic interviews and a vignette. Triangulation of methods refers to using multiple research methods and is one of four typical methods of triangulation meant to add perspective to the research and thus emphasize validity (Tuomi & Sarajärvi, 2018, 166-167). The validity of the interview material was strengthened by simulating a potential real-life situation for interview participants in the form of

the vignette. Conducting the interviews as individual interviews rather than group interviews supported the validity of the interview material, as the participants did not have the opportunity to mirror their responses to others.

The reliability of this thesis is enhanced by reporting in detail all the phases of the study. The conditions of the research interviews were disclosed in detail in chapter *4.3 Interviews*. The research material was examined and analyzed with content analysis, which was considered an applicable analysis method for exploring meaning in the interview participants' subjective experiences. Abductive content analysis is initially content driven, but subsequently connects the analyzed material to existing theory to support the findings of the analysis. Abductive content analysis was considered as best fit for the research purpose, as the objective of this study is to examine subjective patient coping with a data breach event alluding to inductive analysis, while also incorporating existing coping theory. The full process of data analysis was described in chapter *4.4 Data extraction and method of analysis*, and the interpretation of results in chapter *5 Results and analysis* is supported by excerpts from the research interviews. (Hirsjärvi et al., 2016, p. 232–233)

Good ethical research follows the responsible conduct of research, honoring honesty, general attention to detail, accuracy in the recording of results, presenting, and evaluation of the research (Tuomi & Sarajärvi, 2018, p. 150). Regarding research concerning human subjects, Hirsjärvi and Hurme (2008, p. 20) state that true informed consent, confidentiality, management of possible consequences, and privacy are generally considered the most important ethical principles. It is also expected of ethical research to consider the contributions and results of other academics and researchers with care and respect (Tuomi & Sarajärvi, 2018. p. 151).

According to Hirsjärvi and Hurme (2008, p. 20), alongside the generation of new scientific information, the purpose of scientific research has an ethical obligation to try to provide improvement to the humane event that is under study. As research ethics require the consideration of the meaning of the study itself as a way of solidifying the ethical foundation of the research, following this sentiment, the ethical purpose of this study is to offer insights into how the individual victim in the data breach equation copes with the event and to ponder whether there is a systematic problem in data breach practices and laws that leave the individual victim in a vulnerable position after a healthcare data breach event. If the results of the study support this thought, this study may provide foundations for arguments that change must happen. As the measure of civilized society can be seen in the way society addresses and aids its weakest, the findings of this study may provide sharp commentary and criticism on how data breach events are managed and dealt with from the perspective of the individual. The potential social meaning of this study was considered as well, and it is the researcher's strong opinion that individual people as the subjects and owners of their personal data should be adequately protected before and after data breach events. The results of this study may give insights on how protected data breach victims truly feel post breach.

Hirsjärvi and Hurme (2008, p. 20) argue that ethical research must be well planned, and the function of adequate planning is to gain informed consent from data subjects, guarantee confidentiality and consider the potential consequences the study might have on its participants. This study was planned in a way that avoids triggering stress and negative experiences or memories in the research participants, by conducting individual interviews online so that participants and their statements are anonymous to one another and that each participant can choose the physical environment in which they participate in the interview, and by highlighting the vignette's fictional nature. The final reporting has an ethical obligation to ensure confidentiality of the research participants' private details (Hirsjärvi & Hurme, 2008, p. 20).

Transcription of oral interview material is a question of ethics, as the researcher must consider the accuracy of the written transcription in relation to the contents of the spoken statements (Hirsjärvi & Hurme, 2008, p. 20). This was considered within the boundaries of this study by retaining as much of the direct and indirect implications formed by word choices and other linguistic factors. This was made more challenging by the bilingual nature of the study, as the interview data was collected in Finnish, the native language of the interview participants as well as the researcher, but the transcription were later translated to English, the reporting language. The bilingual nature of the empirical data created challenges, as some words and idioms can't be directly translated from Finnish to English. In cases where direct translation compromised the true content of the statement and its context, the statement was translated in a way that retained the implicit meanings of the research participant.

5 RESULTS AND ANALYSIS

This chapter details the results derived from the thematic interviews, followed by the analysis of the results to extrapolate new meaning, and answer the research question. The results are presented one theme at a time and analyzed not only by considering changes in victim behavior but also by considering the victim's thoughts, emotions, and cognitions. The reporting highlights and comments on the themes emerging from the analysis and explaining how the results were analyzed, supported by excerpts of interview statements. Interview participants are referred to in the text as participants 1 to 7 or P1 to P7. The participant references have been randomized in relation to Table 3 to maintain participant anonymity. All participants described having been exposed to data breach news within the past year of the interview.

5.1 1st theme: Patient reaction to personal data breach in healthcare and primary appraisal

This chapter reports the patients' first reactions to learning of a personal healthcare data breach as well as the patients' primary appraisal of the event. Figure 2 presents the results of the abductive content analysis of theme 1 interview material, followed by an interpretation of its contents.

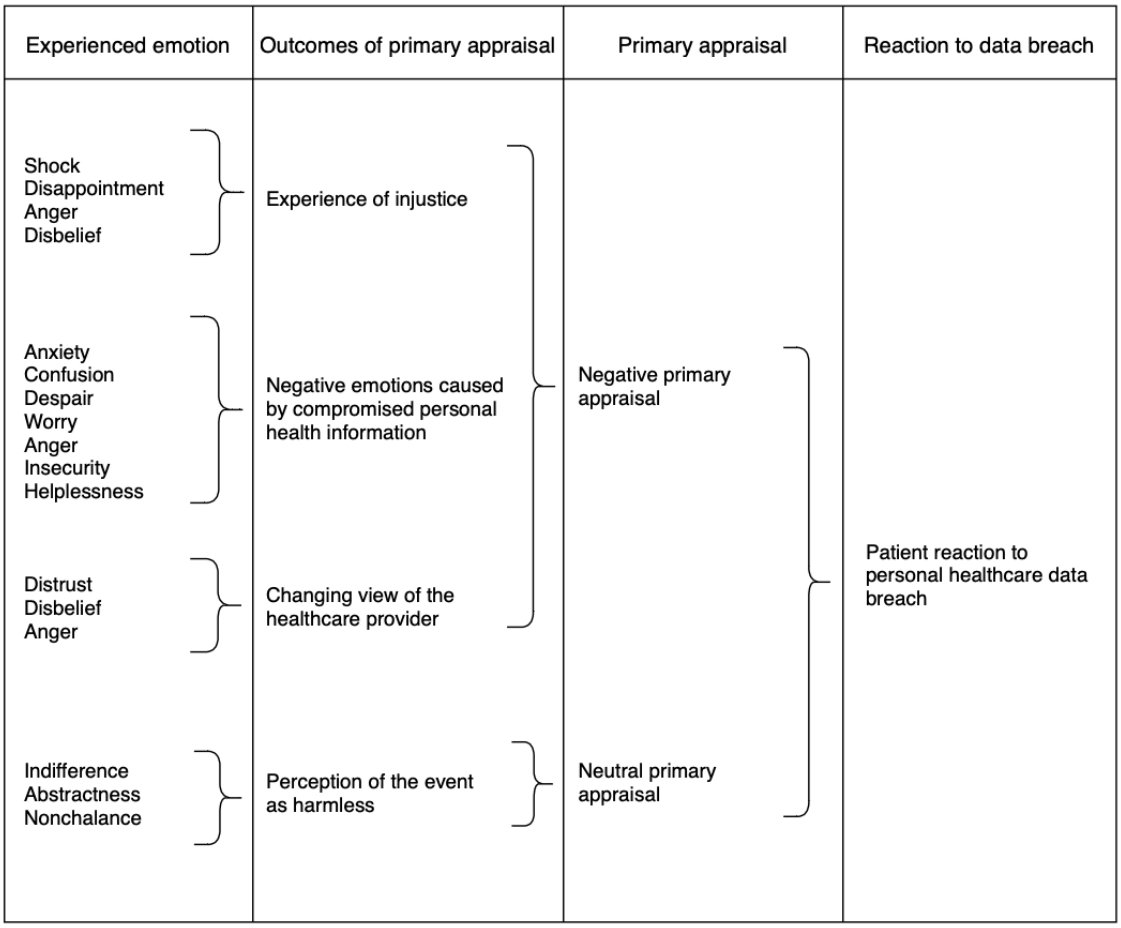

FIGURE 2 Summary of the analysis of patients' first reactions to healthcare data breach

Figure 2 depicts analyzed results of the participants' reactions to the data breach news, including cognitive outcomes that are produced by the patients' primary appraisal of the data breach event. From the right, a patient reacts to a personal healthcare data breach with either a negative or neutral primary appraisal, both of which lead to different perceptions of the event as outcomes of the primary appraisal. Each of the outcomes of primary appraisal are characterized by a set of experienced emotions described by the respondents.

As it is argued that primary appraisal is oftentimes a subconscious cognitive process (Lazarus, 1991b), the interview participants were interviewed more broadly about their reactions to the data breach event. The participants' answers were analyzed for implications for either negative or neutral primary appraisal of the event. According to the interview material, the vignette's healthcare data breach event was more likely to evoke a negative primary appraisal in the respondents as the patients. Analysis of the material shows that six out of seven interview participants clearly indicated their evaluation of the

data breach incident described in the vignette to present a plausible risk of harm to themselves as the vignette subjects.

While being interviewed about their reactions to the data breach event, interviewees described negative primary appraisal by reporting experiences of injustice, negative emotions caused by compromised personal health information, and their changing view of the healthcare provider. These negative experiences allude to a negative primary appraisal, as primary appraisal precedes emotional reaction, and an irrelevant or benign primary appraisal would not produce such negative emotions and experiences (Yih et al., 2020; Lazarus & Folkman, 1984). The participants who described negative perceptions of the event experienced a dissonance in their person-environment relationship, which was subsequently manifested by the generation of negative emotions.

5.1.1 Experience of injustice

Experiences of injustice were described as general negative thoughts towards the event that had transpired. The respondents described feelings of shock, anger and disbelief towards the event stemming from a general speculative foundation instead of the experience of personal victimhood, along with statements such as: *It would be really unfair, I'd feel a strong injustice as to why someone feels they need my or anyone else's health information (P2).* Common statements included the general expectation that health information is handled and stored according to its high confidentiality and a feeling of broken trust as a consequence of the data breach, as well as the outrageousness of the nature of the breach.

> I would be shocked and upset, because I would assume that such information is, as a rule, highly secured and protected. It's personal information, you wouldn't want outsiders to read them. (P3)

> It would be unbelievable, because this kind of thing should not happen. (P2)

> I would certainly also feel angry as to how can this happen in healthcare. (P6)

The statements indicating the experience of injustice cited above have a more objective, less personal quality to them compared to the other statements given by the interview participants regarding the outcomes of primary appraisal, considered later.

5.1.2 Negative emotions caused by compromised personal health information

Six interview participants expressed various negative emotions stemming from their personal medical information's confidentiality being compromised, signaling a negative primary appraisal. This outcome of the negative primary appraisal produced negative emotions including anxiety, despair, worry, shock,

confusion, anger, disappointment and feelings of insecurity and vulnerability. The most commonly described negative emotions were worry, disappointment and anger, evident in statements such as: *It would certainly make me a bit worried because I would not know what information has been leaked and to whom (P5).*

> I would feel insecure and vulnerable, maybe even desperate, because that's the kind of personal stuff that I hope would not be known to anyone other than the people I want to know. Especially if the situation wouldn't get resolved, it would be on my mind all the time and there would be no way forward and that insecure feeling would remain. It would change the way one treats similar companies and approaches the disclosure of their own information in the future. (P6)

Some participants expressed that the intensity of the experienced negative emotions varied based on the type and subjective sensitivity of the health information stolen in the breach.

> It depends on what data was in the breach, if there was something related to one's personal identity and social security number, that could do damage. So, if my personal information was lost in the breach, it would probably result in panic and worry, and I'd probably also be upset and disappointed at the healthcare unit. (P1)

> I don't think I would react initially with very strong negative emotions because such negativity doesn't help. What happened has already happened. I think I'd react more with confusion, so maybe I'd have that kind of mild negative or moderate negative reaction. – – If the data was something really sensitive, and not information about some ear infection or back pain, then my negative reaction would be much stronger. Then anxiety and anger towards the event would definitely come along. (P2)

> If I knew that there was sensitive data, like things about mental health in the Halla system, I would be a bit worried, but if the data was about my visits to a general nurse or to the dentist, then I wouldn't be interested much. I'd maybe react with more acute worry if sensitive health information like my personal mental health information was in the stolen data, but it would be annoying and straining. (P7)

5.1.3 Changing view of the healthcare provider

The third outcome of a negative primary appraisal evident in the interview data was the patient's changing perception of the healthcare provider. Five interview participants described a souring opinion of the healthcare company Halla triggered by experiences of unmet expectations, breached psychological contract and betrayed trust. The respondents described feelings of anger, distrust, incredulity, and disappointment.

> I would feel angry and disappointed towards the company, because I expect that personal information is taken care of and that this should not be my concern. (P1)

> I would feel distrust towards the company because I think the data breach signals that in general things have not been handled well. (P1)

> I'd be angry towards the healthcare unit because they are the ones that I have a service contract with, and they have promised to keep my information protected. It feels like trust has been betrayed. (P6)

Two interview participants differentiated their levels of anger aimed at the healthcare provider based on the presence of aggravating circumstances, indicating speculation on future reappraisal of the situational factors. The potential aggravating factors outlined by the interviewees were factors that affected the breach event, not factors affecting the data residing within the breached healthcare system.

> If there were mitigating factors, like if it was an insider who stole the information, then I think the breach could be considered an accident, but if there were aggravating factors, like if the company had been negligent of encryption or something, then that would make me angrier and more irritated. If there were no mitigating factors, I would react more strongly. (P3)

> Generally, I would trust that that system is done well, and that the attacker has been really skillful, and I would think that I have had bad luck, but if it later turned out that the system security was insanely poor or it was accessed through some strange root password that was like 000, I'd start to have much more anger and frustration towards the system, the system vendor and the administrators. If the breach was caused by a silly mistake, my anger would be greater. (P7)

5.1.4 Perception of the event as harmless

Replying to a question regarding their first reaction to the data breach news, one participant assessed the data breach event as having no negative influence on their personal life:

> I wouldn't really react. I'm not afraid of things like that. Maybe I don't know enough, but I feel like there wouldn't be any information that personal to me that it would bother me. (P4).

Referencing Figure 2, the above statement can be interpreted to signal that participant 4's primary appraisal of the data breach event results in a motive-consistent neutral appraisal of irrelevancy, which does not necessitate coping. Participant 4 perceives the event as harmless and non-influential to their life, characterizing their perception with emotions of indifference, nonchalance and unawareness.

As the analysis of participant 4's answers to questions regarding theme 1 described their primary appraisal of the situation to determine that the event held no special meaning or would cause no harm to their personal life, participant 4 did not describe further significant appraisal of the situation or active response in the answers to questions regarding themes 2 and 3. This can be interpreted as the coping process not being activated in the case of participant 4.

> I wouldn't know what to do, so I would do nothing. If I wouldn't get subjected to harm, I wouldn't really think about it. Only if something bad happened to me would I take action. (P4)

5.2 2nd theme: Perception of controllability and secondary appraisal

This chapter reports the analyzed results of the patients' perception of control following the primary appraisal of the data breach event reported previously in chapter *5.1 Theme 1: Patient reaction to personal data breach in healthcare and primary appraisal*.

The interview data demonstrates the patient's perception of control as the major contributing factor to the outcome of the secondary appraisal and further coping efforts. The interview participants described their feelings and thoughts of what they thought could be done about the data breach situation and the statements of the interview participants displayed a clear dichotomy between feeling of being in control and the feeling not being in control. The interviewees' perception of the presence or absence of control was interpreted based on various direct and indirect responses and statements given by the interview participants. The interview data supporting the two opposing perceptions of controllability are described next.

Four interview participants described feeling like they could take active steps to manage the breach situation, implying a positive perception of control as a result of the secondary appraisal. The participants described a need to control the initial breach situation and a feeling of being able to take active steps to do so: *I would look into what can be done to manage the situation, but I would also feel like I didn't really know what to do (P1)*. In the previous statement, participant 1 alludes to feeling able to respond actively to the data breach event, however also remarking their lack of confidence and uninformedness of the actions that can or should be taken. Participant 1 exhibits problem solving coping activities aimed to reduce the information gap surrounding their experience of the stress-inducing event. These coping activities will be analyzed later in this chapter, but for the sake of demonstrative statements from the raw interview material, the statement is included here to support the interpretation of a positive perception of control.

The respondents' statements about feeling like they could take measures to remedy or alleviate the situation, thus having a positive perception of control, were generally not supported by a high level of confidence in the belief of positive control: *I would take problem solving steps to figure out what I can do. I need to get some control of the situation back but controlling the situation may as well be just wishful thinking, I don't know if there's really anything that can be done (P6).*

Five interview participants described feeling like they had no control over the potential harm presented by the data breach event, describing the negative perception of control in more detail than they did for positive feelings of control.

These statements imply that these participants' secondary appraisal of the situational circumstances of the data breach incident concluded in feelings of helplessness. However, participant specific statements were not always consistent, as in some cases, multiple statements from one interview participant had different perception of control. *Yes, I would probably take steps and look into what I can do, but I doubt I would regain control over the situation (P1).* This implies, that perception of control is highly complex.

Interestingly, it could be interpreted from the interview material that, relating to the perception of no control, there was a dichotomy in the participants' assumption of the control over the confidentiality of the medical data prior to the data breach. Many participants described the perception of no control with a feeling of abrupt loss of control, characterized by the implicit assumption that the stolen medical information was well under control prior to the breach event, and that the control was abruptly lost due to uncontrollable forces: *The breach has already happened, I can't do anything about that situation anymore. No one can do anything about that situation anymore (P2).*

> I have no control over the situation, so it's pointless to try to do anything about it now. (P7)

> At this point, with this much information where it's not known what has been stolen and who has stolen it, I don't really see what I could actively do to remedy it. (P5)

This sentiment of abrupt loss of control was opposed by participant 1 with a general sentiment of 'these things happen' that could be interpreted from statements such as:

> Data breaches happen a lot and even to big companies, so it feels to me like the cyber world is a bit like the Wild West. Some really knowledgeable person can just do whatever they want, so in that sense I feel like the whole data breach question is in nobody's control. You can't protect yourself from such things beforehand, so if it happens, it's just very bad luck. (P1)

The above statement implies the thought that regardless of what proactive security steps are taken by data holders, companies and service providers, the risk of data breach events is never fully under control, thus implying that no one, not the patient nor any other actor, has ever had control over the situation that could be abruptly lost. Participant 7 described a similar, roulette-like sentiment that data breach events, such as the one presented in the interview vignette, are inevitable and happen randomly to random people.

> Well, thinking of this when nothing similar hasn't really happened to me, I think I'd react by thinking that this just happened to me and thousands of others and that I just had really bad luck. (P7)

To conclude this section, the interview data regarding theme 2 indicates that a positive perception of control leads to problem-focused coping, while a negative sense of control leads to emotion-focused coping.

5.3 3rd theme: Coping strategy and coping activities

This chapter explores the patients' deployment of coping strategies and coping activities within the coping process following the secondary appraisal. The results are derived from the interview respondents' answers to questions of the third interview theme, pertaining to what coping activities and conscious efforts the interview participants considered and would employ to restore the strained person-environment relationship following the primary and secondary appraisal, if faced with the personal healthcare data breach presented in the research vignette.

As suggested above regarding the perception of control, the interview material demonstrates a connection between a patient's perception of controllability and chosen coping strategy. The coping strategies that are under investigation within the frame of this study are problem-focused coping and emotion-focused coping, which according to the interview data, are preceded by a positive perception of control and a negative perception of control, respectively.

Figure 3 depicts the summary of results of themes 2 and 3, from patient perception of controllability to chosen coping strategy and the coping activities described by interview participants. These results will be discussed in greater depth later on.

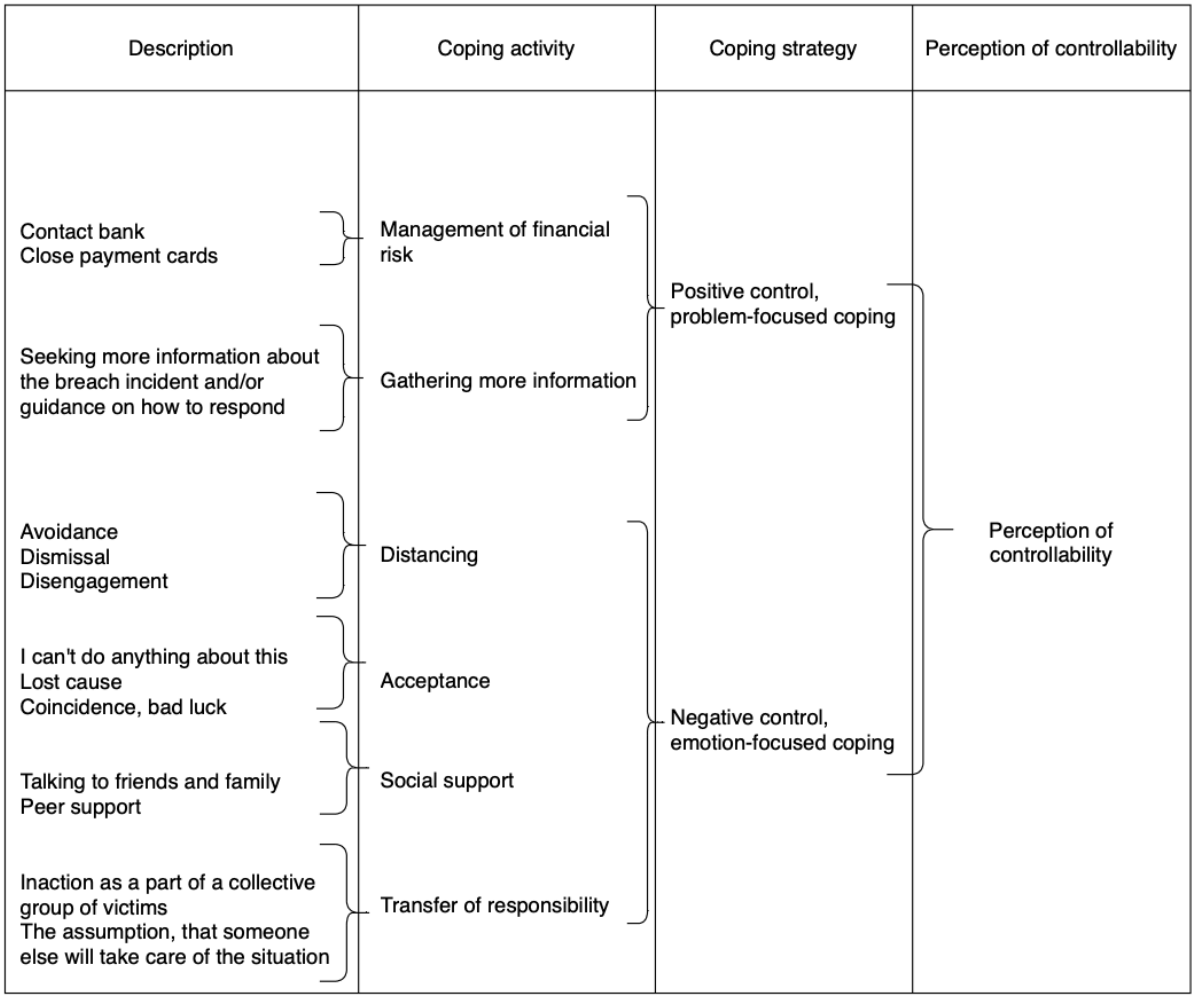

FIGURE 3 Summary of coping strategy and coping activities described by interview participants, divided by perception of controllability

5.3.1 Problem-focused coping

In reaction to a positive perception of control, three participants indicated problem-solving coping actions. These problem-solving activities described by the participants were few and could be reduced to two categories: actively seeking further information and controlling financial risk. The most often cited coping activity that could be interpreted as problem-focused coping was the intention to gather more information about the breach incident itself as well as general guidelines for responding to a data breach event as a victim. Seeking more information is an activity aimed at resolving the problem caused by incomplete knowledge. Thus, the effort of pursuing more complete information to correct the information deficit is an active decision to control external forces influencing one's life.

> Well, after the email or even reading about it in the news, I would try to contact that provider, the health facility, and ask exactly what information of mine has been compromised in the breach. (P7)

Two interviewees expressed a desire to take active steps to secure personal finances from potential future exploitation and abuse as a result of lost personal information. *If my social security number was compromised in the breach, I would look for advice on how to protect myself from fraud. I would make sure there is no financial harm (P3).* These statements are interpreted as active problem-focused coping aimed at reducing the risk of harm caused by the data breach and as a consequence of the respondent's positive perception of control.

> I would immediately look for information on how to proceed, like should some payment cards be closed and who should I contact. I would like to know better what the breach is all about and I'd like to get some control of the situation back. (P6)

Two participants stated that they would choose to disengage in order to wait for the situation to progress and to wait for further instructions, displaying emotion-focused coping in the form of disengagement to facilitate problem-focused coping activities later on: *I would wait for further instructions and then act on them (P5).* Participant 3 expressed similar actions of disengaging for the sake of subsequent information, however making distinctions between their chosen coping actions based on the sensitivity of the information lost in the breach. This is an example of dynamic and nuanced situation specific coping.

> In this situation and at this point, I would certainly wait for more information and possible follow-up instructions. If I got guidelines or advice on how to act, I would definitely follow the advice, because in the case of such a big breach and with such sensitive data, I believe there would certainly be experts figuring it out so I would trust their advice. (P5)

> I would follow media and my email traffic related to the breach, but I would probably not get very stressed. If my social security number and other personal information had been stolen, I would probably monitor media on the breach and ask for advice on what to do to protect myself against fraud, for example. (P3)

While other participants described disengagement in similar terms, similar goal-oriented disengagement for the sake of future problem-solving was not implied in other participants' statements. *I would just let the situation progress on its own (P2).* Statements, such as the one above, imply disengagement, distancing and acceptance for the sake of managing emotional turmoil and distress evoked by the stressor incident, thus implying the employment of these coping activities purely as means of emotion-focused coping.

5.3.2 Emotion-focused coping

Five participants described deployment of emotion-focused coping activities such as distancing, transferring responsibility, positive comparison and finding positive meaning, seeking social support and acceptance.

> I don't want to spend any more time on this, I've already gotten all the bad things out of it. In my opinion, the healthcare company manages their things badly, so then it is up to them to take that responsibility and take care of this situation, I shouldn't have to spend my own time on it. That would seem unfair. (P1)

The above statement displays efforts of distancing, which was analyzed and interpreted to stem from negative emotions such as frustration, disappointment, and anger due to used language and tone. The experienced emotions within the coping process mediate the selection of coping strategy and activities, which in the context of the above statement are avoidance and transfer of responsibility to manage emotional distress and uncontrollability. Likewise, the statement below describes participant 3 distancing themselves to protect their physical and cognitive resources in an event that is considered potentially harmful but where the perception of control is low.

> I would probably let the situation progress on its own. I would take part in class action lawsuits if such things happened, and I would be happy to receive some compensation if that was provided, but I don't think using my own resources and trying to contribute would help much. It's already happened, I can't do much about it anymore. (P3)

Four respondents described desires to transfer the responsibility of handling the data breach issue to external actors to create distance in order to reduce emotional distress and personal charge on the situation. *I feel that it is the company's responsibility to take care of this (P5).*

> Since I would be a pretty small part of the whole breach at that point, or that it's not likely that the breach would affect just my personal information, there would be others too, so I would trust someone else to take care of it and that I don't need to put any more effort into it. (P1)

> I don't think that solving the matter is my responsibility but the company's. (P3)

> I guess if the instructions were to do everything myself, I would follow those instructions and make criminal reports and other reports myself, but if there was a possibility of a class action, for example, I would go for it because it would be easier for me. (P7)

In the quote above, participant 7 displays rational reasoning between problem-solving activities and emotion-focused activities. These rationalizations are dependent of information that, within the vignette-context, was not available to

the respondent, implying that participant 7 is describing two possible avenues of coping activity based on potential future reappraisal of the situation.

Acceptance was described as the participants' method of dealing with perception of having little to no control over the matter. Sentiments regarding how well the acceptance of the uncontrollable nature of the event would manage emotional distress were diverse. Some participants were doubtful, and the thoughts ranged from lasting worry and discomfort to optimistic hopefulness.

> I would just let the situation progress on its own. If the situation would never get resolved and it would never be known who stole the information or why, then I think it would probably leave me worried and a bit distraught. (P2)

> It's likely that once data ends up on the internet then it will also stay there, but I also see it so that the data is also just forgotten in the future. It's too late to try to remedy the situation now. (P3)

> I'd let the situation be, but with other services I would probably be a little more cautious about where I give my information and how I operate online. But in this case, it's a healthcare service breach, so I can't really do much about it because if those services are needed, then your information will also be there, and you can't really do anything about it. The individual doesn't have much control over the situation. (P5)

> Well, I think that I would try to accept the situation and be like this happened to me and thousands of others, I was really unlucky, but this can't affect things like my employment or other relationships, so then it wouldn't be so... It wouldn't be able to do anything, so I would just try to accept the situation even though it would probably be hard. (P7)

Three interviewees spoke of the need to seek social and peer support as a means to relieve emotional distress to varying degrees. Participant 2 had a slightly pessimistic attitude to social support and spoke of it very nonchalantly: *I'd probably talk to a friend about what happened, but it's not like it's going to help the situation or that I can do much about it (P2).* Contrarily, participant 6 addressed seeking social support as a very important and personal activity of grappling with negative events that influence their life: *I would control those negative emotions probably by talking about them to my close circle, I can't block things completely out of my life and move on, it's not something that I can do (P6).* Peer support from other data breach victims was considered by two participants, one of whom argued their need of peer support depending on the sensitivity of their stolen medical information.

> I would probably seek support from my social circle, and I'd also probably seek some peer support online by looking up people who have had similar things happen, so that I could find some sense of how such a breach affects one's life and how likely it is that my information will be misused. (P1)

> If my mental health history had been compromised and was in the possession of the attackers, I might look for peer support, but otherwise I feel that it might be enough for me to read the news on the subject because it would make me feel like I am part of a collective group of victims and alleviate the pressure on me individually. (P7)

Participant 7's above statement refers to a group identity defined by victimhood in the data breach situation, which participant 7 describes to alleviate the feelings of scrutiny off of oneself. In terms of coping theory, this method of relieving emotional distress could be characterized as minimization or trying to see positive in a negative event by reasoning that being one person in a group of many victims is less harmful than being the only victim. Similar thoughts were communicated by other interviewees as well, described in the following citations. *As a part of a larger group of people, I don't feel like I'd be at risk of so much harm as an individual (P1).*

> I feel that this data breach is so large that it doesn't really personify me. If someone were to read my health information, then maybe I won't lose sleep over it (P3).

5.4 Summary of the results

Overall, the results obtained in this study on patient coping with a personal healthcare data breach are consistent with previous research and Lazarus and Folkman's definition of the coping process. According to the results of this study, a patient's coping process with a medical data breach begins with the primary appraisal of the event which can be either neutral or negative. The patient's perception of the event is influenced by the primary appraisal. A neutral primary appraisal results in a perception of harmlessness, whereas a negative primary appraisal of the data breach results in various negative perceptions, enabling the coping process to continue.

According to the results, patients experience distress in three distinct ways as outcomes of a negative primary appraisal of the data breach incident: experience of injustice, negative emotions caused by compromised personal health information and changing view of the healthcare provider. Experiences of injustice were described as general negative and unfavorable feelings toward the incident that had occurred. The second described outcome of a negative primary appraisal was experiencing a range of negative emotions as a result of the breach of the patients' medical information's confidentiality. The third outcome described by the participants was the patient's changing perception of the healthcare provider, propelled by experiences of broken trust and breached contract.

A negative primary appraisal was more prevalent among the interviewees, as a personal data breach was considered as predominantly damaging to the breach victims by the interview participants. However, the results were not unanimous, as one interview participant stood out from the pool of interviewees in terms of impression of harmfulness and their primary appraisal

of the breach. This participant's primary appraisal of the data breach event was neutral, with the event having no negative impact on their personal life, indicating that the event did not necessitate coping and hence prevented the coping process.

The cognitive outcomes and emotions experienced after a negative primary appraisal influenced the patient's secondary appraisal of the data breach incident. The patients' secondary appraisal of the event influenced their perception of controllability of situational factors, which was either positive or negative.

The results indicated that control is a key contributing element to the outcome of the secondary appraisal and subsequent coping attempts. The interview participants described their feelings and thoughts of what they felt could be done about the data breach issue, and their statements displayed a divide between feeling in control and feeling out of control.

Four interview participants stated that they felt they could take active actions to address the breach scenario, suggesting a positive perception of control resulting from the secondary appraisal. Five interview participants acknowledged feeling powerless and like they had no control in the face of the data breach's potential harm. However, it is evident here that research participants could have inconclusive and inconsistent beliefs and considerations regarding their perception of control, as some interview participants described feeling both in control and out of control.

The results signal that a positive perception of control leads to the deployment of the problem-focused coping, whereas a negative perception of control leads to emotion-focused coping. As a result of a positive perception of control, three interview participants described problem-solving activities that were reduced into two categories based on similarity: seeking further information and management of financial risk. The goal to obtain more information to resolve the problem created by insufficient knowledge was the most often mentioned coping activity that could be interpreted as problem-focused coping.

Two participants described choosing to disengage to wait for the situation to progress and to wait for more instructions, demonstrating nuanced coping by using emotion-focused coping activities to facilitate later problem-focused coping actions.

As a result of a negative perception of control, five participants described the use of emotion-focused coping activities such as distancing, transferring responsibility, positive comparison and finding positive meaning, seeking social support and acceptance as their chosen coping activities. Figure 4 displays the flow of the patient's coping process in response to a medical data breach.

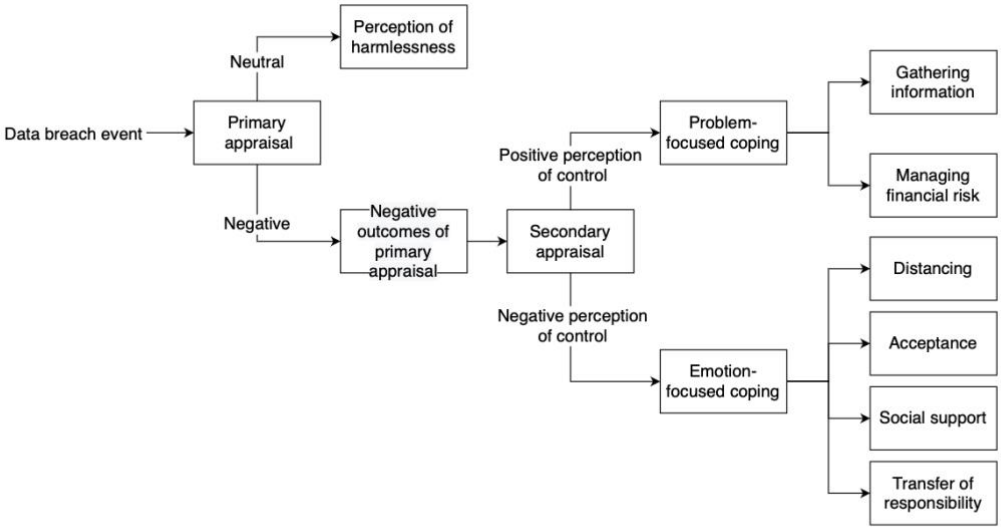

FIGURE 4 Process of patient coping with personal data breach in healthcare, combined from results of themes 1, 2 and 3

Unsurprisingly, the results indicate that how patients cope with a medical data breach is not uniform, but highly subjective. It was indicated by interviewee statements that a patient's coping with the breach event is influenced by what kind of health information is stored within the breached system, what information was stolen and the subjective interpretation of how the patient perceives the stolen information's sensitivity.

The participants emphasized negative emotions more after a negative perception of control than they did after a positive perception of control. This implies that a perception of uncontrollability may magnify negative emotions experienced in relation to the stressful situation more than when the patient perceives the situation as controllable.

6 DISCUSSION

The previous section reported the analysed results of the research interviews. This chapter contains a more elaborate commentary and reflection on the results supported by existing scientific literature. Practical implications of the findings are addressed, followed by a critical examination of the limitations relevant to the study.

6.1 Patient coping with personal data breach in healthcare

The results of this study indicate that the healthcare data breach victims in this study were more likely to appraise the data breach event negatively, thus triggering the coping process defined by Lazarus and Folkman. This is congruent with existing research, as the general assumption in research on the effects of data breach events is that the breach victims consider such events to be negative, harmful and a violation of expectations (Chatterjee et al., 2019; Chen & Jai, 2019; Janakiraman et al., 2018). The results of this study indicated that negative emotions and the use of coping strategies were triggered by the patients' primary appraisal that judged the circumstances to be detrimental or destructive to the individual, confirming the theory that cognitive appraisal, emotions, and coping are all linked (Yih et al., 2020). The study found that the respondents experienced injustice, negative emotions caused by their compromised medical information, and a change in their view of the healthcare provider as an outcome of a negative primary appraisal. The results also suggest that after a negative primary appraisal of the data breach event, a victim may experience any combination of the outcomes described above as their coping process develops.

In terms of experiences of injustice, the research participants expressed generic negative thoughts and feelings targeted towards the breach, characterized by a general thought of "*this shouldn't happen to anyone*", rather than thoughts that were specific to the self or a specific actor. The respondents

described experiences of injustice stemming from unmet expectations of high security and confidentiality in healthcare. This is unsurprising as the link between the experiencing a violation of a psychological contract and the violation of trust between parties is well established (Wang & Huff, 2007; Carre et al., 2018b).

The findings showed that a negative primary appraisal can also result in an outcome of negative emotions such as worry, shock, anger and disappointment triggered by the victim's knowledge of their personal health information being compromised. An interesting finding is that despite the fact that fear is a typical emotion felt when a data breach victim learns of the breach (Chatterjee et al., 2019), the findings of this study indicated no evidence of fear in the participant responses, only worry. However, this may be indicative of the fabricated conditions that allow the interview respondents to consider the event without experiencing the true stressor event, which prohibits drawing conclusions regarding the absence of fear in the described negative emotions reported by research participants.

According to some interviewees, the intensity of the experienced unpleasant feelings varied depending on what kind of health information was stored within the breached system. The participants expressed varied degrees of anger moderated by their subjective perception of the sensitivity of the stored information, contradicting Chatterjee et al.'s (2019) suggestion that the anger experienced by data breach victims is not influenced by the scope and extent of the data breach.

The last outcome of a negative primary appraisal established in the results of this study describes the patients' souring opinion of the healthcare provider due to unmet expectations, breached psychological contract and betrayed trust. What differentiates this outcome from the first outcome of negative primary appraisal described earlier, experiences of injustice, is that the changing view of the healthcare provider described by the research participants considered only the victim's personal relationship with the healthcare provider. All statements that fell under the outcome of experiences of injustice were defined by general views focused towards the data breach itself as a criminal act, rather than the acts or inactions of the healthcare actor.

Respondents described their opinion of the healthcare provider changing for the worse due to unmet expectations, breached psychological contract and betrayed trust. Some participants described changes in their experienced levels of anger influenced by what the participants referred to as aggravating circumstances surrounding the breach event, such as subpar security practices prior to the data breach. Similar findings were described by Bansal and Zadehi (2015), who found a negative relationship between perceived seriousness of violations and violated trust, moderated by the type of privacy infringement in question. In the case of this study, the findings imply that the data breach victim determines a subjective opinion of the situational factors that constitute the potential aggravating factors. The victim's judgement on these situational factors moderates the negative association between the victim's perception of

the data breach event and their changing opinion of the healthcare provider: two participants stated that their opinion of the healthcare provider would drop further, had the breach been caused by internal negligence than in the case where the breach was caused by skilled malicious hacking.

The meaning and significance of a benign primary appraisal in the context of personal healthcare data breaches must also be considered, as the interview findings also included a participant experience of a neutral primary appraisal. In the interview, participant 4 explained their impression of the data breach incident's harmlessness by emphasizing the event's abstract character. This could indicate a lack of understanding of the volume of personal data stored within an electronic healthcare system or the significance of data in the modern world. Similar findings were considered contradictory by Chen and Jai (2019), who found no significant difference in reactions to a data breach between loyalty customers and non-loyalty customers, despite loyalty-customers having had much more personal information compromised. Chen and Jai (2019) hypothesized that consumers might not be aware of the volume of personal data possessed by the victim company, thus not recognizing the impact of the incident. Although the conditions of a retail organization's data breach (Chen & Jai, 2019) and the healthcare data breach investigated in this study are not comparable, the findings are interestingly similar.

One might seek to interpret a sense of emotional coping from participant 4's statements in the form of avoidance and escapism to facilitate psychological adjustment to the circumstances, but within this study, the researcher believes this to be too speculative and unethical with the existing primary data, as such interpretation would reconstruct the contents of participant 4's statements too much. However, Liang, Xue, Pinsonneault and Wu (2019) suggest that inward directed emotion-focused coping can divert the victim's attention away from the stressor, causing them to overlook the problem entirely, dismiss the danger, and deny the repercussions of such a threat. Not paying close enough attention to the incident or ignoring its relevance may cause the victim to be unmotivated to participate in problem-focused coping practices (Liang et al., 2019), which may provide insights to participant 4's perception of harmlessness.

The notion of controllability over the source of stress has been extensively acknowledged in coping literature as having a dramatic influence on how an individual copes with the stressor (Endler, Speer, Johnson & Flett, 2000; Valentiner, Holahan & Moos, 1994). Congruent with this notion, the results of this study indicate that the patients' perception of control is a contributing factor determining the outcome of their secondary appraisal that influences the patients' choice of coping strategy and coping activities. However, the perception of controllability described by the research participants was not always participant-consistent, as some interview participants described perceiving some control over the event yet having pessimistic thoughts regarding their actual efficacy of exerting control: *I would take problem solving steps to figure out what I can do. I need to get some control of the situation back but controlling the situation may as well be just wishful thinking, I don't know if there's really anything that can be done (P6).* This suggests that the participants' combined

judgments of contingency and personal competence of exercising control (Compas, Banez, Malcarne, & Worsham, 1991) within the data breach domain were insufficient, given their low confidence in their positive perception of control over the data breach situation.

> Yes, I would probably take steps and look into what I can do, but I doubt I would regain control over the situation. (P1)

Interestingly, when questioned regarding perception of control, some participant statements implied a duality on how patients generally view the safety and confidentiality of their medical information, without considering specific breach incidents and security failures. Participants 1 and 7 considered the cyber realm and its merging with the healthcare sector to contain an inherent insecurity factor that can't be mitigated, thus vocalizing pessimistic opinions of there never having been proper control and confidentiality over their sensitive information. Other respondents described feeling like control over medical records confidentiality was lost out of the blue. According to these interesting statements, this dichotomy was conceptualized as the experience of abrupt loss of control versus inherent uncontrollability of data safety. Existing data breach statistics paint a pessimistic view of the competence of current data breach prevention aspirations (Bisogni & Asghari, 2020), which in addition to the dichotomy interpreted from the statements in this study may be used as a justification to further research patient expectation of confidentiality as an independent research topic.

Following the first and secondary appraisals, the respondent statements regarding what coping activities and conscious efforts they considered and would use to reestablish the disrupted person-environment relationship were mixed and highly subjective, ranging from deployment of both coping strategies to deployment of either one. When asked to reason their choices of coping activities, the participants gave similar reasonings following many similar themes for each coping activity.

The results of this study indicate that following a positive perception of control in the face of a personal healthcare data breach, patients employ problem-solving coping techniques such as aggressively seeking further information and controlling financial risk. This is supported by Endler et al.'s (2000) finding that a perception of situational control is related to problem-focused coping. Endler et al. (2000) also found that having a stronger sense of control is linked to having less anxiety and relying less on emotion-focused coping. Taking steps to secure personal finances by for example monitoring electronic financial transactions or limiting bank transfers is a common encouraged activity intended for breach victims to mitigate the realization of risks and such problem-focused coping activities are the result of the breach victim's perceived situational control. Consistent with Endler et al. (2000), the statements of participants 1 and 6 indicate that the participants' positive perception of control of the data breach situation allowed them to take problem-solving steps. However, the same participants' impression of self-

efficacy to control the event could be perceived as low, negating the anxiety-controlling benefits of a high perception of control (Endler et al., 2000).

Some participants described choosing to withdraw from making conscious efforts in order to wait for the scenario to develop and for further instructions to be given. Passive waiting, instead of active seeking of information, describes a nuanced coping effort employing emotion-focused activities for the sake of potential problem-solving activities later on, as both forms of coping can be mutually facilitative. Participant 3 described comparable disengagement for the sake of waiting for further information while distinguishing between their selected coping methods based on the sensitivity of the data lost in the incident. This finding doesn't support Liang et al.'s (2019) results suggesting that distancing decreases problem-solving coping activities. Existing coping literature provides evidence supporting the notion that people commonly use different, even clashing coping methods and mechanisms at the same time (Folkman & Lazarus, 1985).

Distancing, shifting responsibility, positive comparison and finding positive significance, seeking social support, and acceptance were characterized by five interview participants as their chosen coping activities, all of which are considered coping behaviors that are part of the emotion-focused coping strategy and have the common objective of reducing emotional distress (Lazarus & Folkman, 1984, p. 150; Folkman, Lazarus, Gruen & DeLongis, 1986). According to Roth and Cohen (1986), emotion-focused coping can result in increasing optimism, which especially in the long run can positively influence the facilitation of a problem-solving approach. However, Roth and Cohen (1986) note that in uncontrollable conditions, the reduction in stress and anxiety produced by avoidant emotion-focused coping may not be as helpful if it hinders the resolution of the stressor causing distress. The potential benefits of emotion-focused tactics in such conditions are contingent on the concurrent or alternate employment of problem-focused strategies (Roth & Cohen, 1986).

The findings of this study indicate that patients employed distancing as a coping mechanism in response to a negative perception of control over the healthcare data breach incident. Participants 1 and 3 described choosing to distance themselves from the situation but rationalized their choices differently. Participant 1 described distancing as a consequence of anger, whereas participant 3 described distancing as a proactive method of protecting their personal resources by directing attention away from the breach event. A possible explanation for patient distancing as a coping mechanism post breach follows Liang et al.'s (2019) suggestion that the objective of psychological distancing is to distract the person from their experienced distress while the dynamic stressor situation evolves. This is suggested within the results of this study, as many research participants emphasized their lack of information as rationale for their coping decisions.

Transferring responsibility and shifting blame as a coping mechanism was a noticeable emotion-focused coping activity in the findings of this study. Four respondents described seeking to externalize responsibility and blame the data

breach event on the healthcare provider. Here, the context of the breach under study makes it easy and arguably permitted for the patients to externalize blame and responsibility to the healthcare facility. According to Liang et al. (2019), transfer of responsibility can be considered outward emotion-focused coping as the patient's wish to shift responsibility is an outcome of outward directed negative emotions. Liang et al. (2019) argue that outward emotion-focused coping facilitates adaptation and successful coping by enhancing problem-focused coping, but as is evident in participant 3's statement *'I don't think that solving the matter is my responsibility but the company's'*, the respondent displays a desire to transfer responsibility to the healthcare provider while also implying the participant's unwillingness to personally act in problem-solving ways.

The participant statements that described acceptance as a coping strategy had an inherent implication of failure to control the situation, followed by acceptance and disengagement. The acceptance coping technique is defined as the idea of accepting the reality of what has happened and that there are currently no active coping strategies available (Garnefski, Kraaij & Spinhoven, 2001; Carver, Scheier & Kumari Weintraub, 1989). According to Carver et al. (1989), acceptance is related to higher self-esteem and optimism as well as lower reported anxiety. The participants' responses implied giving up on trying to alter the circumstances, but the patients' perceptions of their ability to alleviate distress by accepting the condition ranged from skepticism and long-term anxiety to hopefulness, cautiously contrasting with Carver et al.'s (1989) finding of the relationship between acceptance, optimism and lowered anxiety.

Respondents mentioned seeking social support as a way of reducing emotional and psychological distress. Social support has been established in extant literature to be an adaptive mediator between stress and wellness (Folkman & Lazarus, 1985), promoting problem-focused coping in controllable situations and supporting emotion-focused psychological adjustment with uncontrollable stressful events (Valentiner et al., 1994). As the participants of this study described social support as an activity following a negative perception of control, it can be interpreted that the function of such behavior would be to alleviate psychological distress. Liang et al. (2019) argue that social emotional support, such as external actors empathizing with, legitimizing, and exploring the victim's sentiments helps the victim comprehend why the stressful event is causing them distress. Such communication reduces the victim's distress and allows them to concentrate on taking action to eliminate the stressor based on a more objective evaluation of the circumstance. On the part of the breach victim, Liang et al. (2019) claim that venting as a common means of expressing unpleasant feelings may help subsequent rational decision making and problem-solving in the face of stressful situations.

Respondents of this study described feeling less distressed by considering themselves as a part of a large group of victims. While considering emotion-focused coping activities, this thought process may stem from a positive comparison and positive reappraisal of the event following the lines of "*It could*

have been worse." Putting the stressor event into perspective, according to Garnefski et al. (2001), downplays the importance of the incident and emphasizes its relativity. Similar to the effects of acceptance, according to Carver et al. (1989), employing positive reappraisal as a coping mechanism has favorable influence on optimism and self-esteem while mitigating anxiety.

The participant statements mentioned above imply that the respondents feel a sense of group or communal identity, similar to collective victimhood or collective trauma that mitigates their experienced psychological distress. This is positively surprising, as according to (Cross et al., 2019), feelings of isolation may be experienced when a data breach involves highly sensitive information. However, neither the concept of collective victimhood, which is defined as the psychological experience and repercussions of collective victimization perpetrated on another group purposefully (Noor, Vollhardt, Mari, & Nadler, 2017), nor the concept of collective trauma, described as the psychological reactions to a traumatic incident that impacts a group as a whole and is memorialized in the group's collective memory (Hirschberger, 2018), are applicable to the data breach incident described in this study. Therefore, while a large-scale medical data breach may inflict strain and distress on a group of people and individuals within that group may consider the existence of a peer group of victims as a mitigating factor to influence the victim's coping, under the above definitions, the victimization of the data breach victims would not be considered collective victimhood or collective trauma.

6.2 Practical and scientific contribution

This section considers the practical and scientific significance of the findings described in the preceding sections. The findings' generalizability and portability are also considered.

This study doesn't produce novel information on coping theory per se, but it presents new information on how patients' coping process progresses and what coping activities patients deploy in such circumstances of a personal healthcare data breach. As explained in chapter *4.5. Quality of the study*, the ethical purpose of this study is to see if there is a systemic problem with data breach processes that leaves the individual victim in a vulnerable psychological and practical position following a data breach concerning highly confidential medical information. The findings of this study show that patients are unsure what to do in the aftermath of a data breach, and that many victims expect public and private actors to assist them in minimizing possible dangers, thus depending on external actors. Psychological distress as a result of the healthcare breach is frequent, and patients adopt problem- and emotion-focused coping strategies as well as a variety of coping activities to cope with their distress. Due to the uncontrollable nature of data breaches, the distress experienced by the victims will not always be absolved, leaving the patient with the responsibility

to pick up the pieces as best as possible and move on. This can be argued as unjust and can be used as justification for change in policy.

This study gives insights on how healthcare data breach victims feel post breach and how they cope with the data breach event. The results of this study, such as the outcomes of the negative primary appraisal, can assist public and private healthcare providers to better develop their communications and interactions with victims in the event of a personal data breach by identifying which victim experiences should be addressed first.

The findings of this study revealed an interesting contradiction in the participants' perceptions of control over the confidentiality of medical data prior to the data breach. This particular finding may be beneficial to healthcare provider and professionals, as it encourages transparency to discover ways to communicate and reassure patients of applied data protection measures and strategies used to secure patient information and medical records.

In terms of scientific contribution, this study was successful in exploring patient coping with a personal healthcare data breach, and the findings add to the data breach discourse by emphasizing the victim's point of view, perhaps encouraging more future research into the victim's perspective.

6.3 Limitations

An expectation of critical and thorough research is to also consider the failures and limitations of the study. This study, like most others, has certain limitations. In terms of the applied research method, Folkman and Lazarus (1980) argue that the findings of situation-oriented research, such as this study, are not generalizable across circumstances. In addition, while the vignette-approach is novel in the context of data breach studies, it poses a limitation in the form that the participants were provided with incomplete information regarding the vignette incident. This was done to elicit a realistic first reaction to a data breach event from the research participants in order to obtain as much accurate and truthful information as possible for the study. However, it was later discovered that the incomplete information posed a limitation to the study as one of the only problem-solving action that the research participants chose as a coping activity was to gather more information. Gathering more information as a problem-solving coping method is a valid result, but the layout of the study may have limited the depth of the problem-focused coping activities that were deployed by the respondents, as reappraisal following new information was not invited by the vignette.

Another drawback of the vignette technique is that the discrepancy between self-reported future conduct and actual behavior has always been a concern for social science researchers (Hughes, 1998). Researchers frequently seek to relate beliefs of future action to actual behavior, but there is conflicting

data about the usefulness and accuracy of employing vignettes to reflect how individuals behave in real life (Barter & Renold, 1999).

A limitation of this study that restricts thorough analysis of the full coping process is that the data breach event under study was fabricated, thus preventing patients to reappraise the situation as it unfolds. This is a flaw in the research design, and it is recommended to be taken into consideration in future research and research design.

7 CONCLUSIONS

The purpose of this study was to explore patient coping with a healthcare data breach containing personal health information. According to Seh et al. (2020), the healthcare industry is the most compromised, accounting for over 60% of all recorded data breaches in total. As the health information stored and processed within the healthcare sector is highly confidential by nature, the combination of the nature of the information and the highest frequency of data breach events in healthcare creates a compelling challenge to be considered and addressed from the victim's point of view. The objective of the study was to explore how a patient presented with a personal healthcare data breach would cope with such an event and how the patient's coping process would proceed. The research question was the following:

- How do patients cope with personal data breaches that happen in healthcare?

The study was conducted as a qualitative interview study with semi-structured thematic interviews supplemented by a fictional vignette-scenario to induce realistic responses from interview participants. The primary data gathered from the thematic interviews was processed and analyzed with theory-guided abductive content analysis, which first followed initial inductive analysis and later connected to existing theory. This approach allowed for inductive data-driven findings while still considering the research topic within the existing coping-theory framework.

The findings of this study suggest that patient coping with a healthcare data breach follows the general form of Lazarus and Folkman's (1984) definition of the transactional coping process while generating many concurrent outcomes from the coping process, such as the outcomes of primary appraisal (experience of injustice, negative emotions and changing view of the healthcare provider). This is followed by the secondary appraisal of the situation and the patient's perception of control, which influences the patient's chosen coping strategy and coping activities. Following a positive perception of control, the

coping strategy reported by interview participants was problem-focused coping, realized by gathering information and managing financial risk, whereas following a negative perception of control, the reported coping strategy was emotion-focused coping and coping activities such as distancing, acceptance, social support, and transferring responsibility.

The findings also indicate that patients may utilize emotion-focused coping in hopes of facilitating problem-focused coping later as the stressor situation evolves. The results, however, did not show that problem-focused coping was used to facilitate emotion-focused coping. There were also findings that negated all coping, indicating that the simulated data breach event was not considered harmful by the respondent.

The findings of this study show that in the context of this study, patient coping with data breaches is dynamic and can change based on rationale and reappraisal of the incident. The research participants described nuanced coping by employing both problem-focused and emotion-focused coping as a means of coping with the stressor.

The results support Lazarus and Folkman's (1984) concept of the transactional coping process, while disputing some other results of previous research (Chatterjee et al., 2019; Liang et al., 2019) This study contributes to the data breach discourse by exploring and describing what kind of meaning patients assign to intrusive data breach events, by dissecting the coping activities used by patients within the simulated data breach event, as well as by describing the three reported outcomes of negative primary appraisal of the breach event, which can be used to improve communication with data breach victims to support transparency and mitigate the victim experiences of distress.

Because of the broad definition of data breaches and the possibly such disastrous consequences of data breaches in healthcare in cases of critical infrastructure or medical equipment failing or even tampering of patient data, the subject of data breaches in healthcare is much broader than the scope of this thesis and needs further analysis and investigation. This study presented some interesting thoughts to be considered for subjects of further research. In terms of patient coping, the choice of coping strategy can be influenced by personality factors, prior experiences, and habit, and it would be interesting to explore how such antecedent factors influence coping in such a potentially sensitive subject area. Also, due to limitations presented by the research method of this study, the results of this study could be tested in a controlled environment experiment. The dichotomy between this study's research participants' expectation of confidentiality prior to a data breach event should also be studied further as an independent research subject, as well as whether patient coping varies depending on whether the healthcare provider is a private or public actor. An interesting topic would also be the exploration of how the media coverage of past data breaches influences patient response and coping with healthcare data breaches.

REFERENCES

Abidin, M. A. Z., Nawawi, A. & Salin, A. S. A. P. (2019). Customer data security and theft: a Malaysian organization's experience. Information & Computer Security, 27(1), 81–100

Ablon, L., Heaton, P., Lavery, D., & Romanosky, S. (2016). *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information.* RAND Corporation. Retrieved March 24, 2021, from http://www.jstor.org/stable/10.7249/j.ctt1bz3vwh

Bansal, G. & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. Decision Support Systems, 71, 62–77. doi:10.1016/j.dss.2015.01.009

Barter, C., & Renold, E. (1999). *The Use of Vignettes in Qualitative Research.* Social Research Update, Issue 25. https://sru.soc.surrey.ac.uk/SRU25.html.

Bentley, J. M., Oostman, K. R. & Shah, S. F. A. (2018). We're sorry but it's not our fault: Organizational apologies in ambiguous crisis situations. *Journal of Contingencies and Crisis Management, 26(1),* 138–149. doi:10.1111/1468–5973.12169

Bisogni, F. & Asghari, H. (2020). More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws. Journal of Information Policy, 10, 45–82. doi:10.5325/jinfopoli.10.2020.0045

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3(2)*, 77–101.

Brosch, T., Scherer, K. R., Grandjean, D. & Sander, D. (2013). The impact of emotion on perception, attention, memory, and decision–making. *Swiss Medical Weekly, 143(19-20)*. doi:https://doi.org/10.4414/smw.2013.13786

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

Carre, J. R., Curtis, S. R. & Jones, D. N. (2018b). Ascribing responsibility for online security and data breaches. Managerial Auditing Journal, 33(4), 436–446.

Carver, C. S. & Scheier, M. F. (1994). Situational Coping and Coping Dispositions in a Stressful Transaction. *Journal of Personality and Social Psychology, 66(1),* 184–195.

Carver, C. S., Scheier, M. F. & Kumari Weintraub, J. (1989). Assessing Coping Strategies: A Theoretically Based Approach. *Journal of Personality and Social Psychology, 56(2)*, 267–283. doi:https://doi.org/10.1037/0022-3514.56.2.267

Chang, K.-C., Gao, Y.-K. & Lee, S.-C. (2020). The Effect of Data Theft on a Firm's Short-Term and Long-Term Market Value. Mathematics, 8, 808–829.

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

Chernyshev, M., Zeadally, S. & Baig, Z. (2019). Healthcare Data Breaches: Implications for Digital Forensic Readiness. *Journal of Medical Systems, 43(1)*, 1–12. doi:https://doi.org/10.1007/s10916-018-1123-2

Compas, B. E., Banez, G. A., Malcarne, V. & Worsham, N. (1991). Perceived Control and Coping with Stress: A Developmental Perspective. *Journal of Social Issues, 47(4)*, 23–34. doi:https://doi.org/10.1111/j.1540-4560.1991.tb01832.x

Coombs, W. T., & Holladay, S. J. (2002). Helping Crisis Managers Protect Reputational Assets: Initial Tests of the Situational Crisis Communication Theory. *Management Communication Quarterly, 16(2),* 165–186. doi: https://doi.org/10.1177/089331802237233

Cross, C., Parker, M. & Sansom, D. (2019). Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach. *International Review of Victimology, 25(1),* 53–69, doi:10.1177/0269758017752410.

Dion, J. H. & Smith, N. M. (2019). Consumer protection – Exploring private causes of action for victims of data breaches. *Western New England Law Review, 41(2),* 253–286. doi:https://digitalcommons.law.wne.edu/lawreview/vol41/iss2/2

Edwards, B., Hofmeyr, S. & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity, 2(1)*, 3–14. doi:10.1093/cybsec/tyw003

Endler, N. S., Speer, R. L., Johnson, J. M. & Flett, G. L. (2000). Controllability, coping, efficacy, and distress. *European Journal of Personality, 14(3)*, 245–264. doi:https://doi.org/10.1002/1099-0984(200005/06)14:3<245::AID-PER375>3.0.CO;2-G

Ferrick, B. (2018). No Harm, No Foul: The Fourth Circuit Struggles with the "Injury-in-Fact" Requirement to Article III Standing in Data Breach Class Actions. *Boston College Law Review, 59(9)*, 462–481.

Financial Times. (28.5.2010). Global 500 March 2010. Retreived from http://media.ft.com/cms/15951a1e-4899-11df-9a5d-00144feab49a.pdf

Fischhoff, B., Gonzalez, R. M., Lerner, J. S. & Small, D. A. (2005). Evolving Judgments of Terror Risks: Foresight, Hindsight, and Emotion. *Journal of Experimental Psychology: Applied, 11(2),* 124–139. doi:10.1037/1076-898X.11.2.124

Folkman, S. & Lazarus, R. S. (1980). An Analysis of Coping in a Middle-Aged Community Sample. *Journal of Health and Social Behavior, 21(3)*, 219–239.

Folkman, S. & Lazarus, R. S. (1985). If It Changes It Must Be a Process: Study of Emotion and Coping During Three Stages of a College Examination. *Journal of Personality and Social Psychology, 48(1)*, 150–170. doi:https://doi.org/10.1037/0022-3514.48.1.150

Folkman, S. & Lazarus, R. S. (1988). Coping as a Mediator of Emotion. *Journal of Personality and Social Psychology, 54*(3), 466–475. doi:https://doi.org/10.1037/0022-3514.54.3.466

Folkman, S., Lazarus, R. S., Dunkel-Schetter, C., DeLongis, A. & Gruen, R. J. (1986). Dynamics of a Stressful Encounter: Cognitive Appraisal, Coping, and Encounter Outcomes. *Journal of Personality and Social Psychology, 50(5)*, 992–1003.

Folkman, S., Lazarus, R. S., Gruen, R. J. & Delongis, A. (1986). Appraisal, Coping, Health Status, and Psychological Symptoms. *Journal of Personality and Social Psychology, 50(3)*, 571–579. doi:https://doi.org/10.1037/0022-3514.50.3.571

Garnefski, N., Kraaij, V. & Spinhoven, P. (2001). Negative life events, cognitive emotion regulation and emotional problems. *Personality and individual differences, 30(8)*, 1311–1327. doi:https://doi.org/10.1016/S0191-8869(00)00113-6

Gillham, B. (2000). *Research interview.* Continuum.

Gourlay, A., Mshana, G., Birdthistle, I., Bulugu, G., Zaba, B., & Urassa, M. (2014). Using vignettes in qualitative research to explore barriers and facilitating factors to the uptake of prevention of mother-to-child transmission services in rural tanzania: A critical analysis. *BMC Medical Research Methodology, 14*, 21. doi:http://dx.doi.org.ezproxy.jyu.fi/10.1186/1471-2288-14-21

Gwebu, K. L., Wang, J. & Wang, L. (2018). The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *Journal of Management Information Systems, 35(2),* 683–714.

Heikkilä, E. & Hevonoja, J. (21. 10. 2020). Useat tahot tutkivat psykoterapiakeskus Vastaamon tietomurtoa ja kiristystä – Kyberturvallisuuskeskus pitää tapausta poikkeuksellisena. *Yle*. Retrieved from https://yle.fi/uutiset/3-11605223

Hirschberger, G. (2018). Collective Trauma and the Social Construction of Meaning. *Frontiers in Psychology, 9*, 1–14. doi:https://doi.org/10.3389/fpsyg.2018.01441

Hirsjärvi, S. & Hurme, H. (2008). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö.* Gaudeamus, Helsinki University Press.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2016). *Tutki ja kirjoita* (21. ed.). Helsinki : Kustannusosakeyhtiö Tammi.

Hughes, R. (1998). Considering the Vignette Technique and its Application to a Study of Drug Injecting and HIV Risk and Safer Behaviour. *Sociology of Health & Illness, 20(3)*, 381–400. doi:https://doi.org/10.1111/1467-9566.00107

Janakiraman, R., Lim, J. H. & Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing, 82,* 85–105. doi:10.1509/jm.16.0124.

Kamoun, F., & Nicho, M. (2014). Human and Organizational Factors of Healthcare Data Breaches: The Swiss Cheese Model of Data Breach

Causation And Prevention. *International Journal of Healthcare Information Systems and Informatics, 9*, 42–60. doi:https://doi.org/10.4018/ijhisi.2014010103

Kayes, A., Hammoudeh, M., Badsha, S., Watters, P. A., Ng, A., Mohammed, F. & Islam, M. (2020). Responsibility Attribution Against Data Breaches. 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 498–503, doi:10.1109/ICIoT48696.2020.9089466.

Lazarus, R. S. (1991a). *Emotion and Adaption*. Oxford University Press, New York.

Lazarus, R. S. (1991b). Cognition and Motivation in Emotion. *American Psychologist, 46(4)*, 352–367. doi:10.1037/0003-066X.46.4.352

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping.* Spiringer, New York.

Liang, H., Xue, Y., Pinsonneault, A. & Wu, Y. (2019). What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective. *MIS Quarterly, 43(2)*, 373–394. doi:https://doi.org/10.25300/MISQ/2019/14360

Makridis, C. A. & Dean, B. (2018). Measuring the Economic Effects of Data Breaches on Firm Outcomes: Challenges and Opportunities. *Journal of economic and social measurement, 43*, 1–25.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing, 81*, 36–58.

Mikulincer, M. (1994). *Human Learned Helplessness: A Coping Perspective.* (C. R. Snyder, Ed.). The Plenum Series in Social/Clinical Psychology. Springer Science. doi:10.1007/978-1-4899-0936-7

Nach, H. & Lejeune, A. (2010). Coping with information technology challenges to identity: A theoretical framework. *Computers in Human Behavior, 26(4)*, 618–629. doi:https://doi.org/10.1016/j.chb.2009.12.015

Neame, R. (2012). Practical Measures for Keeping Health Information Private *Electronic Journal of Health Informatics, 7(2).*

Noor, M., Vollhardt, J. R., Mari, S. & Nadler, A. (2017). The social psychology of collective victimhood. *European Journal of Social Psychology, 47(2)*, 121–134. doi:https://doi.org/10.1002/ejsp.2300

Perlin, L. I. & Schooler, C. (1978). The Structure of Coping. *Journal of Health and Social Behavior, 19(1)*, 2–21.

Roseman, I. J., Antoniou, A. A., & Jose, P. E. (1996). Appraisal determinants of emotions: Constructing a more accurate and comprehensive theory. *Cognition and Emotion, 10(3),* 241–277. doi:https://doi.org/10.1080/026999396380240

Rousseau, D. (1989). Psychological and implied contracts in organizations. *Employee Responsibilities and Rights Journal, 2(2),* 121–139. doi:10.1007/BF01384942

Rustin, M. (2009). The Missing Dimension: Emotions in the Social Sciences. In: Sclater, S. D., Jones, D. W., Price, H., Yates, C. (eds), *Emotion* (p. 19–35). Palgrave Macmillan, London. doi:https://doi.org/10.1057/9780230245136_2

Ruusuvuori, J. & Nikander, P. (2017). Haastatteluaineiston litterointi. In : Hyvärinen, M., Nikander, P. & Ruusuvuori, J. (eds), *Tutkimushaastattelun käsikirja* (p. 427–444). Vastapaino, Tampere.

Salo, M., Makkonen, M. & Hekkala, R. (2020). The Interplay of IT Users' Coping Strategies : Uncovering Momentary Emotional Load, Routes, and Sequences. *MIS Quarterly, 44 (3)*, 1143–1175. doi:10.25300/MISQ/2020/15610

Scherer, K. R. (1982). Emotion as a process: Function, origin and regulation. *Social Science Information, 21(4-5)*, 555–570. doi:https://doi.org/10.1177/053901882021004004

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare, 8(2),* 133. doi:https://doi.org/10.3390/healthcare8020133

Sen, R. & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems, 32(2),* 314-341. doi:10.1080/07421222.2015.1063315.

Smith, C. A. & Ellsworth, P. C. (1985). Patterns of Cognitive Appraisal in Emotion. *Journal of Personality and Social Psychology, 48(4)*, 813–838. doi:https://doi.org/10.1037/0022-3514.48.4.813

Smith, C. A. & Lazarus, R. S. (1990). Emotion and Adaptation. In L. A. Pervin (Ed.). *Handbook of Personality: Theory and Research* (p. 609–607). New York: Guilford.

Solove, D. J. & Citron, D. K. (2018). Risk and Anxiety: A Theory of Data-Breach Harms. *Texas Law Review, 96,* 737–786.

Statista Research Department. (1.12.2020). The 100 largest companies in the world by market capitalization in 2020. Retreived from https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/

Thoits, P. (1995). Stress, coping, and social support processes: Where are we? What next? *Journal of Health and Social Behavior, Extra Issue,* 53–79.

Tietosuojavaltuutetun toimisto. (n. a.) Personal data breaches. Retrieved from https://tietosuoja.fi/en/personal-data-breaches

Trendmicro. (2015). Follow the Data: Dissecting Data Breaches and Debunking Myths. Retreived from https://www.trendmicro.nl/media/wp/dissecting-data-breaches-wp-en.pdf

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi* (Rev. ed.). Kustannusosakeyhtiö Tammi.

Valentiner, D. P., Holahan, C. J. & Moos, R. H. (1994). Social Support, Appraisals of Event Controllability, and Coping: An Integrative Model. *Journal of Personality and Social Psychology, 66(6)*, 1094–1102. doi:https://doi.org/10.1037/0022-3514.66.6.1094

Wang, S. & Huff, L. C. (2007). Explaining buyers' responses to sellers' violation of trust. *European Journal of Marketing, 41(9/10)*, 1033–1052. doi:doi:https://doi.org/10.1108/03090560710773336

Yih, J., Kirby, L. D., Spitzer, E. G., & Smith, C. A. (2020). Emotion as a process: Appraisal, emotion, and coping patterns across time. *Motivation Science, 6(3),* 221–234. doi:https://doi.org/10.1037/mot0000144

APPENDIX 1 TRANSLATED VIGNETTE

11.5.2021 10.14 Updated 11.5.2021 10.31

Healthcare data breach: This is what is known

Healthcare Facility Halla notifies of a data breach in patient information system, thousands of patients' information compromised

This morning, Healthcare Facility Halla, which provides private healthcare services, announced a data breach on its patient information systems, in which the confidentiality of the health information of thousands of patients has been compromised. It is not yet known how extensive the data breach has been, or how long the breach has lasted. The security of Halla's information systems is being tested in an internal investigation and patient operations continue as normal.

Halla's representative has refused to comment on the case, citing co-operation with the authorities.

In accordance with the Data Protection Act, the individual victims of the breach will be informed in the coming days.

Subject: URGENT: Patient data breach in Healthcare Facility Halla
11.5.2021 11.03
Sender: customerservice@terveyslaitoshalla.fi
Recipient: You

Dear customer,

Healthcare Facility Halla's patient information system has been subjected a data breach, as a result of which your health information has been stolen from Halla's information systems. We do not yet know the full contents of the stolen health information, but the confidentiality of your personal information and health information has been compromised.

We apologize for the situation,
Healthcare Facility Halla