Ethical and organizational learning from data breaches and their impact on employees' behaviors

ABDULHALIM ALHASSAN

SUPERVISOR

Jaziar Radianti

University of Agder, 2022
Faculty of Engineering and Science
Department of ICT and Information Studies

Preface

This master thesis was conducted and written by one student enrolled in the Cybersecurity master’s program at the University of Agder. The thesis was written over the duration of two semesters, as a contribution for the master’s degree assignment. The thesis was conducted in the period between January 2022 and December 2022. The purpose of this study is to investigate how organizations learn from data breaches, what ethics can be added, and how these can affect their employees' behavior.

I would like to express my gratitude to my supervisor, Jaziar Radianti, for her guidance and support during my master's thesis at the University of Agder. She was able to respond quickly to my questions and provide me with feedback. Also, I would like to thank Dr. Marko Niemimaa for his assistance in the literature review and Dr. Nabil Abdoun for his valuable advice online.

I want to also thank the individuals who agreed to be interviewed for my study. They took the time out of their busy schedules to help me finish my research.

Kristiansand

30th of November 2022

Abdulhalim Alhassan

Abstract

Data breaches have become more prevalent in recent years. Despite the obligation to disclose these breaches, many organizations fail to implement effective disaster recovery and public relations strategies following these incidents. Organizational learning is important to avoid the same breaches to reoccur in the future. Through organizational learning, an organization can improve itself by acquiring new knowledge and using that knowledge to improve its performance. The resulting knowledge is then transferred to the members of the organization.

Multiple organizations in Norway and all over the world have been prone to cyber-attacks. The attackers are targeting small, large, and political organizations. Many of these incidents have ended with a huge amount of data breaches.

In this thesis, I aim to find answers to the questions existing in the problem statement by expanding and deepening the search using qualitative research methods. Also, I will try to study this topic phenomenon by raising the ethical and organizational learning of data breaches and studying the behavior of employees before, during, and after breaches aiming to find good answers that could benefit other organizations in the future. However, it’s essential to understand why, and how data breaches have occurred.

Terms & Abbreviations

ACL: Access Control List

CAGR: Compound annual growth rate

GDPR: General Data Protection Regulation

IR: Incident Response

IRT: Incident Response Team

ISM: Information Security Management

ISMS: Information Security Management System

ISO standards: International Organization for Standardization

NCSC: Nasjonalt Cybersikkerhetssenter “National Cyber Security Center”

NIST framework: National Institute of Standards and Technology

NSD: Norsk senter for forskningsdata “Norwegian center for research data”

NSM: Nasjonal sikkerhetsmyndighet “The Norwegian National Security Authority”

SaaS: Data protection platform

SISO: Senior Information Security Officer

SMB: Small and medium size businesses

SOC: Security Operation Center

VA: Vann og avløp “water and sewage”

Table of contents

List of Figures

List of Tables

Chapter 1

Introduction

Nowadays, the critical missions of many businesses have relied on digital platforms to a large degree. Most companies store their data digitally and have digitalized various aspects and work processes of the business's operations. This has triggered a digital transformation in many organizations (Demlehner et al., 2020). This digital transformation has a number of advantages, such as increased productivity, and innovation. However, it has also opened the door for actors who have malicious intentions to attack businesses that have weak cyber-security measures, targeting their valuable assets residing in cyberspace, and causing data breaches in many cases. The Identity Theft Resource Center defined data breach as:
“Data removed by malicious action or error from the database or system where it was created, collected, processed, or maintained. Besides, it is an unauthorized transfer of information from an information system.” (Carter, 2021)

As several organizations are experiencing data breaches, the size of the cyber-security market is growing by around 10.9% CAGR worldwide. According to the ultimate list of cyber-security statistics, the pandemic in 2020 caused a significant increase in cybercrime and phishing. The healthcare industry is the costliest sector for data breaches, with losses estimated to be around $ 7.18 million in 2020. Around 95% of these cyber-security breaches are a result of human errors (Carter, 2021) However, Greig et al., (2015) point out that the focus on employees’ behavior is vital since an “organization’s success or failure effectively depends on the things that its employees do or fail to do” (Da Veiga and Eloff, 2010). Security culture has the potential to play a significant role in this respect (Vroom and Von Solms, 2004).

Since data breaches have been more prevalent nowadays, the rise of the need for cyber-security almost occurs everywhere and is an integral part of most modern organizations (Sen, 2018). However, many pieces of research study risks and resolutions of data breaches focusing on how organizations manage these incidents that occur more often. This highlights the importance of addressing both risks and resolutions in different forms Kent, D. (2021, October 5). Moreover, several studies have already discussed similar issues without addressing ethical and organizational learning, especially after crisis management that is made as a consequence of data breaches.

So, It is important to address this kind of learning from data breaches or in other words learning from digital failure. Firms are known to respond to this failure learning by introducing new organizational routines, incorporating additional safety procedures and protocols (Haunschild et al. 2015, Clay-Williams and Colligan 2015), acquiring infrastructure (Desai 2011), and establishing new organizational units (Rathert, C., & May, D. R. 2007). Ironically, pressures to appease stakeholders and competition for resources that redirect firms' investments and managerial efforts toward profitability over safety priorities can hinder failure learning (Haunschild et al. 2015, Dahlin et al. 2018, Gaba and Greve 2019). Consequently, organizational responses may prove ineffective, leading to repeated failures (Bennett and Snyder 2017).

1.1 Motivation and background

A data breach within an organization can be the entry point for attackers to establish a foothold in the cyber-environment of an organization. The impact of breaches varies, but according to the proof-point report, nearly 60% of organizations lose data, and 35% experience financial loss. The average cost of an organizational breach is $3.86 million according to IBM's Cost of Data Breach Report of 2020 (IBM, 2020). This number varies depending on the size of the organization, but it paints a picture of how costly a data breach can be.

In addition, I was involved in a previous course project where we conducted an interview with a public organization which had actually experienced a cyber-attack and data breaches. The interview focused on different areas including how hacking and data breaches occurred. Therefore, I am motivated to explore the topic further and how we can learn from this evidence. In this thesis, I extend the security breach cases by adding more cases.

Many organizations in Norway and all over the world have experienced data breaches. These incidents have raised various concerns regarding the management of data security. This issue has highlighted the need for organizations to adopt ethical and organizational changes. My goal is to study the various factors that affected the management of data security of these organizations, how they could improve their systems, policies, strategies, and methods, which criteria they follow to implement these changes, what the employees learned from these events to change their behavior regarding data security, and how this can be beneficial for other organizations.

1.2 Problem statement and Research Questions

In view of the vast widespread of cyberattacks and data breaches, it is important for organizations to learn from their failure to protect data. However, most businesses enhance protection systems after data breaches. This is one of the major concerns that will be addressed in this report. Thus, the following research questions are formulated:

Q1. How have the behaviors of the employees changed after the data breaches?
Q2. How are ethics incorporated into the organization after the data breaches?
Q3. In what way organizational learning from data breaches improves the organizational security procedure?

1.3 Scope

Organizational learning is wide fieldwork for research. My topic focuses specifically on ethical and organizational learning from data breaches. Therefore, the other kinds of ethical and organizational learning that are outside of data breach events are not included in my scope of research. Thus, my topic addresses after-data-breaches learning and the change of organizational procedures (processes), privacy ethics, and behaviors.

1.4 Thesis Structure

The thesis is organized to be seven chapters. In Chapter 1, I explain the motivation of this study and the research questions. In Chapter 2, literature reviews and related studies are presented and synthesized. It focuses on studies that are related to data breach incidents, ethics and framework. In Chapter 3, I present the Research Method employed in this study. Chapter 4 summarizes the cases that have been included in this thesis.

In Chapter 5, all results from the data collection are presented, also the case studies used in this study. Chapter 6 is dedicated to the discussion of the results also the limitations of this master thesis. Chapter 7 contains the concluding remarks and lessons learned from this study.

Chapter 2

Literature Review

In this chapter, I first present a general overview of data breach incidents existing in the literature reviews. Then, I summarize the main existing cyber-security ethical framework. And finally, I present the impact of data breach on employees' behavior. The aim is to give an overview of the topic and to present the defined concepts of the study. This chapter will also go through how the literature review has been conducted and the methodology that has been used to find literature for this master thesis. This includes what type of criteria were used, what type of databases were used to conduct searches, why the different databases were chosen and how the literature was selected.

2.1 Search and Selection of Literature

It is very important to find reputable and high-quality literature when conducting research and writing reports. It is critical to determine whether the research problem is intriguing, relevant, and worth investigating. This section examines the methods utilized for collecting the literature and the selection criteria that were applied (Evans, 2002).

2.2 Database Selection

Finding the suitable databases to search in was a crucial stage in the systematic literature review. It's crucial to choose a database that is dependable, trustworthy, and pertinent to our area of research. Additionally, the database needs to allow users to apply sophisticated search criteria, such as date range, keywords, journal's possibility of searching, and language filters, among others.

When conducting a literature search, Scopus, AIS Electronic Library, and Web of Science have historically produced positive results while also being organized and simple to use. Relevance of articles for the chosen keywords as well as a neat result page following a search were two significant priorities in this literature search. These three search engines mentioned above provided the option to search by titles and keywords, making it easier to identify relevant content without receiving an overwhelming amount of irrelevant results. This sped up and improved the selection of literature. Additionally, they are freely accessible via the network of the University of Agder, allowing us to do searches from our homes using the university's VPN service. In the end, these databases were chosen because of their prior familiarity, effectiveness, orderly operations, and propensity for producing accurate search results.

2.3 Basic search

Without any specific inclusion or exclusion criteria, the basic search was conducted as an open search, producing a vast number of results that were difficult to sort through. This was an anticipated outcome and was done as a benchmark for comparison with a more thorough search that considered the established inclusion and exclusion criteria. If only a few articles are found in the results of a simple search, there may be few articles to be found in the results of an advanced search. The table below displays the outcomes of the basic search.

Table 1: Database search results

	Databases		
Keywords	*Scopus*	*Web of Science*	*Association for Information Systems (AIS)*
Data breaches	10,852	116	2866
Organizational learning	107,604	274	22610
Ethical framework	12,460	143	5687
Employees behavior	12,021	3,532	13843

2.4 Inclusion criteria

It was obvious from the prior search, which had without inclusion or exclusion criteria, that the search needed to be more focused and limited. As a result, the inclusion and exclusion criteria that were applied to provide a better search result are presented in this section.

The following inclusion criteria were selected for the database search:

- All literature must date from 2012 or later according to the date requirement.
- All literature must be written in either English or Norwegian, according to the language requirement.
- Unless it is a fresh publication, the literature should be cited by other researchers to demonstrate its validity.
- Only articles pertinent to our area of research will be selected based on the relevance criterion.

The date criteria were used to help focus the search and guarantee that all the literature was still relevant when it was identified. A ten-year time frame was used for all searches. This was done to acquire current results and only show articles from recent enough times. Ten years would produce data that were both time-relevant and could be compared to more recent studies to identify any advancements.

The language requirements were established since the majority of the articles returned by the original search were written in English and because the language used had to be one, we could understand.

The purpose of the citation requirements is to assist guarantee that the articles found are of high caliber. The only time this criterion is exempt is if the article is relatively recent. If the article appears to be relevant and meets all of the other criteria, this criterion might be disregarded.

To make sure that the papers were related to and relevant to my field of research, the relevance criteria, the final criterion, was established. In order to improve the relevancy of the articles in the search results, this was accomplished by categorizing the articles that the databases gave after a search.

2.5 Advanced Search

The advanced search of the literature review was carried out once the primary keywords and parameters for the literature search were established. The sophisticated search involved combining numerous terms with the previously mentioned requirements. The purpose of the advanced search was to maintain the relevant literature and make it simpler to find it while removing unnecessary and undesired results. There were much fewer articles in the advanced search than in the simple search. The basic search returned thousands of useless results when searching for each of the specific keywords utilized, which were unrelated to this master's thesis. More relevant results were returned by combining keywords.

Table 2: Advanced search

Search Word	*Scopus*	*Web of Science*	*Association for Information Systems (AIS)*
Data breaches + Organizational learning	78	12	5
Data breaches + Ethical framework	16	9	5
Data breaches + Employees behavior	89	14	8
Organizational learning + Ethical framework	17	5	6

Organizational learning + Employees behavior	101	9	18
Ethical framework + Employees behavior	1	5	8

2.6 Practical Screening

Several measures were used during the practical screening to further filter the results, weed out irrelevant literature, and ensure that the articles were relevant. The irrelevant articles that have not already been eliminated by the inclusion criteria must go through this step in order to be excluded.
The following were the exclusion criteria that were created:

- Duplicate articles are those that have been gathered twice or more from several databases.
- Articles with titles that seem irrelevant should be avoided.
- Articles with irrelevant abstracts are those whose abstracts seem unrelated.
- Content that seems unimportant after reading it is referred to as irrelevant content.

There were 406 articles found overall thanks to the advanced search. Thirty of these articles were duplicates, thus they were all deleted. Then, after reading and skimming all of these articles' titles, 76 articles struck out as being very relevant and intriguing based only on their names. Another 205 papers were discarded from consideration after reading the abstracts of those that were already included. In the end, the remaining articles' contents were studied to gain a general grasp of the issues they were attempting to address and to gain insight into their substance.
55 further articles were removed as a result of this. A method known as "reverse snowballing" was employed as the final step in the practical screening procedure. Backward snowballing is a strategy that involves searching through a paper's reference list to find other works that might be related (Jalali, 2012). Five additional articles were added to the collection of articles after the snowballing technique was applied to the most relevant articles already discovered. The example of the practical screening is shown below.

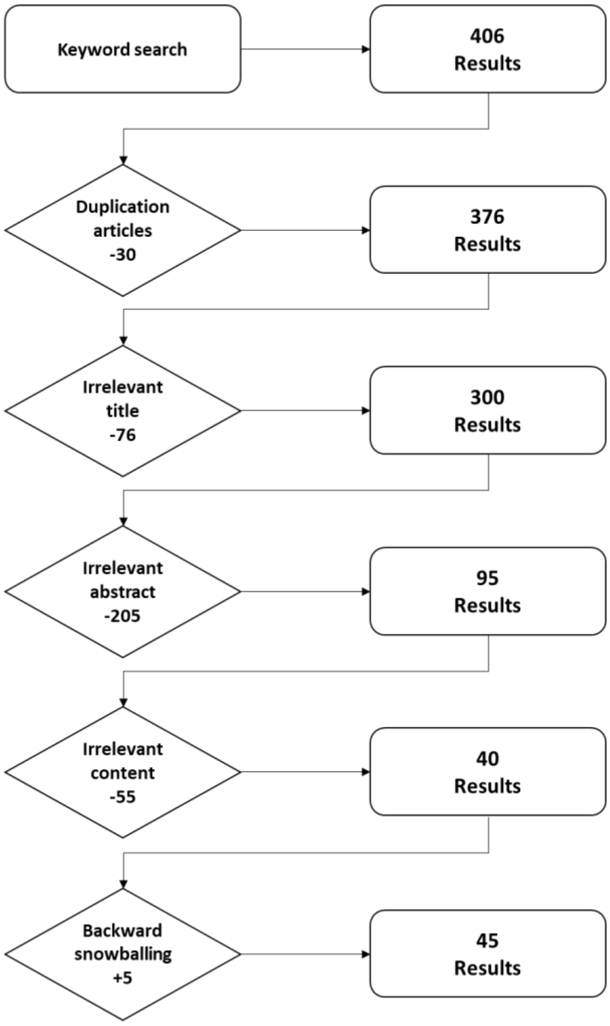


Figure 1: Practical Screening

2.7 Literature Review Findings

It is crucial to make note of the foundational elements that earlier studies in the subject used while analyzing the findings from the literature review. As a result, this section of the thesis will examine intriguing findings and make an effort to pinpoint recurring themes in the relevant literature. Later, these themes and findings can be used to develop an interview guide and find additional relevant data for this thesis.

2.7.1 Concept Matrix

To methodically organize and extract information from earlier research into subjects and themes, a concept matrix was created. A concept matrix is a tool that helps with demonstrating relationships between ideas and themes in the related literature (Davis, 2021). An organizational structure is necessary when gathering data from earlier research and reports in order to identify what information is crucial for the underlying investigation and what subjects' earlier studies cover.

After seeing that there were recurring themes and subjects in the pertinent literature, the following topics were selected:

Table 3: Description of topics in the Concept Matrix

Topics	Description
Data breaches	Incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner
Organizational learning	process by which an organization improves itself over time through gaining experience and using that experience to create knowledge
Framework	generic term commonly referring to an essential supporting structure which other things are built on top of
Cybersecurity ethics	Because cybersecurity is a form of risk management, and because those risks significantly impact other parties, there is a default ethical duty to disclose those risks when known, so that those affected can make informed decisions
Employees behavior	Refers to the behavior of employees at workplace
Organizational Structure	Includes a need for change in organizational structure to improve cybersecurity, includes problems with the existing organizational structure, includes changes to the organizational structure for a positive or negative results for cybersecurity

It was simpler to determine which articles touched on the relevant themes and issues by building a concept matrix with those topics and themes. This provided us with a summary of relevant articles. The 45 papers from the practical screening were initially included in a concept matrix that we constructed, but after further investigating this literature, we discovered that 27 of the articles were not related to our thesis and had to be dropped. Therefore, only the relevant articles were included in the concept matrix.

In order to set the stage for our empirical study and serve as a foundation for conducting and evaluating it against our own findings, a review of prior research literature was done. To compare against our findings, these articles' summaries have been prepared and categorized into three themes: “Data Breach Incidents”, “Cyber-security Ethical Framework”, and “The Impact of Data Breach on Employees’ Behavior”. The conclusions from these articles will eventually be compared to the information and conclusions that are offered in chapter 5.

2.7.2 Data Breach Incidents

There are two main categories of data breaches: intentional and unintentional. An intentional data breach is a type of attack that occurs when a hacker or other threat actors deliberately launch attacks and expose sensitive information to cause harm. An unintentional data breach is an incident without malicious intentions and happens due to human error or processes that are not designed to prevent exploitation (IBM, 2020). The definition and causes of these two categories of data breaches are shown in Table 4.

Table 4: Intentional and unintentional data breaches

Category	*Definition*	*Causes*
Intentional Data Breach	A type of attack that occurs when a hacker or other threat actors deliberately expose sensitive information to cause harm	1. Hackers 2. Malicious insiders 3. State-sponsored actors 4. Terrorists
Unintentional Data Breach	An incident without malicious intentions happens due to human error or processes that are not designed to prevent exploitation	1. Insecure user behavior 2. Loss or re-use of media devices 3. Flawed software 4. Unauthorized disclosure 5. Unauthorized software

In his research, Kongnso (Kongnso, 2015) realized a qualitative multicase study to explore the best practices that can be used by technology leaders to minimize data security breaches for increased business performance. In his work, the researcher selected two cases:

- A banking firm in the North central United States
- A local government agency in the South central United States

After doing the interviews, collecting, and triangulating data, Kongnso answered the main research question of his study: What best practices do technology leaders use to minimize data security breaches for increased business performance?

Based on the obtained results, the author concluded that four themes illustrate the best practices leaders should use to minimize data security breaches for increased business performance:

a. Security awareness
b. Security policies
c. Organization culture
d. Technology and innovation trends

The findings of this research highlighted the importance of technology leadership for technology integration and security awareness initiatives. Also, the obtained results pointed to the necessity to incorporate various business activities in security training programs illustrating the exact nature of data breaches. Furthermore, the author insisted in his work that leaders should become proactive by integrating the industry best practices within the organizations' processes, as well as aligning these best practices with the organizational culture, mission, vision, and objectives. In addition, technology leaders should ensure that their employees are always up to date following the current technology and security trends, as well as knowing the latest vulnerabilities and threats. Despite the focus on proactive policing strategies, the study of Kongnso has several limitations: First, the findings are limited to leaders' best practices. Second, the work targeted a very small sample size which might limit the ability to generalize the research results later.

In their paper, Dileep with other researchers (Dileep et al., 2020) concluded also that employees are the main reason for most data breaches. In fact, their non-compliance with security regulations, policies and guidelines governed by the organization is an essential vulnerability leading to different kinds of attacks including spyware, viruses, and worms.

In a research paper written by Kwon and Johnson (Kwon et al., 2011) presented an empirical analysis of security investment in the healthcare sector to explore the impact of learning effects on breach performance. The researchers seek to identify how different types of security investment affect subsequent security failures by employing organizational learning theory (Kamoun et al. 2014). Using a Cox proportional hazard model for survival analysis, they found that proactive security investments are associated with longer intervals before subsequent breaches than reactive investments. Further, they found that external regulatory pressure can stimulate organizational learning and change (Brown et al. 1991).

The obtained results indicate that proactive investments are more effective at reducing security failures than reactive investments. However, when proactive investments are forced by an external requirement, the effect of proactive investment is diminished. This implies that voluntary, proactive investments have the best performance.

However, they found that an organization might learn more from education or internal policies to prevent insider threats than from implementing technical controls.

In terms of the social effects of organizational learning, the obtained results show that learning by doing through proactive security investments relieves economic incentives, whereas unilaterally mandated procedures do not have any economic incentive (ENISA 2017). The researchers suggested that security managers and policymakers should pay attention to the strategic and regulatory factors influencing security investment decisions.

Despite the focus on learning by doing through proactive security investments, the study of Kwon, and Johnson has several limitations: First, they considered only the investments in IT security controls and did not address the issue of policies and training programs. While implementing controls such as training would have a direct learning effect, their study was more focused on indirect learning effects through learning by doing or learning by using IT security controls (Sat et al. 2020). Second, their model measured security investments as the number of IT security controls, and not the momentary amount of security investment.

In a study done by Buckman et al. (Buckman et al. 2017), they investigate the duration between a data breach occurring within an organization and subsequent data breaches happening at the same organization given different factors such as the organization structure, the relevant law, and the data breach characteristics. Indeed, the authors analyzed the duration using a hazard model. The obtained results from the hazard model provide that the duration between two consecutive data breaches that happened at an organization increases when the breach type of the prior data breach was one of the following types:

a. Unintended disclosure of information
b. A system hack
c. The mishandling of paper records
d. The mishandling of a portable device

The researchers also noted that the duration between two consecutive data breaches increases when the organization is an educational institution, a non-retail business, or a medical organization.

Despite the use of a hazard model, the study of Buckman et al. (2017) has an essential limitation: the collected data set is limited to those organizations who reported a data breach, but they were unable to verify truthfulness in the organization's disclosure reporting.

On the other side, Samantha Mello (2018) conducted research to explore data breaches in higher education institutions and to identify various factors that lead to these data breaches. He pointed out that universities with higher student enrolment are more likely to be breached because they contain personal data and sensitive information about a larger number of students and employees. Also, he found that universities with high financial positions are more likely to be breached due to the higher financial gain to a person with access to breached data. Also, he found that universities with tighter data protection policies are less likely to be breached because they have more control over student and faculty records.

In another study conducted by Yaraghi (2016), he examined recent privacy breaches in the healthcare industry, uncover the underlying factors leading to these incidents, document the lessons learned, and examine how similar breaches can be prevented moving forward. In his research, he concluded that the lessons learned from the breaches can be grouped into two categories based on those that eliminate or reduce:

a. The probability of a breach incident
b. The consequences of a breach after it has happened

After analyzing the results and documenting the lessons learned, the researchers provided some recommendations to healthcare organizations. These recommendations include, but are not limited to:

a. Prioritize patient privacy and use available resources to protect it
b. Better communicate with each other
c. Embrace cyber insurance
d. Better communicate the details of breach incident audits
e. Establish a universal Health Insurance Portability and Accountability Act (HIPAA) certification system

In a recent article written by Ahmad et al. (2020), they concluded that most large existing organizations invest in a dedicated information security management (ISM) function to ensure that their digital assets are very well protected. Indeed, the ISM function conducts several processes, such as

a. Risk assessments
b. Strategy development
c. Policies and training to define roles and guide behavior,
d. Technological controls implementation such as firewalls, anti-virus, etc.
e. Encryption method implementation to restrict unauthorized access

Despite these security countermeasures proposed by Ahmad et al., incidents like data breaches will occur. Alongside the security management function, they found that many organizations also retain an incident response (IR) function to mitigate damage from an attack and promptly restore digital services. However, they also found that few organizations integrate and learn from experiences of these functions in an optimal manner.

In their paper, the researchers draw on organizational learning theory to develop a conceptual framework that explains how the ISM and IR functions can be better integrated. From their point of view, the strong integration of ISM and IR functions, in turn, creates learning opportunities that lead to organizational security benefits including:

a. Increased awareness of security risks
b. Compilation of threat intelligence
c. Removal of flaws in security defenses
d. Evaluation of security defensive logic
e. Enhanced security response

In another study by Wileen Barosy (2019), he conducted research focusing on what operational strategies the chief information security officer (CISO) of high-technology companies use to protect their businesses from cyberattacks. In his research, he asked three cyber-security business leaders a series of questions on strategies to prevent cyberattacks. During the data analysis process, he identified four main themes:

a. Effective leadership: Leadership in the organization was the first factor that participants stressed as important in engaging cybersecurity professionals in their leadership teams.
b. Cyber-security awareness: Cyber-security awareness makes people aware of their responsibilities and roles in information technology.

c. Reliance on third-party vendors: The usage of cyber-security policy and the business leaders’ documents provide details on defending organizations and their assets.
d. Cyber-security training: This training established a cross-training on various product lines and career expansion for the talented remaining employees.

He found the more the business relies on technology to collect data, store, or manage information, the more vulnerable the business becomes too severe security breaches. Also, he concluded that human errors, hacker attacks, and system malfunctions could cost the business financial damage and can jeopardize the business's reputation.

In another study, Hagen et al., (2009) found that the effects of the intervention on security awareness and behavior partly remains more than half a year after the intervention, but that the detailed knowledge of information security issues diminished during the period. The study also discusses how such courseware can contribute to long-term organizational learning compared with human interventions such as action research (Hagen et al., 2011) . Both human resource management and internal promotion are necessary inputs in the process to successfully educate and train employees in information security (Argote et al. 2011).

In another qualitative study, Culnan and Williams (2009) concluded that protecting the privacy of personal information continues to pose significant challenges for organizations. Because consumers are vulnerable in their dealings with businesses due to a lack of information about and an inability to control the subsequent use of their personal information. Also, they argued that organizations have a moral responsibility to these individuals to avoid causing harm and to take reasonable precautions toward that end.

The researchers further argue that firms can enhance their privacy programs by moving beyond merely complying with laws and other regulations and creating a culture of integrity that combines a concern for the law with an emphasis on managerial responsibility for the firm's organizational privacy behaviors. They use two high-profile data breaches experienced by two U.S. companies, ChoicePoint and TJX, to illustrate their arguments for enhancing organizational-level privacy programs based on ethical reasoning. In fact, their paper contributes to the dearth of prior organizational-level privacy research, which has largely overlooked ethical issues, or the personal harms often caused by privacy violations.

They concluded with recommendations for ways organizations can improve their privacy programs by incorporating moral responsibility. It means that a robust governance program embedded within a culture of moral responsibility should, in their opinion, provide a more effective approach to managing privacy because integrity is integrated into the organization's culture (Mattia 2011).

From the literature reviewed with respect to the organizational learning after the breaches, there are similarities or overlapped themes on the learning points after the security breaches (Dhillon 2015), that can be summarized as follows:

Table 5: Synthesize of organization learning after data breaches from literature

Dimensions	Example of concrete learning
Security awareness and training	The need to understand the probability of breaches, the need to understand the consequences (Yaraghi, 2016; Barosy, 2019), Security training (Kongnso, 2015; Ahmad et al., 2020; Barosy, 2019), encourage compliance behavior (Dileep et al., 2020) security behavior (Hagen et al, 2009)
Security policies	Enhance organizational privacy program and data protection (Culnan and Williams, 2016; Mello, 2018), regulatory aspects (Dileep et al., 2020); Prioritization in data protection, cyber insurance, privacy certification (Yaraghi, 2016), enhanced policy and risk assessment, evaluation on defense logic, enhanced security response (Ahmad et al., 2020); Third party policy (Barosy, 2019)
Organization culture and organizational aspects	Improved vision, mission, and objective; improved leadership in technology and efficient leadership (Kongnso, 2015; Barosy, 2019); better communication in the organization (Yaraghi, 2016).
Technology and innovation trends	Proactive security investment (Dileep et al., 2020); technology control such as firewall and antivirus, encryption (Ahmed et al., 2020)
Underreporting event	Underreporting prevents actual learning from security breaches and needs improvement (Buckman, 2017)

One of the research gaps mentioned in the literature is the fact that the ethical aspects of security breaches often are overlooked, and cyberattacks will have an impact on the privacy breaches and violations (Culnan and Williams, 2016). And we noticed from Table 4, most solutions are either technical or organizational in terms of compliance, policy or organizational structure improvements.

In the next subsection, the different cyber-security ethical frameworks are presented.

2.7.3 Cyber-security Ethical Framework

This subsection presents several cyber-security ethical frameworks in the literature that are useful for analyzing different ethical questions related to this field. It begins with the two main frameworks that are very important in practice:

- Principlist framework
- Rights-based principle that is influential in the law

The figure below represents the various cyber-security ethical frameworks existing in the literature.

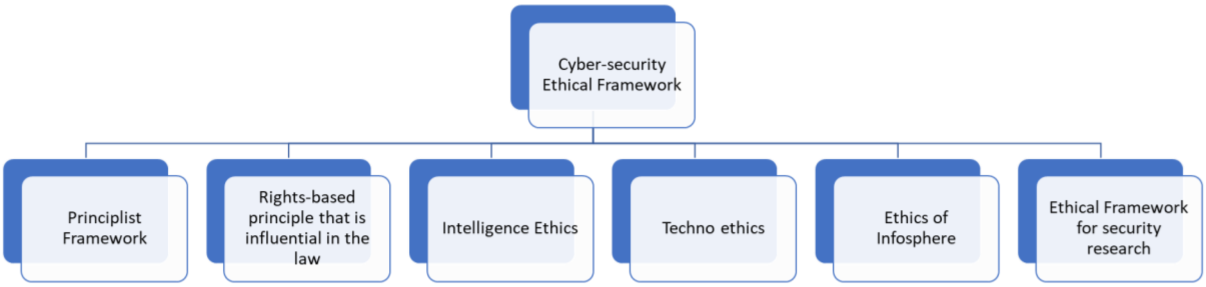

Cyber-security Ethical Framework
Principlist Framework
Rights-based principle that is influential in the law
Intelligence Ethics
Techno ethics
Ethics of Infosphere
Ethical Framework for security research

Figure 2: Various cyber-security ethical frameworks existing in the literature

Since the benefits and harms caused by cyber-security policies and operations are of a probabilistic nature, It is argued that all the cyber-security ethical frameworks should deal with probability and risk (Manjikian 2017). The benefit principle applies in all generality to cyber-security research; it should be understood as the principle of minimizing probable harm (requires considering the full spectrum of risks to persons, including, emotional, physical, reputational, and financial harm) and maximizing probable benefit (Kenneally et al. 2010; Kenneally and Bailey 2013).

The Principlist Framework

The Principlist is an approach of ethics based usually on 3 or 4 principles (limited number of principles) with a grounding in professional ethical practice and common-sense morality. The Principlist is a moderate approach, and a minimalist framework that affords significant flexibility. It leaves to the cyber-security operatives, or the researchers the difficult task of identifying the specific factors and circumstances that should carry weight in deliberations concerning a concrete case. Also, it leaves to the stakeholders the more difficult task of weighing these considerations against each other when trade-offs occur (Wang 2021).

The table below summarizes the existing Principlist frameworks in the literature.

Table 6: Summary of principlist frameworks for cybersecurity ethics

References	Ethical Principles
The Menlo Report (2012)	1) respect for persons, 2) beneficence, and 3) justice
British Academy & Royal Society (2017)	1) Independence, 2) Deep Connection to Diverse Communities, 3) Cross-Discipline Subject Matter Expertise, 4) Closeness to Decision-Making Processes, 5) Durability & Transparency, and 6) Nationally-Focused but Globally-Relevant
Van de Poel (2020)	1) security, 2) privacy, 3) fairness, and 4) accountability
Weber and Kleine (2020)	1) efficiency and quality of service, 2) privacy of information and confidentiality of communication, 3) usability of services, and 4) safety

Loi and Christen (2020)	1) privacy, 2) data protection, 3) non-discrimination, 4) due process and free speech, and 5) physical integrity
Floridi et al. (2020)	1) Falsifiability & Incremental Deployment, 2) Safeguards Against Manipulation, 3) Contextualized Intervention, 4) Contextualized Explanation & Transparency, 5) Privacy Protection & Data Subject Consent, 6) Situational Fairness, and 7) Human friendliness
Morgan and Gordijn (2020)	1) privacy, 2) protection of data, 3) trust, 4) control, 5) accountability, 6) confidentiality, 7) responsibility on business to use ethical codes of conduct, 8) data integrity, 9) consent, 10) transparency, 11) availability, 12) accountability, 13) autonomy, 14) ownership, and 15) usability.
Formosa et al. (2021)	1) Beneficence, 2) Non-maleficence, 3) Autonomy 4) Justice, and 5) Explicability

The rights-based principle that is influential in the law

The second cyber-security ethical framework that is important in practice is the rights-based principle that is influential in the law, in particular the EU law (Christen et al. 2020).

The cyber-security technologies used to protect the individuals from cybercrime may conflict with human rights. Indeed, cybercrime may be defined to include four different wide categories of crime (Brey 2007):

1. Cybertrespass: gaining unauthorized access to data and information systems.
2. Cybervandalism: disrupting processes and corrupting data.
3. Cyberpiracy: reproducing and distributing software or content which violates intellectual property.
4. Computer fraud: misrepresentation of identity or information for the sake of deception for personal gain.

On the other side, what are the rights that need to be balanced with cyber-security? According to Hildebrandt (Hildebrandt, 2013), those rights are:

1. Privacy
2. data protection
3. non-discrimination
4. due process and free speech

From the perspective of a human rights principle, these rights can be seen as a way to balance (in the sense of ‘checks and balances’) the heightened risk to privacy and informational self-determination of all other persons that the data in the infected computers may identify.

Intelligence Ethics

Ross Bellaby (Bellaby, 2012) identified and discussed in his research the two main points concerned the ethics in the domain of cyber-security:

1. The need for an ethical framework
2. The dilemma in the intelligence community

He argued that the right cyber-security ethical framework can reconcile some of the tensions between autonomy and violating people's privacy. Also, he explained that the intended framework should justify the various acts carried out through a 'just war doctrine' (Miller et al., 2021). Ross Bellaby also discussed the different advantages for designing, developing and implementing a normative framework named 'just intelligence' which defines the principles intended to guide ethical intelligence gathering. Mainly, these principles should be planned to reflect the flexibility and the proportionality of ethical framework that builds upon notions of authority, intention, last resort and discrimination.

Technoethics

David Omand and Mark Phythian (Omand et al., 2013) reference the 'Just War tradition' as the historical basis for ethical concerns over intelligence activities prior to asserting that the

jus in intelligent concepts is composed of:

- right intention
- proportionality
- right authority
- reasonable prospect of success
- discrimination
- necessity

These concepts can be used to guide the behavior of intelligence agencies (Miller et al., 2021). The authors state that the consequentialist ethical theory dominates the intelligence industry, hoping that the results of their actions justify the means. As it pertains to secret intelligence operations, the authors point to the value in professional codes of conduct, judicial oversight and a 'democratic license to operate'.

Ethics of Infosphere

Dunn Cavelty mentioned in his research that the asset to protect, viewed from a national security perspective, can be considered as critical infrastructure. This symbolic term is borrowed from the physical world that plays into the logic of a threat model that justifies government protection (Dunn Cavelty, 2014).

However, its meaning in the digital space is quite broad; it's a catch all phrase to mean the sum total of servers and their ongoing performance with respect to the relationship that they have on economic growth and therefore national security. The complicated point here is that there are no physical borders in cyberspace that neatly defines and differentiates between outside and inside threats. Furthermore, the government is not responsible for the management of digital infrastructure, especially that of private business. A resolution to the dilemma would be to focus on protecting humans instead of protecting inanimate technical objects (Buttrick et al., 2016).

Ethical Framework for security research

During the cyber-security research, researchers can find themselves in dangerous situations that may involve, conflict, political violence, insecurity and even terrorism (Baele et al., 2018).

In fact, the unique focus of cyber-security research requires more than a generalist cyber-security ethical framework can offer. In their research, Baele et al classify the types of risks a security researcher faces into three classes:

1. Researcher-related problems
2. Subject-related problems
3. Result-related problems

They argued that these three categories of risks could inform tailored ethical guidelines to cover the specific physical, psychological and emotional harms that subjects and researchers may be exposed to.

2.7.4 The Impact of Data Breach on Employees' Behavior

"Beyond just the financial impact of data loss, most business owners don't realize how data loss can affect other aspects of their business, including their employees," said David Friend, co-founder and CEO at Carbonite[1].

Carbonite, in conjunction with National Small Business Week, has released the *2014 Report on the State of Data Backup for SMBs*, which demonstrates how exposed small and medium size businesses (SMB) are in relation to security, data protection, backup and recovery. The survey compiles responses from 500 IT professionals at companies in the U.S. with fewer than 100 employees. Startling statistics show that 58 percent are not very prepared to experience any amount of data loss, and 40 percent of IT professionals who service small businesses believe it's likely their companies would go out of business if they permanently lost all their files. From the survey responses, five key takeaways for businesses emerged which should serve as a wakeup call to reprioritize how businesses protect their data and its security:

1. Data Is a Silent Killer to the Bottom Line

2. The Non-Financial Impact of Data Loss

3. Data Security Among SMBs

4. Data Backup is Underutilized

[1] Carbonite, Inc. (Nasdaq:CARB): a leading provider of hybrid backup and recovery solutions for businesses.

5. Backing Up Online and to the Cloud

Data loss was familiar to most who took the survey. Nearly two-thirds (62 percent) of IT professionals surveyed had experienced some form of data loss in their careers. While 33% replied that a result had been profit loss and 32 percent cited a missed business opportunity, many also reported that data loss hurt employees. These negative impacts on employees included:

- 25%: Work/life balance of employees suffered
- 24%: Office morale suffered
- 21%: The IT department became micro-managed
- 15%: Employees were fired or laid-off
- 11%: Employees quit

When a data breach occurs, the impact to staff can be tremendous (Dileep et al. 2020). This impact can be broken down into three main categories (Angst et al. 2017):

1. Career path
2. Confidence / Trust
3. Consequences

These three categories are explained in the next paragraphs.

Career path

Often with data breaches, someone loses their job (Li et al. 2014). When we think about scenarios such as vulnerability exploitation or an accidental exposure, there are steps that could have been taken to avoid the breach. With the financial loss, those centered on the way in which the breach took place are often firmly in the firing line. Future career opportunities can also be impacted. The perception that someone worked for “Company A” during the time it was breached can often be a negative stigma that will follow employees on their CV / resume when seeking employment changes.

On the other side, when a data breach occurs the employees will be more motivated to learn more and build knowledge about data security (Abdoun et al. 2017). Their curiosity will increase to know more about the cyber-security countermeasures that should be implemented and how they can tackle future data breach.

Confidence / Trust

The blame game can start to take place within the organization. Looking for faults. This can often pit department against department or employee against employee as organizations look to find the root cause of the issue. Company policy may dictate that rights, permissions and access may need to be reduced as a result of a breach. In turn, this can make staff feel a lack of trust is being placed on them as a result of the breach and cause personality changes such as disgruntlement.

Alena Reva, Head of Human Resources, North America, at Kaspersky says that such personal consequences may affect the company's overall reputation for both external and internal audience: *"Studies have shown, and it is also common sense, that a data breach can cause substantial damage to a brand's value due to a loss in consumer trust, and it will definitely impact a company's reputation as an employer and impact its employees trust. Breaches can draw media attention, which results in unwanted public exposure, and an employee may need to answer unpleasant questions from their family members and friends. Therefore, it is important for companies to be transparent with their people about what has happened, why it happened, what company plans to do to fix it and how employees can help. People know that anyone can make a mistake, but it's important for the company's management to stick to company values managing the aftermath, as how the company comes back from the mistake is what matters for people."*

Consequences

All employees in any industry or company are consumers of another. The data breaches and leaks of said companies can affect your employees and your business in multiple ways such as increasing stress and lowering productivity (Dhillon et al. 2001).

As a result of a breach it is likely that the incident response, management, and triage process will continue for weeks to months to fully diagnose and understand the events. This will mean a significant increase in hours for staff (IT staff in particular). This can disrupt work/life balance opportunities in the short term and potentially long term for certain positions. This can impact their family and home life (Zhang et al. 2009). Data breaches rarely come with the luxury of staffing increases. Not only do employees have to contend with the data breach work, but also the BAU work that will need to continue to be done. Employees will often find themselves pulling 60, 80 even 100-hour workweeks following such an event. Personal financial implications may quickly be felt by employees who quickly realize a data breach will likely impact their chances of bonuses, merit increases and promotions for the months and years to come within the organization (Vance et al. 2012).

There's no denying the emotional impact that people face when they realize that their privacy has been violated. And depending on the type of personal data that was included in the breach, their personal lives and relationships could have taken a hit as well, all of which can bleed into their work environment, leading to lowered productivity and quality of work (Pahnila et al. 2007).

Compromised data and personal information take a lot of work to secure and change. Employees could be overworked by having to visit their banks to secure their accounts and having to work on replacing all their old emails and passwords for those accounts, which are nothing short of a ticking time bomb. As a consequence, the data can also influence the social relationships of employees and their health.

The figure below represents personal consequences of data breaches for employees in SMB and enterprise organizations[2].

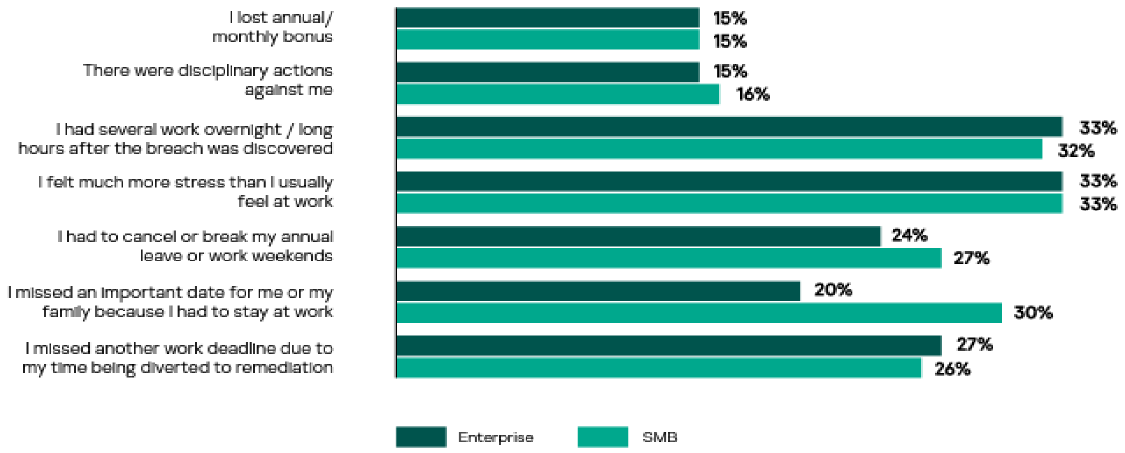


Figure 3: Personal consequences of data breaches for employees in SMB and enterprise organizations[3]

2.8 Conclusion of the Literature Review

“Cybersecurity leaders are burnt out, overworked and in ‘always-on’ mode,” said Sam Olyaei, research director at Gartner. In a survey of 500 IT decision-makers, ThreatConnect found the frequency and severity of attacks are impacting the mental health of cyber-security professionals; 32% or respondents reported feeling highly stressed about work and more than half said their stress levels had increased over the last six months alone. Gartner has argued that the role of cyber-security leaders needs to be reframed. Threat actors are opportunistic and data breaches happen, but they don’t have to be career- or company-ending. Organizations with a good security culture learn from data breaches by implementing policies and controls to reduce the risk of a future risk. Cyber-security awareness training programs help give employees the tools to recognize, report and respond appropriately to phishing attempts. Technologies such as multi-factor authentication (MFA) (Abdoun et al. 2021), endpoint detection and response (EDR), next-generation firewalls, and offline backups can make a huge difference in network defense.

[2] Kaspersky Global Corporate IT Security Risks Survey 2019
[3] Kaspersky Global Corporate IT Security Risks Survey 2019

Chapter 3

The Research Method

This chapter aims to elaborate on the research design, which methods were chosen to answer the research questions, why these methods were chosen, and who are involved as respondents.

3.1 Research Design and Procedures

The following section will address the implementation of the literature review, followed by the development of the interviews and survey. Then, the chosen methods will be critically analyzed, and the chapter will end with some reflections.

The most common approaches in this section are qualitative and quantitative. In this report, I will follow the qualitative approach. The qualitative approach focuses more on case studies. However, "Qualitative research methods are designed to help researchers understand people and the social and cultural contexts within which they live. The goal of understanding a phenomenon from the point of view of the participants and its particular social and institutional context is largely lost when textual data are quantified.“ (Mayers and Avison, 2002)

Quantitative research aims to collect and analyze data collected through surveys, interviews, and polls. It does so by analyzing the data using statistical techniques and by generalizing it across various groups.

In this project, I will use qualitative research represented by interviews.

3.2 Data Collection Methods

Qualitative method is represented by six interviews and the quantitative method is represented by one survey . Because of the the low number of responses received in the survey , I focused on the qualitative method and summerized the survey results in the section 5.6. The research analysis method used for the interviews is thematic analysis.

3.3 Ethical issues

There was a specific way for asking the participants for interviews or for filling out the survey. The most important thing is telling them who I am, what I am studying, and in which university. Besides, the name of my master's thesis and how long it takes for implementing the interview or filling the survey. Because data breach is a sensitive topic, it took more time for some organizations to consent to make the interview. Two organizations refused to consent the interview after waiting three weeks for one and five weeks for the other. One organization asked for additional information. Another one asked to anonymize the name of the company. However, they have the right for that or to withdraw. I sent the questions in advance to all the organizations I interviewed. There were some questions in bold. These questions are more important than the others as they address my topic and problem statement directly.

Regarding the survey, I shared the link of the survey with the largest security facebook group in Norway "IT sikkerhet". The link is the "SurveyXAct" platform. It is a professional survey that belongs to UiA library. Nine participants have completed the survey. Many reasons are expected for getting only nine responses. First, the survey was long and has four pages. Second, there are several open questions. Third, a few people could actually experience data breaches. So, it is not easy to get many participants in this field.

3.3.1 Consent and NSD

Before implementing interviews, I contacted NSD to get consent via an official letter. NSD is the authority that ensures that data about people and society can be collected, processed, stored, and shared safely and legally, presently and in the future. As a result, they approve and consent to my application for my research. The letter contains information about which institute is responsible for the research project, what the project is involved in, and how the participation should be implemented, for example, it is voluntary, and the participant has the right to withdraw. The letter focuses also on privacy: How personal data will be stored and used. For example, personal data for the purpose(s) specified in this information letter. Personal data will be processed confidentially and in accordance with data protection legislation GDPR (the General Data Protection Regulation and Personal Data Act). In addition to that, the letter includes my rights that can be identified to the collected data and who has the right to process this data.

The consent is related to a deadline:

Any personal data including digital recordings will be deleted by the end of the project. The project is scheduled to end [20.12.22]. All personal data including digital recordings will be deleted by [25.08.23].

3.3.2 Transcription

Four semi-sreuctured interviews have been implemented in addition to one with an expert and another with a reseasrcher. After the interviews were completed, the transcription process was then carried out. Each interview lasted around 50 minutes. Two interviews were in Norwegian. Thus, the process of transcription was time-consuming as it took several hours, and each interview produced around 7-10 pages of raw text.

Table 7: **Transcription statistics**

Data Description	**The number**
Interview respondents	4
Average interview length	50 minutes
Interviews in English	2
Interviews in Norwegian	2
Transcription length	7-10 pages
Sent interview invitations	9
Researchers	1
Experts	1
Sent researchers and experts invitations	7

3.4 Table of Interview Respondents

The table below shows the various aspects of the interviews that were conducted in this thesis. It also shows the respondents' job titles, the organization they work for, the type of business they are in, and the size of the company. The data are collected from various companies. Based on the number of the employees, the size of the organization is determined. The information in the table is protected by data protection laws in NSD.

Table 8: Overview of interview candidates

Co de.	**Job title**	**Organizational name (Anonymized)**	**Sector (Private or Public)**	**Size**	**Type of business**
R1	SISO	MelonDB	Private	Large	IT and Security (factory)
R2	IT Consultant	OrangeDB	Public	Large	Restoration of system and infrastructure
R3	System Manager	KiwiDB	Public	Small	IT responsibility in general
R4	Head of IT	PineappleDB	Public	Large	IT

					responsibility in the municipality
R5	Expert	GrapesDB	Private	Large	Cybersecurity engineer
R6	Researcher	CherryDB	Private	Large	Officer at Internal Security Forces

3.5 Qualitative Data Methods

3.5.2 Thematic analysis

Thematic analysis is a type of qualitative research that focuses on the patterns and themes that emerge from various sources. It is usually performed on transcripts or interviews. The researcher then carefully examines the data to identify the common themes and ideas.

There are two different approaches to thematic analysis: Caulfield, J. (2022, July 21)

- An inductive approach involves allowing the data to determine your themes.
- A deductive approach involves coming to the data with some preconceived themes you expect to find reflected there, based on theory or existing knowledge.

The most common form of thematic analysis is through a six-step process according to Caulfield, J. (2022, July 21):

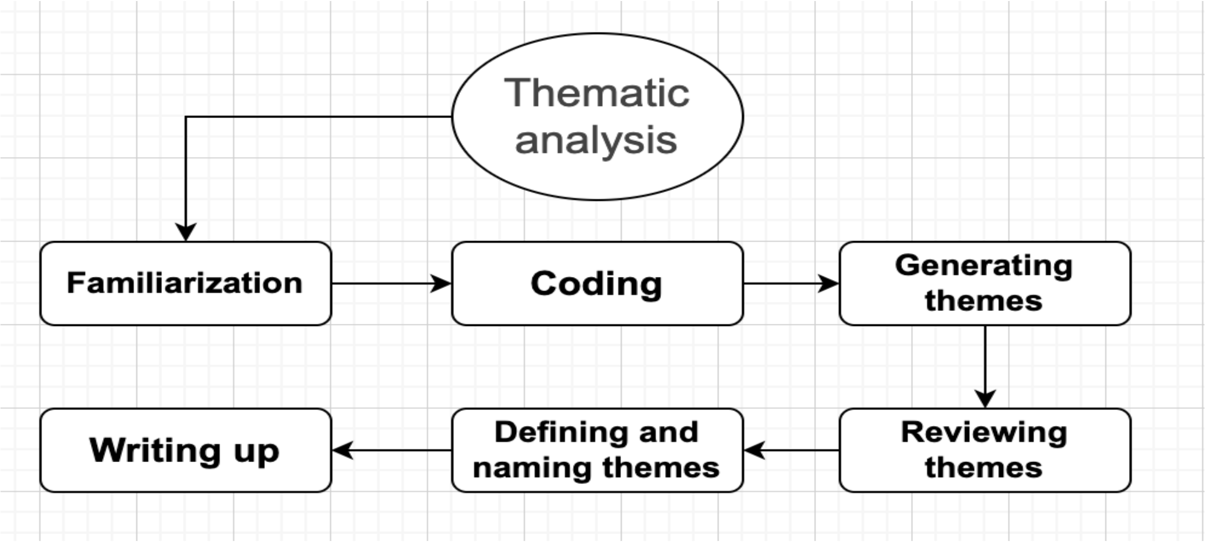


Figure 4: Thematic analysis

Step 1: Familiarization

Getting to know the data collected is the first step in the process of analyzing it. This can be done by transcribing audio or reading through the text. Doing so will allow you to get a better understanding of the data and its various features.

Step 2: Coding

The next step is to code the data. This process usually involves coming up with a set of labels and codes. Usually, coding refers to highlighting the various parts of text. The figure below is a short example code:

Table 9: Coding qualitative data

Interview extract	Codes
In MelonDB, we have coral conduct which sets standards for how MelonDB employees should behave. This sector addresses corruption, fraud. We also have elements of expectations of the employees in terms of safe behaviour with IT systems, for example, clicking the links of the emails and phishing. So, the coral conduct is covering all the aspects of the employees' behaviours. If this is being breached, the company will do a reaction.	● Ethical framework ● Employees behavior with IT ● Ethical impact on employees' behavior

In this extract, I have highlighted different phrases in different colors that correspond to the different codes in the text. These codes represent the ideas or feelings expressed in the text. This process needed to be thorough, as I went through the transcript to highlight everything that caught my attention. New code was also added throughout the text.

Step 3: Generating themes

After creating the codes, we start developing themes. Themes are usually broader than the codes they are based on. Most of the time, one will combine multiple codes into a single theme. In our example, one might start with a combination of codes.

Table 10: Turning codes into themes

The Code of the Main Themes	Examples of the coding
Cyber Attack Events	All related incidents and impacts that occurred when an attack happened. In this study, I use the following categories: Ransom attack, system down, confidentiality, privacy disclosure

Organizational and Ethical Aspects	All related ethical and organizational aspects that link. In this study, I use the following categories: Cyber-security authority and stakeholders, ethical framework, and transparency and reputation
Communication and Information Sharing	All related communication and information sharing. In this study, I use the following categories: Internal Communication and external Communication
Organizational Learning	All related learning from cyber-security events inside the organization. In this study, I use the following categories: Employees behavior, employees training, and crisis management

Sometimes, some of codes might be too vague or not relevant enough. For instance, it does not appear in the data often. One can then decide that some of these are no longer relevant and discard them.

Step 4: Reviewing themes

Before one can start using our themes, one has to make sure that they are accurate and useful representations of the data. This step involves going through the data set and comparing the various themes against it. One can then ask: What can be done to make them better. For instance, if one has issues with them, one can split them up or create new ones.

Step 5: Defining and naming themes

After identifying all our themes, it is time to define them. This process involves coming up with a set of terms that will help us understand the data.

Step 6: Writing up

Like other academic texts, a thematic analysis should introduce the reader to the research question and the approach that we're going to use. It should also explain how we gathered the data, including how one did it through open-ended survey questions or semi-structured interviews. The results or findings section of a thematic analysis typically focuses on each theme in turn. It explains how these come up and what they mean, as well as provides examples of the data. Finally, the conclusion should also expound on the main takeaways and show how the analysis has answered the research questions.

3.5.3 Coding Groups

When it comes to performing research, coding is needed in order to improve the way data is recorded. This discipline can be a common part of one's research procedures, and it can be beneficial to redesign how data is collected. Before oconducting research, one must identify what data is relevant to the subject that s/he is researching for. This can be done by using various techniques and keywords. Having a wide variety of information can help one see the overall picture. Researchers might not be able to see the details of the data they're gathering due to the use of software. This issue can be a problem because it limits their ability to analyze the data.

Learning how to code can help students understand what they are capable of doing with the data they are gathering. In addition to being able visualize the data, learning how to code can help create a more accurate analysis of the data. For instance, I used keywords to describe the various categories of data I was gathering. The table below shows an example of how I used these terms.

Table 11: Interview extract from OrangeDB, an example

Thematic Block	**Interview extract**	**Coding**
During the cyber-attack events	It was not that difficult because absolutely everything stopped and a message and demand for ransom virus came up on the screen. Demands for money appeared. We did not have access to our own systems, so it was not difficult to confirm that it was a cyber-attack.	Ransom attack System is down
	We know but I cannot say since it is under police investigation. In general, the security measures we had were not strong enough to cope with the attack that came, but technical details I cannot tell about.	Confidentiality
	It was in a way a consequence of the data attack and there was later a data leak in the dark web because we did not pay, and it is simply a violation of privacy legislation.	Privacy disclosure
	There was stealing of personal information as I said, there was data leakage later. There was also service downtime on all services over many months because we cannot recover everything at once.	Consequence of the data breach
	There were also reputation costs for our reputation. There were also large financial costs. That is about 40 million to restore the entire municipality again.	Reputational damage

Organizational and Ethical Aspects	We have notified all the relevant authorities, the Norwegian Data Protection Authority was one of them, the national security authority was one of them, the police were one of them and the National Center for Cyber Security was one of them	Cyber-security authorities
	We have done this with the employees. We gave information for the employees immediately and irregularly. As for the inhabitants, we have also informed in various ways. first contacting the Media so that we could be open and honest in the media and notify all citizens. Later, we got a better overview of the scope and problems; We have written and sent SMS to all residents.	Transparency Prioritization
	All experience shows that in such cases when you pay you only get a new claim a little later and more money and you are blackmailed time and time again. The whole world knows that such criminal actors work.	Ethical cyber-security
	There are also rules that describe very well what should be done, who should be informed, and who should be reached. We have done this after the cyber-attack, and we are also engaged specialists in the field to help us.	Administrative controls: 1. Policies 2. Procedures 3. Processes
	We have notified our citizens that the cyber-attack took place. Data may be available online, but we did not know we were just notifying that it might be possible. Later, when it happened, about two thousand files were available online. These 2000 files identified who affected each and then we have made direct contact with every one of those affected.	Ethical framework Dark web
	We also had a dialogue with all companies that have a relationship with our municipality. We have software with technical documentation on our servers. It may be that their technological secrets could be taken by the trosector.	External Communication Communication to Stakeholders
	We have changed our work processes by buying a new system, upgrading a system, and making changes at the technological level. We are going	Risk management

	through a process that takes care of privacy assessments, risk analysis and security analysis that is a third party that we do not do. We have employees who have more security expertise and privacy expertise. Now, we are very careful with that type of work. We practice now a zero-trust principle.	Cyber-security controls and measures Cyber- security requirements: -Process changing -Privacy assessments -Risk analysis

Recommendation/ inter-organisational learning	We have ordered a report with recommendations and any municipality should do to avoid what we have experienced. We need technical systems that detect vulnerabilities that tell us what kind of security holes we need to fix, but we also need expertise to be able to understand the seriousness of the situation and we need a capacity to handle the situation and where the complexity to be more aware of and that is what enables us to better cope with such situation.	Documenting the fails The need for new technologies and experience

Figure 5: Word cloud of the most repeated words in the thesis

Chapter 4

Case Studies

This thesis examined four security breaches that attracted cyber-security professionals and practitioners in addition to t one expert and one researcher who work within the cyber-security field. I anonymized the name of the companies/ organizations and certain details used in this study.

The first case is a company in a big private sector with global business in 40 countries having 35,000 employees worldwide based on the company report available publicly from 2021. For further elaboration and discussion, his case will be referred to as *Case A*.

The second case is a case of a public organization with a small municipality in Norway that has approximately 15,000 population based on the demographic data for 2019. Regardless of the size of the municipality, the security breach event that occurred in this public organization is very impactful, as the malicious actor has used a ransomware technique. The impacts are not only severe data leaks but also economic impacts. This case will be referred to as *Case B*.

The third case is another public organization in a municipality with approximately 114,000 population based on the demographic survey 2022. The organization is relatively small, however, data breaches have not yet occurred before, as compared to other public organizations, this organization seems not to be the most attractive target of attacks, but it has happened, thus triggering strong attention. This case will be referred to as *Case C.*

The fourth case is also a public organization with about 6500 employees. Data breach occurred in a part of the organization infrastructure for water supply. After the data attack, the municipality changed its strategy to strengthen data security for the VA system. This case will be referred to as *Case D.*

4.1 Case study A

In 2019, MelonDB was the victim of a cyber-attack. This incident affected various of the company's business areas. The attack targeted the entire global organization. Extruded Solutions was the most affected area, with significant financial losses and operational issues. Despite the attack, MelonDB's other business areas were able to operate normally. MelonDB worked around the clock to resolve the issue and continue its operations. In response to the attack, the company worked closely with external experts to resolve the issue. All of its servers and PCs were thoroughly cleaned and re-established according to strict guidelines. The company has also reorganized its security team to better identify and respond to cyber threats.

In response to various international and Norwegian authorities, including the National Security Authority of Norway and the Norwegian National Investigation Service, MelonDB is in talks about the cost of cyber insurance. The company has estimated that the total cost of the insurance would be in the range of 550 to 650 million Norwegian Kroner. (Anonymized)

4.2 Case study B

In 2021, OrangeDB was exposed to the worst cyber-attack that has affected any Norwegian municipality to date. All email systems were put out of order, all backups were deleted and all data encrypted so that none of the 1,300 employees in the OrangeDB could use any of their computer systems. OrangeDB was paralyzed after a very extensive ransomware virus. 1000 computers had to be restored, and 1300 employees worked for a long time with pen and paper. The mayor believed they had lost an estimated 35 million NOK. The attack was the worst computer attack aimed at any Norwegian municipality. TheOrangeDB has made an extraordinary effort to uncover what has happened. They have also spent a lot of money on establishing good ICT systems to ensure security. It is quite obvious that the municipality has not had its systems in place. That is why the Norwegian Data Protection Authority has announced a fine of four million krones. However, OrangeDB has chosen not to pay a ransom because the result is usually that the company does not get back data. In addition, ransom helps motivate criminals to continue their blackmail. (Anonymized)

4.3 Case study C

In 2020, we received a message from our supplier of the website, that we had been hacked. The website has been hacked and shut down. Personal information is not lost. The website has been unstable for two days as well. There were problems with the form for registering users, and links on the Main Page were not clickable. The site showed errors when we opened it. Thus, employees had reacted to and notified about. The homepage was immediately shut down.

To prevent anything else from being destroyed, information was posted on the Facebook page for KiwiDB. Only the homepage was affected. The unauthorized parties have not obtained names, addresses, passwords or lending information. There are two completely separate systems. Three of the employees worked furiously for the whole day to save the website content. Two days later, the IT supplier started working on a new secure website platform.

4.4 Case study D

In 2021, PineappleDB was exposed to a hacker attack on part of the infrastructure for water supply. “PineappleDB has been exposed to a hacker attack on a smaller part of the infrastructure for water and sewage. PineappleDB has control over the situation, and all water and sewage systems are functioning as normal. None of the municipality's residents are affected by the situation, and no personal information is lost."

Dagbladet, in collaboration with Municipality Report, writes in its paper that a Russian hacker group is behind the attack. According to the newspapers, the hacker group Avaddon is behind the attack. The newspapers also write that this is confirmed by sources in the PineappleDB.

The attack against the water and drainage system towards PineappleDB took place shortly after another hacker attack against the waterworks in Oldsmar in Florida, USA. The newspapers put these two attacks in connection with each other. In Florida, the hackers are said to have managed to adjust the amount of toxic lye in the water to more than 100 times the normal level - which could have given the users caustic damage to the skin and mucous membranes.

There was never any danger that this data attack threatened the water supply in any way, nor did the hackers gain access to personal information. There was no major threat, but it should never have happened, says business manager ICT S. H. A in PineappleDB to Dagbladet and Kommunal Rapport.

As in many other municipalities, the water and sewerage agency in PineappleDB had its own servers for the water and sewage system. This server park was operated by the VA agency.

After the data attack, the municipality changed its strategy to strengthen data security for the VA system. Now we have a joint strategy, and that is a big advantage. Having a professional ICT organization behind you clearly provides extra security, says A. (Anonymized)

Chapter 5

Findings

This chapter consists of findings that will be presented in the form of a comprehensive analysis of the data collected during the study. The six interviews that were conducted were analyzed using a thematic content analysis method.

Interviews were conducted with four different organizations that had cyber-attacks, as well as one researcher and one expert. All organizations interviewed are large, except for one, which is a part of a large municipality. Both experts and researchers are working in large organizations. However, this study elaborate the findings in different areas when organizations experience data breaches.

Table 7 in (Chapter3) shows the various sizes of companies and the types of individuals interviewed. Most of the respondents were professionals working for public organizations.

5.1 Cyber-attack events

This thematic section contains the events that organizations went through during the cyber-attack including the reaction of the involved stakeholders and their roles. In this situation, certain parties should be informed about the event before advertising it in the public and several consequences in different areas usually appear after the Cyber-attack events.

5.1.1 Career

All the persons interviewed working either in IT or cyber-security fields. All of them are familiar with data breaches events and their impact. Some of the interviewees mentioned also the legal framework for their roles and how they are driven by GDPR.

"I am familiar with the breaches in the department zone we have had, we are also very driven by the GDPR and privacy legislation that came into force in June 2018." KiwiDB respondent

OrangeDB respondent explained the difference in his role before and after the data breach and the influence of the legal framework on his position.

"Before, I was not familiar with this. I have not had experience with the data-attack/cyberattack until last year, nor with ethical aspects. Since last year, I worked a lot with laws and regulations. Now we respect them and know what rules apply and all these types of things".

GrapesDB respondent has not experienced cyber-attack or data breach itself, but he explains what he would do if such events occurred.

"I would go through monitoring systems and getting alert when an event/incident occurs. SOC team would be one of the first ones to know and alert the correct people".

5.1.2 Confidence

One of the most important procedures in cyber-security is confidentiality. Much information should be kept secret or within limited parties. All the organizations I have interviewed tried to limit the damage through different ways.

MelonDB respondent tells about the procedures followed data breach:

“This happens on several thousand PC's and several hundred servers for two nights. After that, it immediately affected our IT infrastructure. When we discovered it, we understood that it was a cyber-attack. So, we immediately started turning off connections in the network and shutting down our servers to prevent more damage to happen”.

KiwiDB respondent focuses on the importance of protecting data from unauthorized people to the extent they deactivated every platform that might have been breached.

“IF you suddenly experience that you receive so many unwanted emails, it may be that unauthorized persons have obtained email addresses from the newsletter list integrated into the website. Therefore, we have deleted and deactivated it”.

It important for the Norwegian organizations to keep their data only in Norway, KiwiDB respondent highlights:

“This has a high degree of certainty that the data stored in Norway on Norwegian servers of the Norwegian system supplier in Larvik and is processed only in the form needed”.

When interviewing OrangeDB, the respondent did not disclose some technical details as the case was under police when I asked about exploiting vulnerability:

“We know but I cannot say since it is under police investigation. In general, the security measures we had were not strong enough to cope with the attack that came, but technical details I cannot tell about”.

GrapesDB respondent did not disclose the followed procedures for notifying customers where s/he works either:

“I cannot speak on behalf of the companies I work with, but usually companies do not notify immediately”.

Moreover, most of the organizations interviewed have asked me to anynomize the name of their companies because many questions have very detailed answers and so do we.

5.1.3 Consequences

When data breaches occur, many consequences come up. These consequences vary according to the level of the data breach. Almost all the respondents have talked about the consequences. In my study, I highlight the most important consequences tha came up based on my thematic analysis of interviews.

The most remarkable consequence when data breach occurs is that the system does not respond or is down. This KiwiDB respondent tells about their data breach event.

“One day, we noticed the website was down. The site has been unstable for two days”.

MelomDB respondent explains the situation in more details as s/he ends with the consequence of clicking on a malware link:

“The attacker(s) got some software, and our system was unable to discover it, and the attacker(s) was able to connect back to the command-and-control centre on the internet. So, the attacker basically removed the control over what was happening on the PC and jump into a new system”.

In addition to the damage of the system or the site, there is a need to build up a new website or at least to fix or develop it. This costs both money and time. PineappleDB respondent assures that when asking about their data breach consequences “*Reputation of course and financial consequences including rebuilding a system through backup”*

MelonDB respondent mentions multiple consequences of their data breach including the financial and operational ones in addition to the loss of production.

“Financial impact which we have reported extremely. It is now up to 800 million Norwegian krone”. S/he adds *“There is also an operational impact. When attack happened MelonDB lost access to the IT system that we use to operate our plans”. “Production for these units jump down to 67% for some plans. It took about one and half months to come back to its rate again”*

KiwiDB respondent tells about the extrem costs of the breach, but s/he indicates that they have got a good website in return. *“Costs: Website 120,000, personnel costs 100,000, but we have got a nice website that is integrated with our -- system on profile”.*

As a researcher, CherryDB highlights that the consequence of cyber attack is mainly to steal personal information *“The consequences of the attacks were mainly stealing personal information and service downtime”*

At end, OrangeDB respondent elaborates about the different conscequeces that came up after their data breach. *“Unfortunately, there was stealing of personal information as I said, there was data leakage later. There was also service downtime on all services over many months because we cannot recover everything at once”*. S/he adds *“There were also large financial costs. That is about 40 millions to restore the entire municipality again”*

5.2 Organizational and Ethical Aspects

Organization's ethical aspects can guide the organizations in their actions. These principles and values can be used by employees and other individuals to make decisions and conduct themselves in a certain manner.

5.2.1 Cyber-security authorities and stakeholders

Certain parties should be prioritized to notify when data breaches occur. Three authorities have been notified in all cases I have analysed. These authorities are Police, The Norwegian Data Protection Authority (Datatilsynet), and National Security Agency in Norway. In addition to these authorities, some organizations have other parties to notify, for example, consulting companies and users as PineappleDB and KiwiDB respondents highlight.

“*We also contacted “Atea” we're using them as consultants we have a frame agreement with Atea when they come to technical consultants”.* PineappleDB.

KiwiDB respondent states *“We have reset all passwords in the entire system and sent SMS and email to all registered users”.*

5.2.2 Ethical framework

Some standards or ethics are followed in organizations during critical times. These are mentioned by both MelonDB and GrapesDB respondents.

"In MelonDB, we have coral conduct which sets standards for how MelonDB employees should behave". The respondent adds *"In security, we are talking about control framework. We are strengthening our cybersecurity capabilities. In cyber-security, we often talk about controls, we use for example "The ISO/IEC 27000" as a control framework"*

"Organizations I have worked with use ISO standards which include many aspects, if not all, of how to run a company. In addition, The NIST framework with alignment to GDPR is also implemented". GrapesDB

Both MelonDB and OrangeDB respondents emphasize on the importance of not paying a ransom as a part of their ethical framework. *"The whole team of the crisis room in the company agreed that we should not go with any discussion with the attackers or pay any ransom. Besides, we have had our backups of the data that were not destroyed in the attack".* MelonDB

"All experience shows that in such cases when you pay you only get a new claim a little later and more money and you are blackmailed time and time again. The whole world knows that such criminal actors work". OrangeDB

While CherryDB assures that all data breach incidents should be dealt with according to a rights-based principle that is influential in the law in addition to adopting "design privacy", updating "audit algorithm" and focusing on preventing data breach from occuring again.

"While privacy is a key topic in any ethical analysis of a data breach, other issues are more pressing, such as the responsibility of organizations to prevent and to repair consequences of data breaches".

Besides, All the parties interviewed follow the ethical framework through risk analysis and risk management in addition to revising the framework frequently.

5.2.3 Transparency and Reputation

It is essential for organizations to be transparent with their employees, customers, or users. At the same time, they should also protect their reputation. The balance between transparency and reputation is somehow challenging. However, all the organizations interviewed were open about the breaches. *"We were open about the root cause we were open about how we handled it. We have taken a lot of steps to avoid it in the future"* PineappleDB respondent. To be open does not mean disclosing information immediately. Therefore, all the organizations follow a prioritization order in notifying the different parties. On the other hand, being transparent keeps your good reputation in the public as happened with MelonDB and KiwiDB. *"Regarding the reputation risk, we were open about the situation and transparent to the media. We did not see that our stock markets decreased based on this. We got quite good feedback from the market about this openness. So, MelonDB did not lose its reputation from this breach".*

"Reputation was not ruined by that episode, on the contrary, we have received a lot of support". KiwiDB

At last, it is important to build trust with consumers or citizens to enhance transparency as CherryDB did in his/her organization *"We built trust and transparency with consumers and citizens, which are part of good information governance, as a means of maximizing the value of information derived from data analytics while minimizing risks.*

5.3 Communication and Information Sharing

During a crisis, it is important that the people who are involved in the communication are aware of how to communicate and share information effectively. This can help minimize the damage caused by a data breach. Based on the thematic analysis, I have divided communication into two categories:

5.3.1 Internal Communication

It is the process of communication inside the organization, for example, among the employees or the head of departments. Some of the organizations tell about the importance of communication internally. This can be through direct communication among the employees or through sharing information by courses and learning. MelonDB respondent points out *"We communicated heavily and internally about the situation. Luckily, when we talk about personal data, we only talk about usernames and passwords"*

PineappleDB respondent indicates their way of sharing information *"Every Tuesday morning, they get this little thing in the e-mail as a new session or a new learning".*

On the other hand, OrangeDB states that the bad communication during the crisis does not help with handling problems. *"The three major areas that we experienced more difficulty or more to learn from are interaction, information, and communication. While the systems are down, it helps little to say that we have teams".*

5.3.2 External Communication

It is the process of communication outside the organization. Stakeholders and users who are not working inside the organization can be communicated after data breach. Consulting companies are also a good example for external communication.

"We contacted Atea (consulting company), as we have a subscription with that incident response team, so we contacted them right away and they started working on the case immediately". PineappleDB

However, external communication can also be in the form of information sharing with other organizations to learn from the experience of the organizations that have been vulnerable to data breaches. *"We have also informed the similar organizations to use the same solutions, one has had weaknesses with plugins, some more security measures were taken from servers. We thought that WordPress with these plugins would again run a risk of poor maintenance both centrally and locally".* KiwiDB

"We have attended different workshops, seminars, and conferences where we have been very open about all this". PineappleDB

In addition to sharing information with other organizations, OrangeDB respondent indicates the importance of documenting everything in case it may happen again and for benefitting similar organizations.

“We also had a dialogue with all companies that have a relationship with our municipality. We have software with technical documentation on our servers”. He adds: *“We have ordered a report with recommendations and any municipality should do to avoid what we have experienced”*

5.5 Organizational Learning

The acquisition of new knowledge can help an organization improve its performance. The resulting knowledge can then be shared with its members. The information can be obtained from the organization itself or from other organizations.

5.5.1 Employees behavior

It is remarkable to know how the bvehavior of employees has changed after cyber attacks or data breaches. All the employees in the organizations interviewed have changed their behaviors dramatically.

MelonDB respondent highlights how they have talked to employees about various risks associated with social engineering and phishing. *“The behaviour change is really enormous especially how to read the phishing emails and report them”.* In addition to that, the ethical framework has also affected the employees' behavior at MelonDB. Therefore, they have elements of expectations of the employees in terms of safe behavior with IT systems. *“The coral conduct is covering all the aspects of the employees’ behaviours. If this is being breached, the company will do a reaction”.* KiwiDB and OrangeDB respondents indicate how the employees have become more conscious regarding how to handle data “*All employees have become more conscious especially when we were to buy a new service (our new website), one must learn how to store data”. KiwiDB.*

“We notice is a little different because now the employees are more suspicious and cautious. They ask more. They ask for more confirmation”. OrangeDB. This idea is aslo mentioned in other words by CherryDB respondent.

“The employee’s security behavior has been changed after data breaches including how employees handle their passwords, how employees interact with organizational data, and how employees use network resources”.

While GrapesDB respondent has another point that the behavior change depends on the employee's role. S/he gives example of an employee of incident response. *“An employee of incident response team would not change behaviour but rather focus on the incident and how to handle according to the plan”.*

However, OrangeDB respondent indicates also the importance of the employees' reaction of other departments for IT employees: *“Our employees have helped the IT department and they have helped us through being patient instead of complaining that nothing works. They have been patient”.*

5.5.2 Employees training

The training of employees is usually conducted when new employees join the organization and after data breaches. Employees typically submit to different courses depending on their role within the organization. In order to prevent human flaws from arising after experiencing a data breach, It is important to consider training. In my study, all of the interviewees stated that their organizations played a major role in training their employees. MelonDB, for example, implemented a mandatory training. *"We have been communicating, doing mandatory training".*

PineappleDB implemented nano learning to make the employees more aware about cyber-security. *"It's nano learning as the purpose of nano learning is to make all the employees more cautious by going through this 5-6 minute a week awareness program".* In addition to that, they send learning sessions via email to all employees and they have had aqn actual course to the system owners. *"Every Tuesday morning, they get this little thing in the e-mail as a new session or a new learning. Besides, we did have a normal course of information security for all the system owners".* KiwiDB has also implemented an obligatory course with a focus on privacy.

"All employees have taken that course both after and before the episode incident with us, how much is involved in knowing spam, phishing methods, secure passwords, locking screens, and lock tests when they are going out. We take privacy seriously". Besides, both the expert and the researcher interviewed in my study assure the importance of employees training. *"The employees have been trained. They participated in many courses related to cybersecurity such as Information security awareness, Data protection, Cyber first responder and others".* CherryDB

5.5.3 Crisis management

The incident management team should thoroughly manage the details of a data breach to minimize its impact. This can be done through the establishment of a cyber crisis team, the prioritization of incidents, and the use of effective communication. Even before the incident occurs, it should be organized to ensure that the various activities are conducted in a secure and orderly manner. According to the respondents of MelonDB and KiwiDB, their organizations have already implemented some of these steps after they had experienced a data breach.

*"We have established a **cyber crisis team** reporting to the cooperate emergency team. So, we have organised quality, IT and security resources in a structure way. We did not have that before. Now, we have organised the incident procedures. As soon we have a risk, we get this team and start to manage the situation not only in the breach situations".* MelonDB

"We also have regulations that we follow: reporting, handling, and crisis management in such cases". KiwiDB

5.6 Other Findings

I initially planned on conducting quantitative and qualitative research for my study, but due to the low number of responses, I decided to focus on qualitative research. This section will also include the survey's findings distributed in ……. The survey consists of questions related to the person and expertise, During the cyber-attack events, Organizational and Ethical Aspects, Organizational learning, and Recommendation respectively. The majority of the responses are placed in the first, second, and last sections since there are several multi-choice questions in the third and fourth sections. These questions are difficult to answer as they cover the ethical framework. The respondents roles are: Janitor, Security Advisor, Student, Advisor, CEO, Analyst, Senior Consultant, and It support. They have been in their jobs between 2 and 15 years. Most of them are familiar with data breaches. Here are some examples of data breaches they experienced:

Data extraction, Rootkit installed on server to send data out, Someone malicious abused our two-factor authentication by SMS to inflict SMS-sending costs on us, Explorer of outdated CMS plugins, Ransomware attack where data was threatened to be sold or leaked, and Placement of cryptolocker.

These are the vulnerabilities that were used to breach the systems:

- Mainly the screen
- Poor architecture
- phishing, no network segmentation, and social engineering
- Uploading files on website without specific file format allowed .bat and .exe files to be uploaded on website and onto server
- It was possible to request sms-es with two-factor authentication (2FA) codes via script. It was not a vulnerability as such, but a slight potential to cause harm
- Exploit in a plugin mase file uploads available to anonymous users.
- Unused virtual machine in Azure was forgotten about
- Remote Desktop (RDP)

Below are the responses about how the attackers exploited the vulnerabilities:

- Server was exposed to internet
- Spear-phishing with malicious content containing ransomware
- Lucky us it didn't seem to send/transfer any data out from the server
- They created a script that requested thousands of sms in quick succession, causing a higher than usual cost of operating to our company
- Updated user registry, and gave themselves admin rights
- The attacker got access to the Windows Virtual Machines (VM), and use Active Directory (AD) escalation from there. Got the entire network, and took down the entire organization.
- Gained access through Remote Desktop (RDP)

Here are some examples of how employees knew about the attack:

- Attacker initiated a contact
- The news
- The IT partner of our organization found it
- The organization received an unusual amount of bills for sms
- Noticed new users
- Ransomware locked computers and attackers contacted management
- Errors appeared

The purpose in most attacks was financial and the consequences were mostly service downtime and economic costs. The costs of the attacks that belong to participants' organizations are between 30000 and 35 million norwegian kroner. The stakeholders that first notified are CEO, department manager and datatilsynet (Norwegian Authority for Data Privacy). The first procedure taken outside the organizations according to the survey participants is informing police and Datatilsynet. Besides, the organization that had a rootkit as a vulnerability, removed it and restored backup files before rootkit was installed. Other organizations created a task group to counter the continuous breaches and make them impossible. Regarding the ethical framework, it is mostly implemented through ethical awareness. Most employees in the participants' organizations have become more cautious. They have also learned more about privacy.

At last, the participants recommended some procedures to organizations to avoid similar data breaches:

- Backup is gold
- More control on suppliers side
- Make sure you only allow the files you need, and never .exe/.bat files
- Use more time to consider security holes
- Automated updates

Chapter 6

Discussion

The chapter will discuss the interpretations of the findings from the thematic analysis of the interviews. Some of the findings from the literature review will also be addressed in this chapter, and they will be compared and contrasted against those from the interviews. I will try to find similarities and other connections between the two.

6.1 Change management

Following the data breaches that occurred in the oraganizations included in my study, many changes have occurred in the way they approach and manage their data. These changes have become an inevitable need for the affected organizations.

MelonDB have implemented some structural and technical changes targeting the IT model. *"The whole structure is not changed. We have target operating model for IT. Security is a part of this modell.* S/he adds*: "We did strengthen the security especially from the technical side, but on a longer term, we have also had an important discussion about management".*

The various departments of PineaplleDB have been integrated into a single IT system. This has resulted in the organization's structure being changed.*"I think the changes we have done now they are a part of a large professional department or a large professional unit. However, a few communes in Norway are still in that situation where their "water supply" units have their own IT or data that are outside the rest of the organization".*

In response to the data breach, OrangeDB has made changes in various departments. These include the implementation of new policies and procedures aimed at improving infrastructure completely. *"In addition to the organizational change, we have also changed our technical infrastructure completely, nothing that was left. We started all over from scratch. Technical infrastructure was changed, and our work processes were completely reversed. IT department is no longer with us".*

The most significant change that OrangeDB has made is that it no longer has an IT department. Instead, it hires a company to run its system. *"Now, we do not have an IT department with us internally. Our IT department is now a company out there that we pay for to run our IT systems".*

6.2 Employees behavior in literature versus in interviews

The study conducted by Dileep et al (2020) notes that employees are the main reasons for most data breaches. This suggests that they should change their behavior after the incident. However, the findings of the literature review on employees behavior are not similar to those of interviews.

The interviewees avoided talking about the negative effects of the incident on the employees' behavior. Instead, they talked about the positive aspects of the change in their behavior. This is because they were focused on the positive aspects of the incident instead of the negative ones extracted from the literature review.

6.3 Layoffs VS Recruitment

The literature review indicates that many employees left their jobs due to the data breach. This idea is supported by the fact that an interview revealed that many of the employees who were working in the IT department were laid off. On the other hand, MelonDB respondent noted that the investment in cyber-security is very important. Thus, there is a need for more people in addition to new technologies in this field. *"My advice is that you assess cyber security capabilities in a moralistic view and discuss of course with management if they accept the risk or not and if risk within cyber is not accepted then that you raised investment on the program to strengthen cybersecurity capabilities and by doing that you also reduce the risk".*

6.4 Cyber-security awareness

Wileen Barosy (2019) extracted that cyber-security awareness makes people aware of their responsibilities and roles in information technology. Following data breach incidents, awareness is being raised about the importance of protecting personal information. This idea is supported by various literature reviews and interviews. All the interviewees referred to that through following different techniques. MelonDB, for example, followed a white hacking method to enhance the awareness among employees. *"We have also sent false phishing emails to get people click on the link, if they do, they get an educational video about how they should behave".* In KiwiDB, the employees have become more aware and strict. This made some users comment ironically that they are so strict as a bank. *"All employees have become more aware after the incident especially regarding processing of data with password, log in. We have had to be very strict for some of our users who are not digitally good. You are not Norway's bank!!"*

However, CherryDB respondent, who is also a researcher, indicates that cyber-security awareness is a kind of employees education. *"Information security awareness refers to employees' overall knowledge and understanding of potential information security-related issues and their ramifications, and what needs to be done to deal with security-related issues".*

6.5 Cyber-security requirements

Many requirements should be considered when addressing cyber-security. The most important ones that I extracted from both literature review and interviews are the administrative controls including policies, procedures, and processes.

Kwon, and Johnson (2011) found that an organization might learn more from education or internal policies to prevent insider threats than from implementing technical controls.

PineappleDB respondent highlighted that these controls are a part of the IT organization *“We have taken steps to secure this part of the of the system so now they are a part of the IT organization and they and they follow all the processes and procedures from IT”.*

Besides the administrative controls, OrangeDB also has a variety of other requirements that are related to risk analysis and privacy. These include a framework for rules that define who should be contacted and how they should be handled.

“We are going through a process that takes care of privacy assessments, risk analysis and security analysis that is a third party that we do not do. We have employees who have more security expertise and privacy expertise”. S/he adds *“There are also rules that describe very well what should be done, who should be informed, and who should be reached”.*

6.6 Recommendations

Throughout the interviews, I had a thematic section that included recommendations. This section allowed me to gather various pieces of advice that could be beneficial to individuals and organizations working in cyber-security. Here are summarization of the most important ones:

- Follow the regulations
- Put the technical level in the place
- Build more cyber-security capabilities and invest more in cyber-security
- Use “bow tie level” to reduce the probability of an incident happening in the future
- Use proper Information Security Management System (ISMS) and try to be aligned with 27001 standards.
- Seek to understand the critical factors that influence the security choices made by employees
- Include all the departments in a large professional IT unit
- Stay always up-to-date and try to use new technologies
- Document all the fails make sure to not happen again
- Do not focus on the fault, but on how to solve it

6.7 Limitations

This chapter will present and discuss limitations related to the study. The preparation of a research study on the topic of data breaches, focusing on organizational learning, ethics, and employee behavior will likely reveal some of the limitations of the research. Some of these became apparent when I started to do the research. When I performed a systematic literature review, one of the main findings revealed how employees can be affected by data breaches and how these can lead to personal concequences.

Regarding the interviews, most interviewees stated that they had reservations about answering certain questions and providing information. The confidentiality of the topic and the sensitivity of it were some of the factors that prevented many organizations from giving their consent for the interview. It took several weeks for others to come up with a decision. Besides, three of interviewees asked for more explaination for “ethical framework” questions. Some of them think that these kinds of questions are difficult to answer, including the expert and the researcher.

According to the researcher, my topic is wide-ranging and covers various aspects, such as technical aspects of data breaches and the psychological aspect represented by employees’ behavior. It also talks about the social cyber-security aspect inside the organization.

Chapter 7

Conclusions and Suggestions for further research

In the first part of this chapter, I will conclude my study and discuss the lessons I learned from it. In the second part, I will explore the possibilities for further research. The study was conducted to look into how organizations can learn from data breaches with a focus on employees’ behavior and how they can prevent such incidents from happening in the future. It additionally focused on the ethics like transperancy and the importance of sharing information among organizations.

7.1 Conclusion

The first step in the master thesis process was to conduct a literature review to identify the previous studies that were done on the topic. This was done to see if there were any data points that could be used to improve the findings of the study. One of the most significant findings from the review was the negative effects of data breaches on the employees' behavior. However, there are some findings that are to discuss in literature review and interviews results which is the need for ethical frawework inside the organizations. The term “ethical frawework” could be a liitle bit difficult, but MelonDB respondent, for example, called it control framework as this term is more suitable for cyber-security.

The lessons I learned form the research are mainly about time management and having alternative plans regarding the research. My initial plan was to conduct quantitative and qualitative research. When this plan did not work, I shifted my focus to qualitative research. I initially planned on conducting seven case studies, but this was difficult because many organizations did not want to talk about their data breaches they experienced for different reasons. Therefore, I sent many requests to experts and researchers to get only two positive answers. This operation took much time and made me overwork in the last days before the deadline.

7.2 Suggestions for further research

The thesis aims to shed light on an important topic, that is connected to data breach. Further research is needed to analyze how employees play a role in the implementation of the ethical fromework or control framework in an organization. It can also explore the various administrative controls that an organization should have in place to ensure that its cyber-security is protected.

Further research could also be conducted to improve the knowledge of employees and the effectiveness of communication within an organization to prevent data breaches. This could additionally help prevent the impact of data breaches on the business.

References

Anonymized (2020). “Cyber-attack on Anonymized Company”. {Accessed: May. 17, 2022}

Anonymized Authors (2021) “Hacket anonymized organization får 16 millioner kroner i statsstøtte” {Accessed: May. 17, 2022)

Anonymized (2022) Hevder russere står bak hackerangrep mot Anonymized organization. Accessed 28 November 2022.

Abdoun, N., El Assad, S., Manh Hoang, T., Deforges, O., Assaf, R., & Khalil, M. (2021). Authenticated Encryption Based on Chaotic Neural Networks and Duplex Construction. Symmetry, 13(12), 2432.

Abdoun, N., El Assad, S., Hammoud, K., Assaf, R., Khalil, M., & Deforges, O. (2017, December). New keyed chaotic neural network hash function based on sponge construction. In 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 35-38). IEEE.

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology, 71(8), 939-953.

Angst, C. M., Block, E. S., D'arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches (January 24, 2016). Angst, CM, Block, ES, D'Arcy, J., and Kelley, K, 893-916.

Argote, L., & Miron-Spektor, E. (2011). Organizational learning: From experience to knowledge. Organization science, 22(5), 1123-1137.

Barosy, W. (2019). Successful operational cyber security strategies for small businesses (Doctoral dissertation, Walden University).

Bennett, V. M., & Snyder, J. (2017). The empirics of learning from failure. Strategy Science, 2(1), 1-12.

Bellaby, R. (2012). What's the harm? The ethics of intelligence collection. Intelligence and National Security, 27(1), 93-117.

Baele, S. J., Lewis, D., Hoeffler, A., Sterck, O. C., & Slingeneyer, T. (2018). The ethics of security research: An ethics framework for contemporary security studies. International Studies Perspectives, 19(2), 105-127.

British Academy & Royal Society, “Data Management and Use: Governance in the 21st Century,” 2017.

Brown, J. S., & Duguid, P. (1991). Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation. Organization science, 2(1), 40-57.

Buckman, J., Bockstedt, J., Hashim, M. J., & Woutersen, T. (2017). Do organizations learn from a data breach. In Workshop on the Economics of Information Security (WEIS) (pp. 1-22).

Buttrick, H. G., Davidson, J., & McGowan, R. J. (2016). The Skeleton of the Data Breach: The Ethical and Legal Concerns. Rich. JL & Tech., 23, 1.
Carter, Rebecca. (2021). Den ultimate listen over cybersikkerhets statistikk for 2022. Findstack. Accessed 8 September 2022.

Caulfield, J. (2022, July 21). How to do thematic analysis: Step-by-step guide & examples. Scribbr. Retrieved November 14, 2022, from https://www.scribbr.com/methodology/thematic-analysis/

Clay-Williams, R., & Colligan, L. (2015). Back to basics: checklists in aviation and healthcare. BMJ quality & safety, 24(7), 428-431.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. MIS quarterly, 673-687.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. Computers & security, 29(2), 196-207.

Dahlin, K. B., Chuang, Y. T., & Roulet, T. J. (2018). Opportunity, motivation, and ability to learn from failures and errors: Review, synthesis, and ways to move forward. Academy of Management Annals, 12(1), 252-277.

Davis, B. (2021, April 30). What is a concept matrix? – MVOrganizing. Mvorganizing.org.

Demlehner, Q., & Laumer, S. (2020). Why context matters: Explaining the digital transformation of the manufacturing industry and the role of the industry’s characteristics in it. Pacific Asia Journal of the Association for Information Systems, 12(3), 3.

Dileep, K., Venkatesh, R., Kumar, B. S., Rao, K. U., & Kshatra, D. P. (2020). Analysis of Data Breaches and Its impact on Organizations. International Journal, 8(10).

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and engineering ethics, 20(3), 701-715.

Dhillon, G. (2015). What to do before and after a cybersecurity breach. American University, Washington, DC, Kogod Cybersecurity Governance Center.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information systems journal, 11(2), 127-153.

ENISA. (2017). Cyber Security Culture in Organisations. European Agency for Network and Information Security.

Evans, D. (2002). Database searches for qualitative research. Journal of the Medical Library Association, 90(3), 290.

Floridi, L., Cowls, J., King, T. C., & Taddeo, M. (2020). How to design AI for social good: seven essential factors. Science and Engineering Ethics, 26(3), 1771-1796.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and machines, 28(4), 689-707.

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. Computers & Security, 109, 102382.

Gaba, V., & Greve, H. R. (2019). Safe or profitable? The pursuit of conflicting goals. Organization Science, 30(4), 647-667.

Greig, A., Renaud, K., & Flowerday, S. (2015, October). An ethnographic study to assess the enactment of information security culture in a retail store. In 2015 World Congress on Internet Security (WorldCIS) (pp. 61-66). IEEE.

Hagen, J., Albrechtsen, E., & Johnsen, S. O. (2011). The long-term effects of information security e-learning on organizational learning. Information Management & Computer Security.

Haunschild, P. R., Polidoro Jr, F., & Chandler, D. (2015). Organizational oscillation between learning and forgetting: The dual role of serious errors. Organization Science, 26(6), 1682-1701.

Hildebrandt, M. (2013). Balance or trade-off? Online security technologies and fundamental rights. Philosophy & Technology, 26(4), 357-379.

How much does a data breach cost. IBM. (2020). Retrieved November 13, 2022, from https://www.ibm.com/reports/data-breach

Jalali, S., & Wohlin, C. (2012, September). Systematic literature studies: database searches vs. backward snowballing. In Proceedings of the ACM-IEEE international symposium on Empirical software engineering and measurement (pp. 29-38).

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 (IJHISI), 9(1), 42-60.

Kenneally, E., & Dittrich, D. (2012). The Menlo Report: Ethical principles guiding information and communication technology research. Available at SSRN 2445102.

Kenneally, E., Bailey, M., & Maughan, D. (2010, January). A framework for understanding and applying ethical principles in network and security research. In International Conference on Financial Cryptography and Data Security (pp. 240-246). Springer, Berlin, Heidelberg.

Kenneally, E., & Bailey, M. (2014). Cyber-security research ethics dialogue & strategy workshop. ACM SIGCOMM Computer Communication Review, 44(2), 76-79.
Brey, P. (2007). Ethical aspects of information security and privacy. Security, privacy, and trust in modern data management, 21-36.

Khan et al. (2019). Data Breach Risks and Resolutions. Bepress Guest Access. Retrieved November 13, 2022, from
https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1061&context=amcis2019

Kongnso, F. J. (2015). Best practices to minimize data security breaches for increased business performance.

Kwon, J., & Johnson, M. E. (2011, June). An Organizational Learning Perspective on Proactive vs. Reactive investment in Information Security. In WEIS.

Li, L., He, W., Xu, L., Ivan, A., Anwar, M., & Yuan, X. (2014, August). Does explicit information security policy affect employees' cyber security behavior? A pilot study. In 2014 enterprise systems conference (pp. 169-173). IEEE.

Loi, M., & Christen, M. (2020). Ethical frameworks for cybersecurity (Vol. 21, pp. 73-95). Cham, Switzerland: Springer.

Myers, M. D., & Avison, D. (Eds.). (2002). Qualitative research in information systems: a reader. Sage.

Mello, Samantha, "Data Breaches in Higher Education Institutions" (2018). Honors Theses and Capstones. 400. URL: https://scholars.unh.edu/honors/400

Manjikian, M. (2017). Cybersecurity ethics: an introduction. Routledge.

Mattia, A. (2011). Utilizing a learning loop framework in IS security. International Journal of Business and Social Science, 2(21).

Morgan, G., & Gordijn, B. (2020). A care-based stakeholder approach to ethics of cybersecurity in business. The ethics of cybersecurity, 119.

Miller, S., Regan, M., & Walsh, P. F. (2022). National Security Intelligence and Ethics (p. 336). Taylor & Francis.

Omand, S. D., & Phythian, M. (2013). Ethics and intelligence: A debate. *International journal of intelligence and counterintelligence*, *26*(1), 38-63.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07) (pp. 156b-156b). IEEE.

Plachkinova, M., & Maurer, C. (2018). Security breach at target. Journal of Information Systems Education, 29(1), 11-20.

Rathert, C., & May, D. R. (2007). Health care work environments, employee satisfaction, and patient safety: Care provider perspectives. Health care management review, 32(1), 2-11.

Say, G., & Vasudeva, G. (2020). Learning from digital failures? The effectiveness of firms' divestiture and management turnover responses to data breaches. Strategy Science, 5(2), 117-142.

Sen, R. (2018). Challenges to cybersecurity: Current state of affairs. Communications of the Association for Information Systems, 43(1), 2.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. Information & Management, 49(3-4), 190-198.

Van de Poel, I., & Christen, M. (2020). Core values and value conflicts in cybersecurity: beyond privacy versus security. The Ethics of Cybersecurity, 45.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & security, 23(3), 191-198.

Weber, K., & Kleine, N. (2020). Cybersecurity in Health Care. In The Ethics of Cybersecurity (pp. 139-156). Springer, Cham.

Wang, Q. (2021). Three essays on organizational determinants of data breach risk.

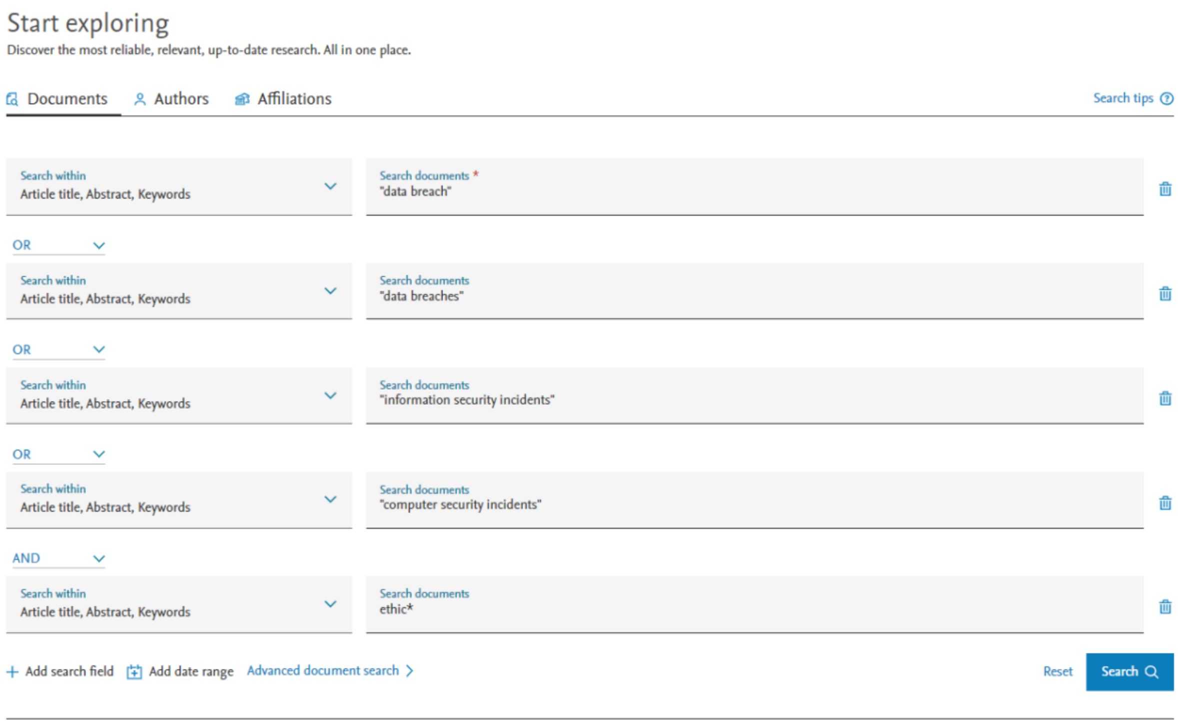
Yaraghi, N. (2016). Hackers, phishers, and disappearing thumb drives: Lessons learned from major health care data breaches. Center for Technology Innovation at Brookings.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. Information Management & Computer Security.

Appendix A

Literature review search

A.1 Practical screen



Start exploring

Discover the most reliable, relevant, up-to-date research. All in one place.

Search within: Article title, Abstract, Keywords — Search documents *: "data breach"

OR

Search within: Article title, Abstract, Keywords — Search documents: "data breaches"

OR

Search within: Article title, Abstract, Keywords — Search documents: "information security incidents"

OR

Search within: Article title, Abstract, Keywords — Search documents: "computer security incidents"

AND

Search within: Article title, Abstract, Keywords — Search documents: ethic*

Appendix B

Interview questions

Ethical and organisational learning from data breaches and its impact on employees' behavior

The following interview questions were prepared for conducting my qualitative research. These questions are divided into different categories to get more punctual answers. Based on these questions, I will follow a semi-structured interview. This can lead to more open dialogue between me as an interviewer and interviewee. The interview will not take more than 40 minutes. The questions in bold are the most important ones as they address my topic directly.

No need for sensitive information and you can skip the question you do not want to answer.

Thematic Block	Questions
About the person and expertise	1. Could you present yourself/ selves and your role in the organization? 2. How long have you been working in your current position? 3. How familiar you are with data breaches and their ethical aspects of it?
During the cyber-attack events	4. How did you know that a security breach/cyber-attack occurred? 5. What were the vulnerabilities? 6. How did the attackers exploit the vulnerabilities? 7. What was the purpose of the attack? 8. Has the attack harmed others? 9. What were the direct and indirect consequences of the attacks (for example, stealing personal information, service downtime, reputation, economic costs, rebuilding a system and website, and so on)? Can you explain further?

Organizational and Ethical Aspects	10. To whom did you notify when you knew about the attacks? What was the procedure? 11. Did you notify people (employees, customers) that might be affected by the breaches? What was the procedure? **12. What is the most essential ethical framework followed in your organization to deal with security breaches?** **13. What kinds of ethical considerations were considered when notifying the security breaches to the affected parties?** 14. How is this ethical framework implemented in day-to-day work especially when data breaches happen?
Organizational learning	15. **How did the behaviours of the employees change after the data breaches**? - **Have the employees submitted to some courses or training**? **16. How did your organization learn from the incident?** **17. How did your organizations change the structure after data breaches based on your learning from incidents?** **18. How did the existing ethical framework influence organizational learning?** 19. Have you updated the incident response plan after the security breaches? **20. Have you revised the ethical framework in your organization after the data breach? If yes or no, why? In what way the existing ethical framework is adequate or not adequate?** 21. Have you experienced other cyberattacks after conducting some changes?
Recommendation/ inter-organisational learning	22. Based on your experience: **a. How do recommend similar organizations to do?** b. **What could be done better?** c. **What is the best thing you have learned from previous security breaches?**

Appendix C

NSD and Consent

Describe the purpose of the project in more detail and indicate the scope of the project.
Briefly outline the project's objectives / research questions
Indicate whether it is a research project, a doctoral thesis, a bachelor's/master's thesis, other student project etc.

If you or others will use the collected personal data for other purposes (e.g. teaching or other research projects), describe these other purposes.

Who is responsible for the research project?

University of Agder
Faculty of Political Science, Department of Information Systems

Why are you being asked to participate?

Participation is based on the organizations that have experienced data breaches.

I have found the person's contact details from the internet and I contacted with organizations directly.

Describe how the sample has been selected (population, selection criteria and how many people have been asked to participate), so that it is clear why the person is receiving this inquiry

If applicable, indicate whether you have received the person's contact details from another (and indicate any approval/permission obtained in order to do this), or whether another has sent out this information letter on your behalf.

What does participation involve for you?

Describe the methods (online/paper-based survey, interview, observation, etc.), the scope, what type of information will be collected and how the information will be recorded (electronically, on paper, sound/video recording), e.g.:

It is an interview; the participant is represented of an organization. In the interview, the participant is going to answer to different groups of questions. It will take approx. 45 min; the answers will be recorded electronically (sound).
I will also share an electronic survey, but it is not in the EU

- *« If you chose to take part in the project, this will involve that you fill in an online survey. It will take approx. 45 minutes. The survey includes questions about (describe the most important questions/topics). Your answers will be recorded electronically»*

If applicable, indicate that you also will collect information about the participant from other sources – such as registers, records/journals, educational records, other project participants, etc., e.g.:

- *«I will also ask your teacher to provide information about you in an interview. It will be information about (describe the most important questions/topics). I will record the interview and will take notes»*

If children will participate, provide information that parents/guardians may on request see the survey/interview guide etc. in advance.

If there are multiple groups of participants, be clear about what participation will involve for each group, or give a separate information letter to each group.

Participation is voluntary

Participation in the project is voluntary. If you chose to participate, you can withdraw your consent at any time without giving a reason. All information about you will then be made anonymous. There will be no negative consequences for you if you chose not to participate or later decide to withdraw.

Expand on this if the person being asked to participate is in a situation where they are dependent on the person asking. E.g. «It will not affect your treatment at the hospital / your relationship with your school/teacher, place of work/employer etc.(..)»

Your personal privacy – how we will store and use your personal data

We will only use your personal data for the purpose(s) specified in this information letter. We will process your personal data confidentially and in accordance with data protection legislation (the General Data Protection Regulation and Personal Data Act).

Only my supervisor at UiA has access to the data, all the data will be locked in a file
I do not want to gather names, only ages and occupations

- *Describe who, in connection with the institution responsible for the project, will have access to the personal data (e.g. the project group, student and supervisor, etc.)*
- *Describe which measures you will take to ensure that no unauthorized persons are able to access the personal data, e.g. «I will replace your name and contact details with a code. The list of names, contact details and respective codes will be stored separately from the rest of the collected data», you will store the data on a research server, locked away/encrypted, etc.*

If applicable, indicate:

- *the name of the data processor that will collect/work with/store data, e.g. online survey provider or transcription service*
- *that persons from other institutions will be given access to the personal data, name the institutions, indicate the number of people and what type of information they will have access to (e.g. whether they will have access to data that can be directly linked to individual participants, or to collected data that has been de-identified)*

- *that personal data will be processed outside the EU (e.g. fieldwork, analysis, cloud computing, conferences), name the institution and country, describe security measures.*

Describe whether participants will be recognizable in publications or not, and to what extent. If applicable, indicate what type of personal information will be published (e.g. name, age, occupation etc.).

What will happen to your personal data at the end of the research project?

Any personal data including digital recordings will be deleted by the end of the project
The project is scheduled to end [20.12.22].
All the personal data including digital recordings will be deleted by 25.08.23

Your rights
So long as you can be identified in the collected data, you have the right to:

- access the personal data that is being processed about you
- request that your personal data is deleted
- request that incorrect personal data about you is corrected/rectified
- receive a copy of your personal data (data portability), and
- send a complaint to the Data Protection Officer or The Norwegian Data Protection Authority regarding the processing of your personal data
-

What gives us the right to process your personal data?
We will process your personal data based on your consent.

Based on an agreement with *[*University of Agder
Faculty of Political Science, Department of Information Systems*]*, NSD – The Norwegian Centre for Research Data AS has assessed that the processing of personal data in this project is in accordance with data protection legislation.

Where can I find out more?
If you have questions about the project, or want to exercise your rights, contact:
University of Agder
Faculty of Political Science, Department of Information Systems via:

Student: Abdulhalim Alhassan abdula17@uia.no telephone: 97373109
Supervisor: Jaziar Radianti jaziar.radianti@uia.no telephone: 98668761

- *[Insert name of institution responsible for the project]* via *[insert name of the project leader]. For student projects you must include contact details for the supervisor/the person responsible for the project, not just the student.*
- Our Data Protection Officer: *[insert name of the data protection officer at the institution responsible for the project]*
- NSD – The Norwegian Centre for Research Data AS, by email: (personverntjenester@nsd.no) or by telephone: +47 55 58 21 17.

Yours sincerely,

Project Leader

Student (if applicable)

(Researcher/supervisor)

Consent form

Consent can be given in writing (including electronically) or orally. NB! You must be able to document/demonstrate that you have given information and gained consent from project participants i.e. from the people whose personal data you will be processing (data subjects). As a rule, we recommend written information and written consent.

- *For written consent on paper you can use this template*
- *For written consent which is collected electronically, you must chose a procedure that will allow you to demonstrate that you have gained explicit consent (read more on our website)*
- *If the context dictates that you should give oral information and gain oral consent (e.g. for research in oral cultures or with people who are illiterate) we recommend that you make a sound recording of the information and consent.*

If a parent/guardian will give consent on behalf of their child or someone without the capacity to consent, you must adjust this information accordingly. Remember that the name of the participant must be included.

Adjust the checkboxes in accordance with participation in your project. It is possible to use bullet points instead of checkboxes. However, if you intend to process special categories of personal data (sensitive personal data) and/or one of the last four points in the list below is applicable to your project, we recommend that you use checkboxes. This because of the requirement of explicit consent.

I have received and understood information about the project *[insert project title]* and have been given the opportunity to ask questions. I give consent:

☐ to participate in *(insert method, e.g. an interview)*
☐ to participate in *(insert other methods, e.g. an online survey) – if applicable*
☐ *for my/my child’s teacher to give information about me/my child to this project (include the type of information)– if applicable*
☐ *for my personal data to be processed outside the EU – if applicable*
☐ *for information about me/myself to be published in a way that I can be recognised (describe in more detail)– if applicable*
☐ *for my personal data to be stored after the end of the project for (insert purpose of storage e.g. follow-up studies) – if applicable*

I give consent for my personal data to be processed until the end date of the project, approx. *[insert date]*

(Signed by participant, date)

Appendix D

Interview extracts

Interview extract MelonDB

Thematic Block	Interview extract	Coding
About the person and expertise	MelonDB had a significant breach in 2019 with a cyber-attack. That is basically my experience. We have noted an incident of the same magnitude and other smaller incidents. I can say that my experience is back to 2019 in this context.	Incident management

During the cyber-attack events	When taken down by a ransomware attack, unfortunately we did not discover that until the encryption of our files started. This happens on several thousand PC's and several hundred servers during the night of – and - . After that, it immediately affected our IT infrastructure. When we discovered it, we understood that it was a cyber-attack. So, we immediately started turning off connections in the network and shutting down our servers to prevent more damage to happen.	Ransom attack Incident response
	We learned that the attacker breached our infrastructure three months before the encryption started.	Exploiting the vulnerability
	The initial attack factor was a phishing email. It looked legitimate. Clicking on the link introduced malware to the computer. The malware did not have an updated signature on the antivirus. The antivirus signature was updated a few days later. It was already too late in this context	Ransomware attack by phishing
	The initial attack factor was a phishing email. It looked legitimate. Clicking on the link introduced malware to the computer. The malware did not have an updated signature on the antivirus. The antivirus signature was updated a few days later. It was already too late in this context. So, when the user clicked on the link, this affected his computer. Then, the attacker(s) got some software, and our system was unable to discover it, and the attacker(s) was able to connect back to the command-and-control centre on the internet. So, the attacker basically removed the control over what was happening on the PC and jump into a new system.	Patches Control the system
	Phishing and installing nasty tools to do the literal move. The (start tools) could read passwords in the directory system. These tools are not really visible in the file system. The tools used by the attackers call to map and understand the full infrastructure and use the information to automatically plan a place for the ransomware because ransomware is a separate virus that they put on a distinct system as a last stage of the attack.	Boot to control the system
	The purpose as we believe had purely criminal and financial motivation. The attackers wanted to require a ransom and decrypt the encrypted files.	Purpose of the attack
	Not that attack, but the same criminal actor was behind a series of similar attacks on other companies during the first half of 2019	Previous attacks for the same actor

	Financial impact which we have reported extremely. It is now up to 800 million Norwegian crones. There is also an operational impact. When attack happened MelonDB lost access to the IT system that we use to operate our plans The impact was not on the production of the upstream business. In the downstream business, we have a lot of smaller plans around the world. There, they lost IT systems, they also lost visibility about which product is going to be produced to which customer including orders. Production for these units jump down to 67% for some plans. It took about one and half months to come back to its rate again. Regarding the IT perspective, we had a recovering project that lasted for three months, and all our IT people and suppliers worked only on recovering the IT system. Regarding the reputation risk, we were open about the situation and transparent to media. We did not see that our stock markets decreased based on this. We got quite good feedback from the market about this openness. So, MelonDB did not lose its reputation from this breach. On the high-level statement, we realize that the framework we had was not enough to tackle the risk today. Now, we are preparing for the situation again that led to significant changes regarding the control framework and the way we monitor and follow up how the organisation is really implementing the security requirements.	Extreme financial Impact Operational impact Downstream impact The impact of IT loss on the production Reputational risk Transparency Control framework

Organizational and Ethical Aspects	First reported to the police. Since there are also personal data, we have also informed datatilsynet (Norwegian Data Protection Authority) that cooperate with other countries. National security agency in Norway. MelonDB is a part of the national critical infrastructure. We have already informed them.	Cyber-security authorities
	We communicated heavily and internally about the situation. Luckily, when we talk about personal data, we only talk about usernames and passwords, that category of personal data. We did not really have sensitive data.	Internal communication Personal data
	The data itself was encrypted. The encrypted files saved in MelonDB. The attacker did not take out or leak any information out of MelonDB. We could assure to our employees that none of their sensitive data have been compromised. It is only about usernames and passwords that attacker may use to make an attack on MelonDB. However, it did not affect our customers either.	Data exploitation
	In MelonDB, we have coral conduct which sets standards for how MelonDB employees should behave. This sector addresses corruption, fraud. We also have elements of expectations of the employees in terms of safe behaviour with IT systems, for example, clicking the links of the emails and phishing. So, the coral conduct is covering all the aspects of the employees' behaviours. If this is being breached, the company will do a reaction.	Ethical framework Employees behavior with IT Ethical impact on employees' behavior
	When the incident happened, regarded our crisis management team, at six o'clock in the morning, the crisis team was basically the top management on the table including SISO and CEO. The whole company was mobilized instantly to manage that situation including the corporate emergency team because we have procedures for managing crisis.	Crisis management team
	You can call it ethical framework, but in security, we are talking about control framework. We are strengthening our cybersecurity capabilities. In cyber-security, we often talk about controls, we use for example "The ISO/IEC 27000" as a control framework, then we put this control out of responsible (donor) and regard them to document that comply with the requirements. In addition, we check and verify in implementing in the security side.	Control framework Documentation

Organizational learning	We have been communicating, doing mandatory training. We have talked a lot about phishing, risks, social engineering and how attackers constantly trying to get information about individuals or the company to use that to make people click on links or read documents. So, the behaviour change is really enormous especially how to read the phishing emails and report them.	Mandatory training Employees' behavior change
	We have also sent false phishing emails to get people click on the link, if they do, they get an educational video about how they should behave.	White hacking Disscussion
	We have learned a lot. Immediately, we did strengthen the security especially from the technical side, but on a longer term, we have also had an important discussion about management. We have seen that this is a risk must be reduced. So, we have been building a multi-year cyber response program to support our capabilities to manage cyber-security risk. That leads to organisational change because we get stronger mandates, we build a capacity in security function, we get more people on board, technical and operational level, and more competence	Organizational change Organizational Improvements and procedure
	The whole structure is not changed. We have target operating model for IT. Security is a part of this model.	Structural change
	On the high-level statement, we realize that the framework we had was not enough to tackle the risk today. Now, we are preparing for the situation again that led to significant changes regarding the control framework and the way we monitor and follow up how the organisation is really implementing the security requirements.	Control framework changes
	We have established a **cyber crisis team** reporting to the cooperate emergency team. So, we have organised quality, IT and security resources in a structure way. We did not have that before. Now, we have organised the incident procedures. As soon we have a risk, we get this team and start to manage the situation not only in the breach situations.	Cyber crisis team Crisis management
	However, we have prepared ourselves for other potential incidents and vulnerabilities, but we have seen an incident or a risk yet.	Readiness for similar risks
	Cyber-security framework and control framework. We have revised it once. However, we are in a change, so we want to do a new update.	Up-to-date framework

	(Even after data breach) We have experienced hundreds of cyber-attacks every day, but we are stooping them without having impact. We have had a few incidents like compromising, but we were able to stop them before they damage. The whole team of the crisis room in the company agreed that we should not go with any discussion with the attackers or pay any ransom. Besides, we have had our backups of the data that were not destroyed in the attack. We were very confident after few days that we could actually bring back and retrieve the encrypted data. Therefore, we did not need to evaluate being ransom to the attacker(s). Thus, we did evaluate paying the ransom for ethical reasons and for not needing for that.	Cyber-attacks Ethical approach in handling crises Backups

Recommendation/ inter-organisational learning	Having the technical level in place. Those companies which do not have this in place, they are still being compromised for ransomware attacks. My advice is that you assess cyber security capabilities in a moralistic view and discuss of course with management if they accept the risk or not and if risk within cyber is not accepted then that you raised investment on the program to strengthen cybersecurity capabilities and by doing that you also reduce the risk.	Technical level Cyber-security management Investing in Cyber-security
	Building cyber security capabilities could be better. It is a long journey because it's about organizational change.	Building cyber security capabilities
	We have been using the "bow tie level". This is basically on one side you look at how can you reduce the probability of an incident happening and an incident happening that's in the middle and then on the other side that's more about reducing the impacts.	Risk assessment (Bow tie)
	The point is that of course first the risk reduction by reducing the probability for an attack to happen. This is much about technical barriers and so on.	Technical barriers
	We prioritize rapid risk reduction first in terms of taking down the probability that we will be we will have a breach and then and I looked at that stuff we could go more into this reducing the impact.	Prioritization
	I think this practical experience help people to understand what this cyber risk is about. Talking about cyber-security risk is very intangible for people. I think the best thing for me is that people now understand that this really can happen and if it happens it has consequences that you lose your IT systems for months.	Practical experience in Cyber security Understanding Cyber security

Interview extract OrangeDB

Thematic Block	Interview extract	Coding
About the person and expertise	I have been familiar with the data-attack since last year.	Cyber-security Awareness
	Before, I was not familiar with this. I have not had experience with the data-attack/cyberattack until last year, nor with ethical aspects. Since last year, I worked a lot with laws and regulations. Now we respect them and know what rules apply and all these types of things.	Data security Practice Cyber laws and regulations
During the cyber-attack events	It was not that difficult because absolutely everything stopped and a message and demand for ransom virus came up on the screen. Demands for money appeared. We did not have access to our own systems, so it was not difficult to confirm that it was a cyber-attack.	Ransom attack System is down
	We know but I cannot say since it is under police investigation. In general, the security measures we had were not strong enough to cope with the attack that came, but technical details I cannot tell about.	Confidentiality
	It was in a way a consequence of the data attack and there was later a data leak in the dark web because we did not pay, and it is simply a violation of privacy legislation.	Privacy disclosure
	There was stealing of personal information as I said, there was data leakage later. There was also service downtime on all services over many months because we cannot recover everything at once.	Consequence of the data breach
	There were also reputation costs for our reputation. There were also large financial costs. That is about 40 million to restore the entire municipality again.	Reputational damage

Organizational and Ethical Aspects	We have notified all the relevant authorities, the Norwegian Data Protection Authority was one of them, the national security authority was one of them, the police were one of them and the National Center for Cyber Security was one of them We have done this with the employees. We gave information for the employees immediately and irregularly. As for the inhabitants, we have also informed in various ways. first contacting the Media so that we could be open and honest in the media and notify all citizens. Later, we got a better overview of the scope and problems; We have written and sent SMS to all residents. All experience shows that in such cases when you pay you only get a new claim a little later and more money and you are blackmailed time and time again. The whole world knows that such criminal actors work. There are also rules that describe very well what should be done, who should be informed, and who should be reached. We have done this after the cyber-attack, and we are also engaged specialists in the field to help us. We have notified our citizens that the cyber-attack took place. Data may be available online, but we did not know we were just notifying that it might be possible. Later, when it happened, about two thousand files were available online. These 2000 files identified who affected each and then we have made direct contact with every one of those affected. We also had a dialogue with all companies that have a relationship with our municipality. We have software with technical documentation on our servers. It may be that their technological secrets could be taken by the trosector. We have changed our work processes by buying a new system, upgrading a system, and making changes at the technological level. We are going through a process that takes care of privacy assessments, risk analysis and security analysis that is a third party that we do not do. We have employees who have more security expertise and privacy expertise. Now, we are very careful with that type of work. We practice now a zero-trust principle.	Cyber-security authorities Transparency Prioritization Ethical cyber-security Administrative controls: Policies Procedures Processes Ethical framework Dark web External Communication Communication to Stakeholders Risk management Cyber-security controls and measures Cyber- security requirements: -Process changing -Privacy assessments -Risk analysis

Organizational learning	Our employees have helped the IT department and they have helped us through being patient instead of complaining that nothing works. They have been patient, they have waited, and they had a calm relationship.	Employees' behavior after data breach
	We notice is a little different because now the employees are more suspicious and cautious. They ask more. They ask for more confirmation. The email as an example, you see that there are many different scams on emails and text messages. There has been more awareness.	Personal consequences of data breaches for employees
	One was the IT department that worked IT operations, security privacy and that kind of things. The other was an innovation department that worked on project work. These two units / departments / are now gone. They ended and a completely new unit was formed, all the employees who worked in the IT department no longer work with us.	Structural change Technical improvements
	They are no longer at work because our director has chosen to outsource IT operations to an external company. Now we do not have an IT department with us internally. Our IT department is now a company out there that we pay for to run our IT systems.	Layoffs
	the incident response in relation to the data attack last year does not fit well with this current risk that will come from Russia in relation to Ukraine.	Incident response
	It is feared that data-attacks may occur in Norway, but the type of data attack that is expected is not the same as what happened to us last year.	Proactive cyber-security measures
	Yes, we have revised it, not just once, but we have put in our quality system so that such a reassessment takes place regularly. Since the computer attack last year, we have already revised it twice, soon we will go on the third. Such revising is a part of everyday life.	Ethical framework revising
	The three major areas that we experienced more difficulty or more to learn from are interaction, information, and communication. While the systems are down, it helps little to say that we have teams.	Challenges during crisis

	We have ordered a report with recommendations and any municipality should do to avoid what we have experienced. We need technical systems that detect vulnerabilities that tell us what kind of security holes we need to fix, but we also need expertise to be able to understand the seriousness of the situation and we need a capacity to handle the situation and where the complexity to be more aware of and that is what enables us to better cope with such situation.	Documenting the fails The need for new technologies and experience

Interview extract KiwiDB

Thematic Block	**Interview extract**	**Coding**
About the person and expertise	I am familiar with the breaches in the department zone we have had, we are also very driven by the GDPR and privacy legislation that came into force in June 2018. When we acquired the new system and other systems we have negotiated and signed data processing agreements with the suppliers we have received since 2018. With the work and everything related to data storage, data sharing, insight into personal information and deletion of them and that you should only store the information you need to get service performed, I am well acquainted with, but more theoretical and not much practical.	Cyber-security Awareness Cyber laws and regulations Data processing

During the cyber-attack events	One day, we noticed the website was down. The site has been unstable for two days. There were problems with the form for registering users, and links on the Main Page were not clickable. The site showed errors when we opened it. There was a vulnerability in a plugin used by the website. The website is WordPress-based and contains several plugins. The website has been in use for more than four years. The plugins have not been updated in a while. We have plugins for arrangements, comments on social media, newsletters etc. We are uncertain which plugin contained the vulnerability. The newsletter and comment function were the one that we considered to have gone astray so that unauthorized persons could retrieve a list of newsletter recipients and not least e-mail addresses and names that have written their names on those who have commented on various articles on the website. We have immediately deleted it and sent an email to anyone with a request to change the password. Be aware that their email addresses may not have gone astray and may be used for spamming. IF you suddenly experience that you receive so many unwanted emails, it may be that unauthorized persons have obtained email addresses from the newsletter list integrated into the website. Therefore, we have deleted and deactivated. First, I have sent a message that this has happened to all registered email addresses, around 2000 addresses that have been notified of the episode. Another weakness, but we do not know if it was exploited or monitored, those who have entered the site could monitor activity, but we do not know how long and at what times. Those who have used the website to log in to "MinSide" for the system could an unauthorized get what has been typed for a username as a loan number and they could also see which password they have used but it was known in the form of star points. Therefore, we have reset all passwords in the entire library system and sent SMS and email to all registered users that they should create a new password to the system as approximately 70,000 persons, the biggest work was to reset the system users' passwords and they were given a deadline to make a new one. We have done this for security reasons to be 100% sure that everything that has come on our website will reset, delete and start from scratch.	System is down Plugin vulnerability Nonupdated plugin Proactive procedures Cyber-security warning Post-hack steps The possibility of authorization Notifying the users Resetting the system

	The attackers gained access to a kickstart file and used it to access a backup of the website. The backup contained the user credentials of nine website administrators. Additionally, 40 people who had commented on the website had their email addresses leaked.	Access tool
	We cancelled the newsletter immediately when we detected the attack because the attackers may have installed JavaScript on the live website to gather login data on the website visitors.	Precaution procedure
	For a while, we have had a temporary page, WordPress-based, but not a single plugin website.	Finding solution
	We signed an agreement and launched a new website that is integrated with the -- system and which covers the GDPR agreement with the – system.	Advancing the service
	Costs: Website 120,000, Personnel costs 100,000, but we have got a nice website that is integrated with our -- system on profile.	Financial loss
	Reputation was not ruined by that episode, on the contrary, we have received a lot of support.	Reputational impact

Organizational and Ethical Aspects	We have notified in the order: Privacy Office, Datatilsynet (The Norwegian Data Protection Authority), system provider and our users.	Cyber security stakeholders
	We have sent SMS to be sure that nothing can go wrong. We did not notice anything afterward, for example, no one came to us to complain about anything due to hacking. Only a few asked us to delete them from the system.	Users' reaction
	We have internal courses, and internal training that has privacy and security, we also have regulations that we follow: reporting, handling, and crisis management in such cases well prepared in our municipality. We also have something called security week every time in October, so privacy is focused on.	Internal training Crisis management
	All employees have taken that course both after and before the episode incident with us, how much is involved in knowing spam, phishing methods, secure passwords, locking screens, and lock tests when they are going out. We take privacy seriously.	Obligatory courses
	Initially, it took us an hour to initiate action. That is, the killed newsletter module destroys it, disables it, removes all email addresses, and sends an email that they should be aware that their email addresses could practically go astray. We have immediately disabled all administrator accounts and asked the administrator not to use the page to log on. They have removed it quickly from the domain shop's pages. The next day we have also been on a secure connection with a simple HTML page with information for all users about what has happened.	Removing the risk Informing the users via webpage
	24 hours after the attack, we went out with open information for everyone. Think the most important thing to do when we talk about ethics is that one should not try to hide this and that one should take it seriously and try to diagnose, the extent of the damage and repair it not least reset everything.	Transparency
	We have also informed the similar organizations to use the same solutions, one has had weaknesses with plugins, some more security measures were taken from servers. We thought that WordPress with these plugins would again run a risk of poor maintenance both centrally and locally.	External communication and learning
	All employees have become more aware after the incident especially regarding processing of data with password, log in. We have had to be very strict for some of our users who are not digitally good. You are not Norway's bank!!	Cyber security awareness

Organizational learning	All employees have become more conscious especially when we were to buy a new service (our new website), one must learn how to store data. This has a high degree of certainty that the data stored in Norway on Norwegian servers of the Norwegian system supplier in Larvik and is processed only in the form needed. Everyone has been required to take a privacy course, mostly an online course that must be completed. More awareness of what to do when on duty. “Never forget to leave the PC before the screen is locked, do screen sharing, remember to stop it when you are done so that no personal information will be shown to unauthorized persons”. We have secured the public area so that no personal information will be shown to unauthorized persons that no one can attack the server of the municipality. We have both taken internal rounds and secured the network even more. We have reminded several times how important it is to secure a PC, change passwords often, and do several things in practice. All our cloud services are on SaaS. That is, those operations will not be held by suppliers once. We have learned to think a little more and to be aware of what can go wrong, to check carefully, to make sure that our requirements for the creation of new systems and services and to take this with privacy and storage of personal data of data in in line with the regulations. The crisis management plan is in line with the municipal plan and the privacy representative. We have an information security manager in the municipality. We also have a system manager and system owner-managers in the municipality who must all be involved in the process if this is how the incident occurs. It is defining the extent of the damage, who is affected, and notifying the data audit and several actors involved to ensure the least damage. We have received a new handling plan after the GDPR came into force in 2018 in addition to two-factor authentication access to its services, PCs, and email before entering the system. It has been introduced to increase the security rate significantly. Good plans existed before the incident and the same plans were revoked after the incident, but the general threat picture we see in Norway and other countries means that one must constantly	Employees behaviour Data protection /process/ Privacy course Securing infrastructure Data protection platform New awareness thoughts Crisis management Responsibility order GDPR

	work with plans, security methods and awareness for all employees. This is something that changes continuously.	Security methods

Recommendation/ inter-organisational learning	The best thing, I think we have done everything right and we have also received from datatilsynet that we have handled the situation well. The first thing we have learned is not to use a WordPress page with many different plugins or third-party liver doors. ○ Follow the regulations ○ Have a dialogue with the information security manager in the comment or privacy representative ○ Inform all involved actors and the audience ○ Report to the data audit ○ Work actively and continuously ○ Put privacy and security first	Situation handling Learning from flaws Recommendations

Interview extract PineappleDB

Thematic Block	**Interview extract**	**Coding**
About the person and expertise	I'm quite familiar with it. There was somebody else in the organization that handle it at that point. This person has quit working in PineappleDB. We had the information security officer that was handling it.	Cyber-security Awareness

During the cyber-attack events	One morning, we were informed by the people working in this area that when they logged onto the system, they just got the message up on the system. They understood by the way that it had been attacked. So, they contacted the information security officer in PineappleDB that is a part of my organization.	Detecting the attack
	First, this happened too to this organization unit called “Vann og avløp” “Water and wastewater” This had its own data center and at that point was not part of the rest of the IT community in PineappleDB. They were not included in the IT department until the incident. After that, IT took the responsibility for “vann og avløp” The impact for what happened was that when we realized that they had been hacked, we contacted Atea (consulting company), as we have a subscription with for that incident response team, so we contacted them right away and they started working on the case immediately.	Post-attack procedures Area attacked Consulting company
	This was a server that had access to the Internet, and I guess it was updated with the last updates from Microsoft, so it was exposed to Internet. The server was exposed, the vulnerability was from the server, and they exploited that.	Incident response team Server vulnerability
	Reputation of course and financial consequences including rebuilding a system through backup, but no personal information was exposed.	Cyber attack consequences

Organizational and Ethical Aspects	We contacted the IRT team, set up a task force in the municipality, and we contacted and reported it to the police datatilsynet, “the Norwegian Data Protection Authority”, and “National Cyber Security Center”. We also contacted “Atea” we're using them as consultants we have a frame agreement with Atea when they come to technical consultants.	Cyber-security authorities Stakeholders
	There were no customers that were affected. There were no suppliers that were affected. It was only internal personnel that was affected, and they were affected in a way that they were not able to go in. This was a monitoring system where they could follow a different thing. So, it was no part of the production, but it was a portal where they could follow what was going on in the production.	Cyber-attack impact
	They had to send old people to the different production sites and people were following it at the production. It's a kind of service downtime but only internal and it did not affect the water supply or the product or the water supply. It was more for the internal office people that they were not able to do the monitoring, so they decided to send people out to the different production sites and until we were able to rebuild the system or the server, we had people on sites.	Finding solutions after the service downtime
	We have operational security board that meets every Monday. Since this episode, this unit of the commune has been a part of that security operation board every Monday. We have taken steps to secure this part of the of the system so now they're part of the IT organization and they and they follow all the processes and procedures from IT.	Administrative controls: 1.Policies 2. Procedures 3. Processes
	We have also started our internal program for older employees “nano learning” so every week we've had a session that we send out to all the employees but when it comes to nano learning, so we have different topics. Is it called nano learning? Yeah, nano learning by jungle map. So, we have different topics like for three or four weeks and then once a week we send out lessons that are part of that topic.	Employees’ learning
	We've been doing this now to make sure that the organization or the thousands of employees are more aware of the risk that people can try to know how to take care of password make sure they don't open any links and all those things. Thus, we have a one-year program going now, so it's a kind of course like 5-6 minutes once a week. We were very open about that. First of all, we reported it to the police soon after that to the National Security Board we	Cyber-security awareness

	posted it on our Internet homepage and we were open about it when journalists contacted us, different newspapers. So, we were very open. we've also been a part in different conferences and seminars where we also have talked and gone more into details about what happened including technical details.	Transparency External Communication
	That's handled through our quality reporting systems where we have risk analysis at different unit levels. In PineappleDB, we have a quality reporting system where regularly the different units have to do risk analysis. We have also ethical issues that is one part of it. That's something that set in a system from the quality report team or the audit team. We have a quality audit team in PineappleDB, and they address this frequently.	Quality reporting system Risk assessment

Organizational learning	This was only affecting a small group of people maybe 15 to 20 people in the organization. Of course, when it comes to those people, they are now more aware of all the risk and the impact what could have happened.	Cyber awareness
	Regarding the other employees, I think the behavior has changed because of nano learning. We are doing once a week. I think that's where the change has come and that's what we hold. So, they have become maybe more cautious. It's nano learning as the purpose of nano learning is to make all the employees more cautious by going through this 5-6 minute a week awareness program.	Employees' behavior after data breach
	Every Tuesday morning, they get this little thing in the e-mail as a new session or a new learning. Besides, we did have a normal course of information security for all the system owners. PineappleDB has about 250 different applications or systems and each system has a system owner. We have about 80 to 90 system owners.	Course and learning
	We've also had one course for them when it comes to information security like 1/2 a day course and we're also planning a two-day course for all those people in the area of information security, and we have an external we will have an external consultant that's conduct a two-day program within that area of information security.	Information sharing
	The former information security officer in PineappleDB has taken a certification within the security area. He was in Germany for a ten-day course for years and so it was an admitted course. We are now hiring consultancy from Atea that also has all these proper certifications.	Course and certifications Learning abroad
	We were open about the root cause we were open about how we handled it. We have taken a lot of steps to avoid it in the future like I said this this unit is now a part of the IT organization. They are part of the operational security board every Monday.	Transparency Proactive cyber-security measures
	We subscribed to different things to be updated on all the modifications and all the all the awareness programs around us. We subscribed to NSM security board. We subscribed to something called "health set" that they're doing scanning for us all the time. So, we have taken a lot of steps in the last year and a half to avoid this. We have changed the structure like I said the unit that used to be on its own no partner is now a part of the IT organization.	Subscriptions to new technologies

	I would think it affects the organizational learning as the whole organization with different units has to go through like I said risk workshops and things like that. The incident response plan is being continually updated because we get new systems, and we get new applications etc. So, we have a plan how to respond to different types of incidents. That's the plan we have together, so by lost in service from IT, for instance. We have a plan that has 10 to 12 different scenarios and how we respond to them. We have also done business impact analysis for all the systems. In this situation, we have an analysis that's updated all the time and how we respond what's the important things and where we start. We are also doing practical training in this context that we have different scenarios and how we respond at them.	Structural change Risk workshops Incident response plan Practical training for different scenarios

Recommendation/ inter-organisational learning	Many of them are still in the situation that we used to be where this area of “water supply” “vann og avløp” that they are living their own lives and not being part of the of the rest of the organization. I think the changes we've done now they're a part of a large professional department or a large professional unit. However, a few communes in Norway are still in that situation where their “water supply” units have their own IT or data that are outside the rest of the organization. We have attended different workshops, seminars, and conferences where we have been very open about all this. I think other organizations can learn and are learning from our experience because we are being contacted by different organizations about this. “Water supply” should have been implemented in the rest of the organization that they should not have been in their own unit, but they should have been a part of the rest of the IT system.	One IT unit External learning and communication

Interview extract GrapesDB

Thematic Block	**Interview extract**	**Coding**
About the person and expertise	Very familiar as it is a part of my job	Familiarity
During the cyber-attack events	I would go through monitoring systems and getting alert when an event/incident occurs. SOC team would be one of the first ones to know and alert the correct people. My answer here would be to look at Owasp top 10. Those vulnerabilities are very relevant and realistic. I do know that phishing is one of the most attractive "exploits" that is very efficient and still used. I can personally say that there have been several phishing attempts towards me which I have managed to avoid. Without disclosing any information, I also know that mismanaged access control list (ACL) has led to a successful attack.	Cyber-attack alert Common vulnerabilities Cyber-Attack tools

Organizational and Ethical Aspects	The moment the attack has been discovered; certain roles will be alerted to start the incident response plan. Those are the incident response team, CISO, The management team etc.	Notifying stakeholders
	Notification of customers happens after a certain amount of time. I cannot speak on behalf of the companies I work with, but usually companies do not notify immediately. They try to find the breach, its reason, and its damage. Once all information has been gathered, then the affected companies/customers will be notified. I do not remember the exact amount of time a company has before they notify, but there is a law for that certain situation that states a company must notify about the attack and who has been affected by it.	Notifying customers
	Organizations I have worked with, use ISO standards which includes many aspects if not all how to run a company. In addition, The NIST framework with alignment to GDPR are also implemented. Lastly the NSM basic principles. All those combined is what makes essential to operate both secure and ethically in my opinion.	Ethical standards and principles
	The frameworks I mentioned in question 12 are implemented throughout the organization on every level. There is no difference in implementation of the frameworks. These frameworks are supposed to help you prepare and know what to do when breaches happen, or the organization should operate. Meaning if something happens and the organization does not follow their plan or does not have a plan, the framework has then not been implemented correctly and needs to be revised.	Benefits of the frameworks

Organizational learning	It depends on the employee's role and position. An employee of incident response team would not change behaviour but rather focus on the incident and how to handle according to the book/plan. The first time handling an incident might be a bit overwhelming, but the training and practise the companies do regardless of having an incident or not will prepare the employees for these situations.	The importance of employees training
	All employees must go through security courses. I have seen several companies give security courses and educate their employees about security and the importance of it. From the top of the chain all the way to the bottom, including people who work in building cantine.	Security course
	Organizations usually focus on the 7 steps of incident response. After recovery, usually they would follow up the incident to see what happened, how and what could've been done to prevent. for example, if it is a phishing attack. The organization would make sure to educate the company by sending every to a course (which happens annually anyways). If it is a zero-day vulnerability, the response would be to patch it ASAP. It all depends on the type of attack.	Incident response plan
	The framework I have mentioned if implemented correctly should give the whole organization proper knowledge on security, ethics, goals, policies etc. The whole organization would be on "the same page".	Cyber security requirements
	Incident response plan gets reviewed and updated regardless of a breach or not. Most organizations do it annually unless they see the need to implement/update something right away. If the organization sees the need to update the response plan due to their response not being sufficient or efficient enough during the breach, then that would happen yes.	Updating incident response plan

Recommendation / inter-organisational learning	I would recommend all organizations (small or big) to have proper Information Security Management System (ISMS) and try to be at the very least aligned with 27001 standards. The ISO standards covers most if not everything an organization needs when it comes to security. IF that standard is too big for the company, then I would recommend NSM's assistance, they have one that is based on NIST, ISO and other well-known frameworks/standards in the world which fits for smaller companies. just to be clear when I say iso 27001 standards and ISMS, that includes, policies, procedures, incident response etc. I would say that’s where organizations will find out what could’ve been done better to avoid these situations in the first place. my personal recommendation would be to stay updated, learn from others, do not think you won’t be a victim of an attack, and always have the mindset of an attacker (what would I do if I was him). I have learned that communication and right attitude is key. Do not focus on whose fault is, but rather how can we solve this, later what could’ve been done to prevent, lastly find the cause and make sure it does not happen again. I have experienced that some organizations focus mostly on whose fault it was (so they could point the finger) instead of handling the situation (not only about breaches but security in general).	Information Security Management System ISO standards Stay updated Communication Disc

Interview extract CherryDB

Thematic Block	Interview extract	Coding
About the person and expertise	I am Dr.-----. I had a Ph.D. degree in Electrical and Electronics Engineering (speciality in data security) from Polytech – Nantes / France. I am graduated from the faculty of engineering / Lebanese university in 2009. I had a master's degree in network and telecommunication from Saint-Joseph University. I am working in the field of Cybersecurity since 2009.	Researcher role
	I am so familiar with data breach, and I have a great experience in data security. I heard about the ethical concept in cybersecurity, but I didn't go deeper.	Familiarity
During the cyber-attack events	We will receive notifications that our data offered for sales in the dark web. Also, we noticed sudden changes to our critical infrastructure or system passwords and accounts.	Knowing the security breach
	Mainly it was a Human vulnerability. A person clicked on a suspicious link in a phishing email.	Vulnerability reason
	Using social engineering techniques, the attack gained unauthorized access to our system and exploit the vulnerability using a malicious software.	Exploiting techniques
	The purpose of the attack was to control our computer systems and to steal the data held within our databases.	The purpose of The attack
	The consequences of the attacks were mainly stealing personal information and service downtime.	The consequences of attack

Organizational and Ethical Aspects	If we quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused.	Proactive cyber-security measures
	The most ethical framework followed in our organization to deal with data breaches is the rights-based principle that is influential in the law. we adopt the “design privacy” approach and we update the “Audit algorithm”	Ethical framework
	While privacy is a key topic in any ethical analysis of a data breach, other issues are more pressing, such as the responsibility of organizations to prevent and to repair consequences of data breaches.	Privacy
	Based on our ethical approach, we built trust and transparency with consumers and citizens, which be part of good information governance, as a means of maximising the value of information derived from data analytics while minimising risks. To take additional steps to safeguard consumer privacy, ethics would certainly suggest that businesses should voluntarily adopt higher standards for data protection.	Transparency

Organizational learning	After the data breaches, the employees have been trained. They participated in many courses related to cybersecurity such as Information security awareness, Data protection, Cyber first responder and others. Also, this effective behavioral change program was carried out an audit of existing practices.	Employees training
	The employee’s security behavior has been changed after data breaches including how employees handle their passwords, how employees interact with organizational data, and how employees use network resources. User awareness about the laid down information security policies and greater policy visibility encourages compliance with security policies.	Employees behavior Employees’ awareness
	After data breaches, the organisation specified the critical elements that cybersecurity team must learn from the incident and look into before influencing behavior:	Organizational learning
	● Design and deliver impactful security education, security awareness training, and overall security awareness.	Security awareness
	● Seek to understand the critical factors that influence the security choices made by employees.	More understanding of C A
	● Design and develop systems and apps and processes and the physical environment that helps to account for user behavior.	Architecture
	● Develop metrics to help to measure behavior change and to show the return on investment (ROI).	Developing ROI
	The organization design and develop robust and human-centred security programs to address and reduce the number of incidences associated with poor employee security behavior.	Security design

Recommendation/ inter-organisational learning	Information security awareness refers to employees' overall knowledge and understanding of potential information security-related issues and their ramifications, and what needs to be done to deal with security-related issues. The creation of human-centred security awareness programs will prove to be the tipping point in ensuring top-notch security for your organization's networks and data. A good security education program acts as a deterrent, but it must be ongoing for effective deterrence. To improve information security in an organization, more than just simple awareness is required to change employee security behavior effectively. The ideal program helps to build synergy between departments to understand the prevailing state of security behavior fully. The organization will then more to allocate more investment to help address the identified risks. we learned that we should have a clear policy inside the organization. Also, we learned that the security team must be empowered enough to run their programs but remain responsible and accountable.	Cyber-security awareness Cyber-security Education Prevailing Cyber-security behavior Investing in Cyber-security Organizational policy