UiA University of Agder

Master

Ethical Frameworks in Organizations for Cybersecurity

An exploratory study on Ethical Frameworks adopted by Norwegian organizations for cybersecurity

Robert Zakariassen & Daniel Mikkelsen

SUPERVISOR

Devinder Thapa & Nadia Saad Noori

University of Agder, 2022

Faculty of Social Sciences

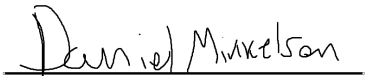
Department of Information Systems

Acknowledgements

This master thesis is a completion of the master's program (MSc) in cybersecurity management at the University of Agder (UiA). The master thesis was conducted by two students that had multiple courses in ethics within cybersecurity where they found interesting topics which were not heavily researched on before. The purpose of this study was to find out what types of ethical frameworks were used for cybersecurity, and what type of ethical frameworks were used by organizations for cybersecurity in a Norwegian context. Additionally the research is used to help raise awareness around ethics related to cybersecurity and how this can help improve decision making in an organization and reduce the mistakes that the employees make.

We would like to thank our advisors, Professor Devinder Thapa and Associate Professor Nadia Saad Noori at the Department of Information and Communication Technology at UiA for providing good feedback, guiding us in the right direction and encouraging us. We would also thank them for assisting us in creating a topic and taking us in the right direction in our research. This big research project would not have been possible to complete without the help that we got from them. Lastly, we would like to thank all the interviewees that contributed to the interviews and decided to share their expertise and knowledge regarding the topic.

Kristiansand
3rd June 2022



Daniel Mikkelsen

Robert Zakariassen

Abstract

Cybersecurity is of critical ethical significance, because cybersecurity technologies have an important impact on human well-being as they make possible many contemporary decisions, which affects the human organizations that rely on the accessibility and integrity of data and computer systems. In cybersecurity it is important to have ethical principles and guidelines which are effective. The reason for this is that cybersecurity has a critical impact on ethics, since cybersecurity technologies have an important impact on human well-being as well as ethical trade-offs and complex moral issues, such as whether to pay hackers or not. There are a lot of ethical issues raised by cybersecurity such as what type of sensitive data to keep and what to remove, paying ransomware or testing and deceiving the employees through social engineered testing. Therefore it is important to choose an ethical framework that helps solve those issues. In this master thesis the researchers try to address what type of frameworks are used for cybersecurity and which framework should different Norwegian organizations choose to implement for their organization. The thesis will also use interviews to achieve and find out what ethics organizations use, by using a list of questions through semi-structured interviews, which are based on our research questions, and what was discovered in the existing literature. Furthermore, the researchers examine the different ethical theories that the frameworks are based on and what the differences are in those theories. The research outcome will help to choose what type of framework the organizations should choose when it comes to their ethical issues, dilemmas and values. The three main frameworks that were examined are the principlist framework, human-rights/right-based framework and Consequentialist/Utilitarianism Framework. The study uses a qualitative exploratory research approach, with semi-structured interviews to gather data from several organizations within cybersecurity in Norway. The results are analyzed and compared to existing research, to achieve a theoretical understanding of the result. The study identifies what type of ethical frameworks exist and uses different characteristics on how to compare ethics, ethical guidelines and values to the ethical frameworks. In this research work the researchers focused on examining different types of organizations and businesses operating in Norway by looking at what ethical frameworks organizations use and how ethical frameworks, guidelines and standards are used in Norwegian organizations in the context of cybersecurity. Main outcome of this study shows that none of the organizations uses a specific ethical framework, but the ethics of the organizations can be compared to two of the different types of ethical frameworks for cybersecurity. These two are the principlist framework and the human-rights/rights-based framework and some of the organizations use a combination of both of them. This research work contributes to raising awareness on the lack of knowledge and interest around ethical frameworks used for cybersecurity in Norwegian organizations. Furthermore, the outcomes of this exploratory study provided an overview on how different sectors work with ethics when it comes to cybersecurity. The work presented in this thesis provides insights to Norwegian organizations on existing ethical framework in cybersecurity; these insights can help guide strategic planning on organizational level, policy making and guidelines, which will help maintain their overall security and improve decision making.

Table of Contents

List of Figures

List of Tables

List of Abbreviations	
Systematic Literature Review	SLR
Thematic Content Analysis	TCA
Information Technology	IT
Computer Society Digital Library	CSDL
Artificial Intelligence	AI
Distributed Denial of Service	DDoS
General Data Protection Regulation	GDPR
European Union	EU
Norwegian Center for Research Data	NSD

European Economic Collaboration Area	EØS
International Organization for Standardization	ISO
National Institute of Standards and Technology	NIST
Information Systems Audit and Control Association	ISACA
Forum Incident Response Security Teams	FIRST
Nasjonal Sikkerhetsmyndighet	NSM
Center for Information Security	CIS
Information Technology Infrastructure Library	ITIL
Norsk Senter for Forskningsdata	NSD
Information Security Forum	ISF
Online Informative References	OILR
Information Communication Technology	ICT
Payment Card Industry Data Security Standard	PCI DSS
Control Objectives for Information Technologies	COBIT
Information Security Management System	ISMS
Global Steering Group	GSG
Cybersecurity and Infrastructure Security Agency	CISA

Table 1: List of Abbreviations

1. Introduction

The ethical issues raised by cybersecurity practices and technologies are of critical importance. Cybersecurity raises important ethical trade-offs and complex moral issues, such as whether to pay hackers to access data encrypted by ransomware or to intentionally deceive people through social engineering while undertaking penetration testing. There are a lot of discussions around the technical solutions to cybersecurity issues, but there is far less focus on ethical issues raised by cybersecurity. In this thesis the researchers will look at different ethical frameworks, ethical guidelines and the ethical theories. The reason for this is to look at how the ethical frameworks can help solve the ethical issues that are raised by cybersecurity practices. Cybersecurity is of critical ethical significance, because cybersecurity technologies have an important impact on human well-being as they make possible many contemporary decisions, which affects the human organizations that rely on the accessibility and integrity of data and computer systems (Formosa, Wilson & Richards, 2021).

Ethical frameworks are useful for reasoning what course of action may provide the most moral outcome. In many cases, a person may not use a reasoning process, but rather do what they simply feel is best at the time. Others may reflexively use a principle learned from their family, peers, religious teachings or own experiences. In ethics there have been many principles that can aid in ethical decision making (PennState n.d). In this day and age it becomes more and more important to protect the human users of the systems. The term cybersecurity explains its main goal when it comes to ethics which is to create a state where we are free from danger or threats in cyberspace. But in ethical theory security in itself does not play an important part. But there are sentral parts in being insecure that plays a big part in ethical theorizing, such as being harmed or injustice. The positive orientation to overcome those conditions are referred to values such as justice and benevolence, not security in itself. Reasons for this might be that the term “security” is used in a more general sense. In moral theory security is usually not an ethical value of its own, but rather an instrumental value to protect ethical values. Thus as an instrumental value security can be unethical as well. Either when the goal or the means to establish security is done in an unethical way (Loi & Christen, 2020).

Ethical guidelines on the other hand are used by groups or organizations to define what actions are morally right or wrong. The guidelines are often used as guides to tell users and employees how to perform their duties (Alleydog, n.d). Cyber-ethics is what separates security personnel from the hackers. It is the knowledge of right and wrong, and the ability to adhere to ethical principles while on the job. Cybersecurity professionals have access to the sensitive personal data they were hired to protect. So it is imperative that employees in these fields have a strong sense of ethics and respect for the privacy, laws and regulation of their customers. One of the most important ethical policies and guidelines that organizations can have and use is openness and honesty. If something goes wrong it is important to inform about it so that it can be fixed before it is too late (Reciprocity, 2021). By using qualitative interviews this thesis will investigate what ethical frameworks different organizations use or adapt for bettering their security and how this impacts their decision making.

1.1 Research Aim

There is little existing research, which looks at what type of ethical frameworks that are used by organizations for cybersecurity. Therefore the thesis will look into in what way ethics are considered in frameworks and which theories are often used when it comes to Cybersecurity. What differs from one organization to another in the way they handle the ethical parts of cybersecurity. Does the products, technologies or working tasks that the organization uses affect which ethical approaches are used, and what type of frameworks, guidelines, laws and regulations are used, adopted and made to secure the ethical part of cybersecurity. The thesis will use different Norwegian organizations from different sectors to see if there is a difference between their ethical frameworks, guidelines and standards, and if there are similarities between the ethical frameworks, guidelines and standards for the different organizations.

1.2 Research Questions

The goal for this qualitative research is to study what types of ethical frameworks are used for cybersecurity. What are the most used ones in different Norwegian organizations and do the sectors affect what type of frameworks, guidelines, and standards they use?

In the thesis there have been several interviews as well as literature reviews conducted to answer our research questions and to gather as much necessary data as possible. The different interviews and literature have helped answer the research questions below.

- What type of ethical frameworks are used or connected to cybersecurity?
- How are ethical frameworks, guidelines and standards used in Norwegian organizations for cybersecurity?

1.3 Significance of the Study

The study is important, because it looks at which ethical frameworks, guidelines, and standards that are used in organizations for cybersecurity. It will also give more knowledge about what ethical principles, ethical guidelines and ethical framework that work best for organizations. It will help organizations in choosing the appropriate ethical framework as the study will look at why the different organizations either use the same ethical framework, ethical guidelines and ethical theories/principles or different ethical frameworks, ethical guidelines and ethical theories/principles for their organization as a whole or for their cybersecurity.

1.4 Approach to the Study

In this research project the thesis will focus on the ethical framework, guidelines and standards in organizations for cybersecurity. The researchers will use a qualitative approach that focuses on the behavior and perception of the organization's managers and IT experts. The method that is going to be used is the exploratory study method. By using this method the thesis will get a closer look at the organization's ethical framework, guidelines, standards and

what kind of ethical practices they have in their organizations. The researchers will use interviews to get an understanding on how the organizations decide what type of framework, guideline or standards they are going to use. What type of policies are going to be made and used to secure the ethical aspects of cybersecurity. Do they focus more on the theoretical part of the ethics when making a decision or do they look more on the practical use of the ethical guidelines.

1.5 Research Motivation

The motivation for the chosen topic comes from the fact that ethical frameworks, ethical guidelines and standards are not a main focus when it comes to cybersecurity. Even though cybersecurity affects all organizations and users of the internet. The motivation is to look at how ethical frameworks, ethical guidelines, and standards can help improve the decision making for the employees which can help them maintain security and reduce the mistakes done in a critical situation. From the literature review, the researchers see that there is little research on the topic focused on ethical frameworks, ethical guidelines, and ethical standards when it comes to cybersecurity. Therefore the research will focus on this gap and might give organizations a new look at how to approach ethical issues and decision making in their organization and towards cybersecurity.

1.6 Research Activities

The different planned research activities in the research are the following:

1. **Literature Review**
   The literature review will focus on getting good relevant literature towards the topic of the thesis, which will help answering the research questions. The methodology that is used for the literature review is called Systematic Literature Review (SLR). Systematic Literature Review consists of 8 different steps, some of those steps focus on including and excluding different literature. The way that was chosen to do this was to make two different tables. One table is for the included literature being used in the thesis, the second table consists of the different excluded literature and reasons for why it was not relevant. Literature review is a large task and will be one of the most time consuming activities done in the thesis.

2. **Qualitative Interviews**
   The research method used to gather the necessary primary data will be qualitative interviews. The researchers will focus on using a semi-structured interview method and plan to interview different organizations from different sectors. The different interviews will be digital and the programs used to conduct the interviews will be either Zoom or Microsoft Teams. Since the different interviews and transcriptions are the most important part the main focus will be spent on this part.

3. **Analysis of the Interviews**
   To make the analysis of data more manageable the analysis method that is chosen to be used is Thematic Content Analysis (TCA).

4. **Findings and Discussion**
   The findings give an overview of what was found in the qualitative interviews. While the discussion part elaborates on how the findings in the interview and the data and information from the literature relates to each other. These two parts are also the chapters where the research questions are answered.

1.7 Structure of the Thesis

Chapter 1 - Introduction: This chapter gives an introduction to the thesis, what the topic and research is about, what type of research questions are going to be answered, why this research is significant, what the approach in the research is like, the motivation for the research and the topic and which type of activities are done through the thesis.

Chapter 2 - Literature Review: The literature review goes in-depth on what type of method is used to gather relevant literature that helps answer the research questions. It shows which types of electronics libraries are used in the searches, what type of keywords are used in the searches and information about the literature being used in the thesis.

Chapter 3 - Methodology: The methodology chapter contains information about both qualitative and quantitative research. It states how the research would have been done with the different methods, and informs about which method is used in the thesis. It also shows how the data from the interviews are analyzed and used in the thesis.

Chapter 4 - Findings: Findings will present the relevant data from the interviews which will later help answering the research questions for the thesis.

Chapter 5 - Discussion: The discussion chapter will look into the researcher's perspective, thoughts and discussions around the thesis, it will also look into the results.

Chapter 6 - Conclusion: The chapter focuses on giving a conclusion for the research and thesis as a whole. The researchers will give insight and reflections to the research and how the results can be utilized. Lastly the chapter contains recommendations for future work on the research, research contributions and reflections.

References: This section of the thesis gives an overview of the different sources and references used throughout the thesis.

Appendix: Appendix includes the inclusion and exclusion of the literature review, the consent form and the interview guide.

2. Literature Review

When doing research it is fundamental to have good, reliable and relevant literature. It is important because it describes how the proposed research is related to prior research in statistics and that it is not the researcher's own assumptions and conclusions. This section will show what type of research method that is used and look at what kind of databases that are used with search keywords, advanced search, and the steps to do the review. This section also looks at what related research is used and how these literatures are found.

2.1 Literature Review Methodology

The main method used for the research method is the systematic literature review (SLR). The systematic review is a research method and a process for identifying and critically appraising relevant research, as well as for collecting and analyzing data from said research (Liberati, Altman, Tetzlaff, Mulrow, Gøtzsche, Ioannidis, Clarke, Devereaux, Kleijnen & Moher, 2009). The method used for researching relevant literature is searching different electronic libraries and research databases. When doing the literature review it was important with keyword and syntax searching. The relevant keywords and syntax for searching through the databases were “ethical framework”, “ethical frameworks in cybersecurity”, “ethical framework principles”, “ethical framework in IS development”, “ethical framework cybersecurity”, “cybersecurity ethics and organizational culture” and “code of ethics in cybersecurity”. These were keywords related to the problem area and they were open searches without any special requirement, which resulted in huge amounts of search results.

The guideline used for conducting and completing this literature review is Kitchenhams and Charters “Guidelines for performing Systematic Literature Reviews in Software Engineering” from 2007. The three main stages from their systematic review are: planning the review, conducting the review and reporting the review.

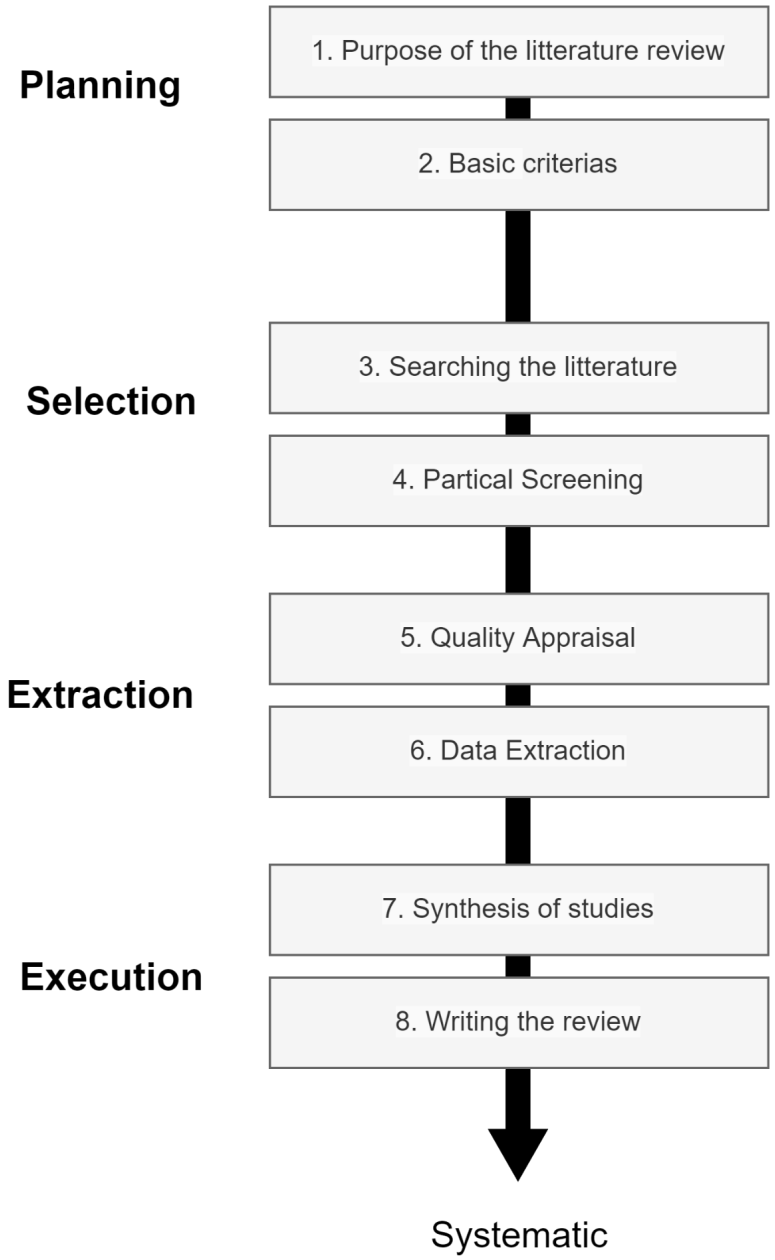


Figure 1: Systematic Literature Review Methodology (Zakariassen & Mikkelsen)

2.2 Search Strategy

The first section is called database selection and it is for deciding on what databases to search and look for literature in. When choosing databases to look for there were some criterias that these databases needed to have. The databases needed the possibility to apply advanced filters so it would be possible to filter the search by date, keywords and related areas. These databases also needed to be relevant for the study.
The databases and electronic libraries chosen to look at relevant literature was:

- Scopus - a large multidisciplinary database covering published material in the humanities and sciences.

- AIS eLibrary - A central repository for research papers and journals articles from the information systems academic community.
- ScienceDirect - Provides access to a large bibliographic database of scientific and medical publications.
- IEEE Computer Society Digital Library (CSDL) - Is the first-ever digital library evolved in IEEE.
- Web of Science - Is a collection of databases that index the world's leading scholarly literature in the sciences, social sciences, arts, and humanities.

Other search methods that were used for additional results were using a search engine like Google Scholar. When conducting searches the process was to first look through the various databases with normal search, then apply advanced search and in the end use the "snowballing" technique when an interesting literature was found to find related literature. The snowball technique is a technique going through the references from collected articles to see if there are references to articles not already included in the collected literature. This "snowball" technique was useful to find additional articles and research that could be relevant for the research problem.

	Database					
Keywords	Scopus	AIS eLibrary	ScienceDirect	IEEE Computer Society Digital Library (CSDL)	Google Scholar	Web of Science
Ethical Framework	18 125	5173	104 056	70 907	3 430 000	14 082
Ethical Frameworks in Cybersecurity	40	269	687	6266	27 400	27
Ethical Framework Cybersecurity	42	269	687	71 920	35 600	28
Ethical Framework Principles	3039	2741	41 365	79 254	2 670 000	2172
Ethical Framework in IS Development	4368	5111	83 847	576 463	3 420 000	3376
Cybersecurity Ethics and Organizational Culture	0	158	267	8 945	23 600	0
Code of Ethics in Cybersecurity	8	174	410	678 482	21 500	5

Table 2: Table of database searches results

The advanced search method was used to filter the search to make it more specific to the field of study, making it more relevant and reliable. There were created some specific filters on the databases to do so:

- The searches should be within information technology (IT), cyber security, computer science or related areas.
- The searches syntax/keyword should be about the search topic
- The research should be available and not be locked or not accessible to the public.

2.3 Practical Screening

After searching the researchers found a lot of different literature sources. But many of them were not useful for the studies so the researchers needed to narrow them down. In practical screening the researchers need to find out what to include and what to exclude to support the study. The researchers made criterias for the literature to make it easier to include and exclude them. The literature is weighted against the criterias and research questions. The researchers created the following criterias for the screening:

- **Date of publication**: The researchers would want newer studies, because of new frameworks and theories used for cybersecurity.
- **Publication language**: The language in the literature must be English or Norwegian.
- **Content**: The articles, literature and papers need to contain information about ethics, ethical approaches, ethical theories, ethics and organizational culture, ethical frameworks and their use in cybersecurity. They should also contain information which helps with answering the research questions.
- **Source**: The information needs to come from trustworthy sources and not sources such as blogs or wikipedia.

2.4 Quality Appraisal

Quality Appraisal will go through how the different literatures were excluded in the literature review. The process was built on iterations, first off we read through the title of relevant papers, then excluded the ones who were irrelevant to the research questions or that did not use ethics which are used in cybersecurity. Then the researchers started to exclude literature by reading the abstract, lastly the researchers read through the literature which was more relevant and excluded the ones that were less relevant to the research questions and criterias.

To make it easier to show the literature reviewed we made two tables. The first table is an overview of literature that is excluded. It shows the reason for excluding the literature, if it was because of the title, abstract or full text. The second table shows the literature which is included to help answer the research questions, it shows which research question the literature was beneficial to help answer. The table also shows what type of data collection method is used, and the literature's relevance from one to ten. Lastly it has a justification part which justifies the relevance ranking of the literature. The tables can be found in Appendix C and Appendix D.

2.5 Data Extraction

The inclusion tables were inspected to extract data that would help answering the research questions that are stated in section 1.2. The relevant data is also found in section 2.7 as outcome of the literature review. There is also a concept matrix made for the included literature in section 2.7.1, this helps to categories which ethical theories or principles the different literatures uses or writes about. This made it a lot easier to retrieve relevant data from the different literatures.

2.6 Analysis and Synthesis Data

In the review there have been used different fields in the inclusion table to analyze and synthesize the literature. Each of the literature that has been put in the inclusion table has been registered with what type data gathering method is used in the literature. The research also used a field for measuring the relevance of the literature towards the different research questions, the relevance ranges from 1 to 10. Lastly there is a justification field which describes why the literature that is included is relevant towards the research questions and problem. This field also helps to justify the relevance mark that the literature gets. This helps including and retrieving relevant literature easier as well as sorting it and getting a better overview of where to use the different literatures.

2.7 Outcome of Literature Review

This section will give an overview on different relevant literature that is included to answer the research questions and problems. It will give a more in-depth knowledge about the relevant data in the literature as well as different ethical theories and approaches used to make the frameworks and ethical guidelines for cybersecurity. After that there is going to be an overview in section 2.8 which summarizes the literature.

It is important to find good relevant research that describes different ethical frameworks that are connected or used when it comes to cybersecurity. Some of the research papers that are found and fulfilled the requirements are Formosa et.al. (2021), Loi & Christen. (2020), Macnish & van der Ham. (2020), Vallor & Rewak. (n.d), and Shoemaker, Kohnke & Laidlaw (2019). They look into different ethical frameworks that can help better the security of an organization, some of the frameworks that are written about and connected to cybersecurity are the principlist framework, which is based on existing work in the field of ethics, bioethics and AI ethics. The different papers also look into common frameworks for understanding the general ethical duties to others. Some of those frameworks are consequentialist/utilitarian ethical framework and deontological ethics. The papers also describe two types of best practices. First focusing on the best practice for functioning ethically in cybersecurity practice and the second set identifies best practices for living and acting ethically in general. There are also important frameworks like human rights/right-based which focus on human rights over the outcome of a decision or dilemma being good.

Some of the papers look into the problem of teaching professional ethics to future cybersecurity specialists. They also look at cybersecurity students getting a course curriculum

about cybersecurity ethics. Those papers help look into if this might help the security and adaptation of ethics for organizations by the graduates understanding cybersecurity ethics better. The papers that look into this are Blanken-Webb, Palmer, Deshaies, Burbules, Campbell & Bashir (2018), Hamburg & Grosch (2017), and Adaryukova, Bychkov, Merkulova & Skylda (2020). The papers bring in the three main ethical frameworks within the western philosophical tradition, the different ethical theories that the frameworks are based on are deontological ethics, consequentialist ethics and virtue ethics. Looking into those frameworks is a good start for thinking about ethics, but the cutting-edge nature of cybersecurity pushes upon the limits of the frameworks and it is vital to consider a global perspective for engaging in ethical thinking. Blanken-Webb, Palmer, Campbell, Burbules & Bashir (2019) is a book chapter that considers the need to prepare a generation of cybersecurity professionals to defend and secure digital infrastructure. It addresses the need to cultivate powerful capabilities in students who are often young and inexperienced which will be at the forefront of ethical technological challenges that stand to shape the future of society. The book chapter addresses the emerging realm of cybersecurity ethics in order to help to guide instructors in developing course content that will speak to the vital area of concern of managing ethical challenges and the burden of responsibility that comes along with its increased technological skills and its access to highly sensitive networks.

When looking at ethical frameworks for cybersecurity in organizations it is important to look at what types of codes, standards, regulations and laws that organizations adapt to for their ethical frameworks and guidelines. Relevant research that looks into codes, standards, regulations and laws are Somaiya,Vidyanagar & Vidyavihar (2015) and Persson & Hansson (2003)The different articles, papers and chapters focus on human rights connected to surveillance, privacy and how national laws and International laws are adapted and changed to fit their needs and fulfill requirements.

Two of the papers looked into how decision making has an impact on the code of ethics and how emotions can affect an individual's ethical decision process. Those two were Gaudine & Thorne (2001) and McNamara, Smith & Murphy-Hill. (2018). It was also found that it was not clear whether different emotions promote and/or discourage ethical decision-making in the workplace. The last source especially looked at how ACM code of ethics affects software related decisions and found it from a behavioral ethics study with engineering students, engineering developers, measuring their responses to ethical vignettes. They found out introducing participants to consider the ACM code of ethics in their decision making had no observed effect when compared with a control group.

While researching the researchers found that the culture of the organizations is heavily included when it comes to its ethical foundation. What type of organizational culture is used by the organization affects what type of ethical frameworks, guidelines and theories the organization chooses to adapt. Some of the relevant studies that were found focusing on cultural aspects are Malyuk & Miloslavskaya (2016) and Douglas, Davidson & Shwartz (2001). Technological countermeasures are not enough and therefore it is important to foster the culture of cybersecurity.

Dupuis & Renaud (2021) looks at how fear appeals are used in many domains. Cybersecurity researchers are starting to use fear appeal in experiments, where many are reporting positive outcomes. But there are ethical concerns related to the use of fear to motivate action. In the

paper they explore this aspect from the perspectives of cybersecurity fear appeal deployers and recipients.

Blanken-Webb & Cloutier (2020) paper addresses mounting calls for ethical inquiry in cybersecurity by proposing consideration of the ethics of care as a guiding philosophical framework. It offers a general introduction to the ethics of care in relation to cybersecurity, followed by a targeted discussion of care ethics' unique contribution as a philosophical framework for considering cybersecurity's position at the edge of technological innovation.

Yaghmaei, van de Poel, Christen, Gjordijn, Kleine, Loi, Morgan & Weber (2017) white paper outlines how ethical discourse on cybersecurity has developed in the scientific literature, which ethical issued gained interest, which value conflicts are discussed, and where the "blind spots" in the current ethical discourse on cybersecurity are located. The white paper is based on extensive literature with a focus on three reference domains with unique types of value conflicts: health, business/finance and national security.

2.7.1 Concept Matrix

This part of the literature review will focus on developing the conceptual framework for the literature review by explaining the theories of ethics in cybersecurity and the theoretical frameworks, approaches and concepts.

The concept matrix gives a visual representation on relevant themes in the different literatures. The concepts are based on different ethical theories and approaches towards a framework. The concepts will be elaborated more below in the Ethical Foundations.

Articles	Concepts					
#	Consequentialist	Human Rights	Deontological	Virtue	Utilitarian	Code of Ethics
Formosa et al. (2021)			x			
Loi & Christen. (2020)	x	x	x			
Macnish & van der Ham. (2020)			x			
Vallor & Rewak. (n.d)	x		x	x	x	

Blanken-Webb et al. (2018)	x		x	x		
Blanken-Webb et al. (2019)		x	x		x	
McNamara et al (2018)	x					x
Dupuis & Renaud (2021)	x	x	x	x	x	
Gaudine & Thorne (2001)	x					
Hamburg & Grosch (2017)	x		x			
Yaghmaei, et al. (2017)	x	x	x	x	x	x
Blanken-Webb & Cloutier (2020)		x	x	x	x	
Persson & Hansson (2003)		x				x
Adaryukova et al. (2020)			x	x	x	x
Douglas et al(2001)					x	x
Malyuk & Miloslavskaya (2016)						x

Table 3: Concept matrix

Ethical Foundations

There are two broad approaches to cybersecurity ethics that have emerged. The first approach is to apply core underlying moral theories, such as utilitarianism, directly to cybersecurity issues. Utilitarianism is a theory which says that doing an action is right if it tends to happiness or pleasure and wrong if it tends to produce unhappiness or pain. In simpler terms

that the consequences of an action state if it is wrong or right (Duignan, 2021). The second approach is to develop a cluster of mid-level ethical principles for cybersecurity context. Both of those approaches use casuistry which analysis what is right and wrong from case to case by using general ethical rules (Formosa et al., 2021). The following subchapters describe different ethical theories that are used in different ethical frameworks.

Consequentialist

Consequentialist theories derive from ethical principles to guide moral action from the likely consequences of those actions. The most known form of consequentialism is utilitarian ethics, which uses principles of the "greatest good" to determine what the moral obligations are in any given situation. The good in utilirism is measured in terms of happiness or pleasure (Vallor & Rewak, n.d).

Human Rights

Human rights are a focus when it comes to cybersecurity, technologies for cybersecurity that aim to protect privacy and confidentiality, such as encryption, are in general aligned with human rights. The threat to human rights is typically not cybersecurity, but inadequate cybersecurity or the lack thereof (Loi & Christen, 2020).

Deontological

Deontological ethics are rule or principle-based systems of ethics, in which one or more rules/principles are claimed to tell us what the moral obligations are in life. Moral rights are often used to make basic laws, and are often invoked to justify the making of new laws, or the revision or removal of existing ones. One modern idea which can be considered is "universal human rights" that all countries must agree to accept and respect (Vallor & Rewak, n.d).

Virtue

Virtue ethics focuses not on rules for good or bad actions, but on the qualities of morally excellent persons. Such theories are character based, it tells what type of virtuous character a person is like, and how that moral character develops. Such theories also focus on the habits of action of virtuous persons, such as the habit of moderation as well as the virtue of prudence or practical wisdom (Vallor & Rewak, n.d).

Utilitarian

Utilitarian thinkers believe that at any given time, whichever action among those available is most likely to boost the overall sum of happiness in the world is the right action to take, and the moral obligation to do. This is another way to think about the common good, but utilitarians are sometimes charged for ignoring the requirements of individual rights and justice. One way to look at it is that sacrificing one individual for the greater good of many is a utilitarian way to do it (Vallor & Rewak, n.d).

2.7.2 Ethical Part of Cybersecurity

The ethical part of cybersecurity is important as it protects the user/human of the systems well being and sense of security. Cybersecurity also raises important ethical trade-offs and complex moral issues, such as whether to pay hackers to access data encrypted by

ransomware or to intentionally deceive people through social engineering while doing a penetration test on the organization. But when ethical issues are discussed in cybersecurity there are strong disagreements about the best conceptual framework to use for understanding those issues. To deal with this problem, they redeploy to a cybersecurity context and principlist framework, based upon literature in ethical AI and bioethics. That focuses on five ethical principles: beneficence, non-maleficence, autonomy, justice and explicability. These principles will conflict in different situations and therefore needs to be balanced in a context-sensitive manner, which can result in a range of ethical trade-off that are explored by examining the ethical issues that are raised in four common cybersecurity contexts: penetration testing, distributed denial of service (DDoS), ransomware and system administration. By focusing on those common cases the researchers can analyze and understand the basics of cybersecurity ethics (Formosa et al., 2021).

Emerging Trend

There is a massive emerging trend in ethical literature on cybersecurity or computer and information security. Cybersecurity is an academic discipline that is organized around the pursuit of securing data, networks and computer systems. There are various technologies used in cybersecurity such as firewalls and encryption which are used to achieve the security goals in the face of various threats such as viruses or phishing attacks. Most human institutions rely on integrity, functionality and reliability of data, systems, and networks that cybersecurity technologies make possible. It uses ethical issues at the core of cybersecurity practice because these secure the ability for people and groups to live well. Even if the ethical literature on cybersecurity is fairly recent it builds on hacker ethics and pioneering work in computer ethics (Formosa et al.,2021).

2.7.3 Extraction of Literature

The extraction of literature chapter will give information about the main ethical frameworks, ethical guidelines, approaches, laws and methods that can help organizations to increase their security with ethics. It also gives an insight of different factors for organizations to look into and maintain privacy and ethics towards laws and regulations in Norway as well as the EU.

Ethical Frameworks

In this part of the literature review the research will go through the key concepts and frameworks that were found in the review. Many of the included literature touches upon the same concepts and frameworks. The main takeaway in this section is to get a better understanding of the main frameworks used for cybersecurity, and discuss the options that are available for the organizations to use. There is not that much literature focused solely on ethical frameworks for cybersecurity, but the researchers identified five papers that write about this topic. Those papers are Formosa et al. (2021), Loi & Christen. (2020), Macnish & van der Ham. (2020), Vallor & Rewak. (n.d) and Shoemaker et al. (2019). Those are the main literature that the researchers will use but the other included literature is also relevant since they introduce problems and solutions that are found in those five literatures. In order to understand more about the ethical approaches and frameworks that are used in cybersecurity, the researchers chose to go more in-depth about the main frameworks that are seen used in the literature.

The main frameworks that are brought up in the literature are:

- Utilitarianism Framework
- Principlist Framework
- Human-right/Right-based Framework

Consequentialist/Utilitarianism Framework

Vallor & Rewak. (n.d) defined consequentialist such: "Consequentialist theories of ethics derive principles to guide moral action from the likely consequences of those actions". The most famous form of consequentialism is utilitarian ethics which uses the principle of the 'greatest good' to determine what the moral obligations are in any given situation. The 'good' in utilitarian ethics is measured in terms of happiness or pleasure (where this means not just physical pleasure, but also emotional and intellectual pleasures). The absence of pain (whether physical, emotional etc.) is also considered good, unless the pain somehow leads to a net benefit in pleasure, or prevents greater pain (so the pain of exercise would be good because it also promotes great pleasure as well as health, which in turn prevents more suffering). Utilitarian thinkers believe that any given time, whichever action among those available to me is most likely to boost the overall sum of happiness in the world is the right action to take, and my moral obligations. The difficult part with utilitarianism is that it is difficult to know with certainty whether the consequences of actions are good or bad. This is one of the limitations of utilitarianism.

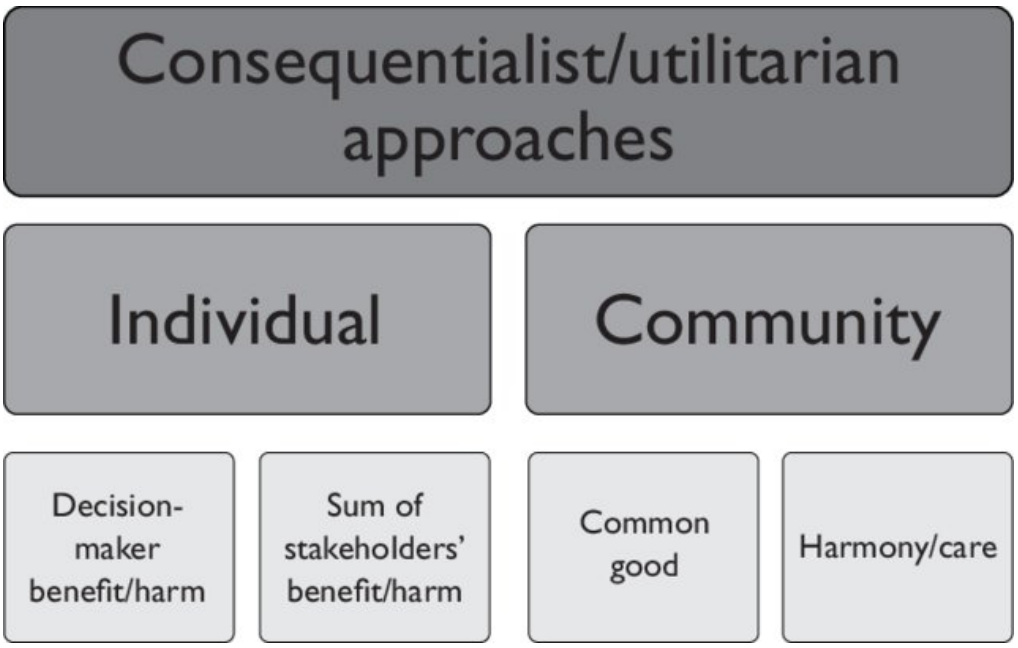


Figure 2: Consequentialist approach (Mustajoki & Mustajoki, 2017).

Principlist Framework

Principlism is a form of deontology and justifies moral reasoning by appealing to the method of reflective equilibrium and to common morality (Beauchamp & Rauprich, 2016). This principlist framework is based on literature from ethical AI and bioethics that focuses on five ethical principles: beneficence, non-maleficence, autonomy, justice and expliciliblity. Principlist is by far the most used approach for ethics in cybersecurity. This approach is good at bringing forth the relevant ethical principles in a particular domain and the ethical conflicts

that exist through case analysis. According to the framework the researchers can specify the five basic principles of cybersecurity ethics as follows:

Beneficence: Cybersecurity technologies should be used to benefit humans, promote human well-being, and make our lives better.

Non-maleficence: Cybersecurity technologies should not be used to intentionally harm humans or to make our lives worse overall.

Autonomy: Cybersecurity technologies should be used in ways that respect human autonomy. Humans should be able to make informed decisions for themselves about how that technology is used in their lives.

Justice: Cybersecurity technologies should be used to promote fairness, equality, and impartiality. It should not be used to unfairly discriminate, undermine solidarity, or prevent equal access.

Explicability: Cybersecurity technologies should be used in ways that are intelligible, transparent, and comprehensible, and it should also be clear who is accountable and responsible for its use (Formosa et al., 2021).

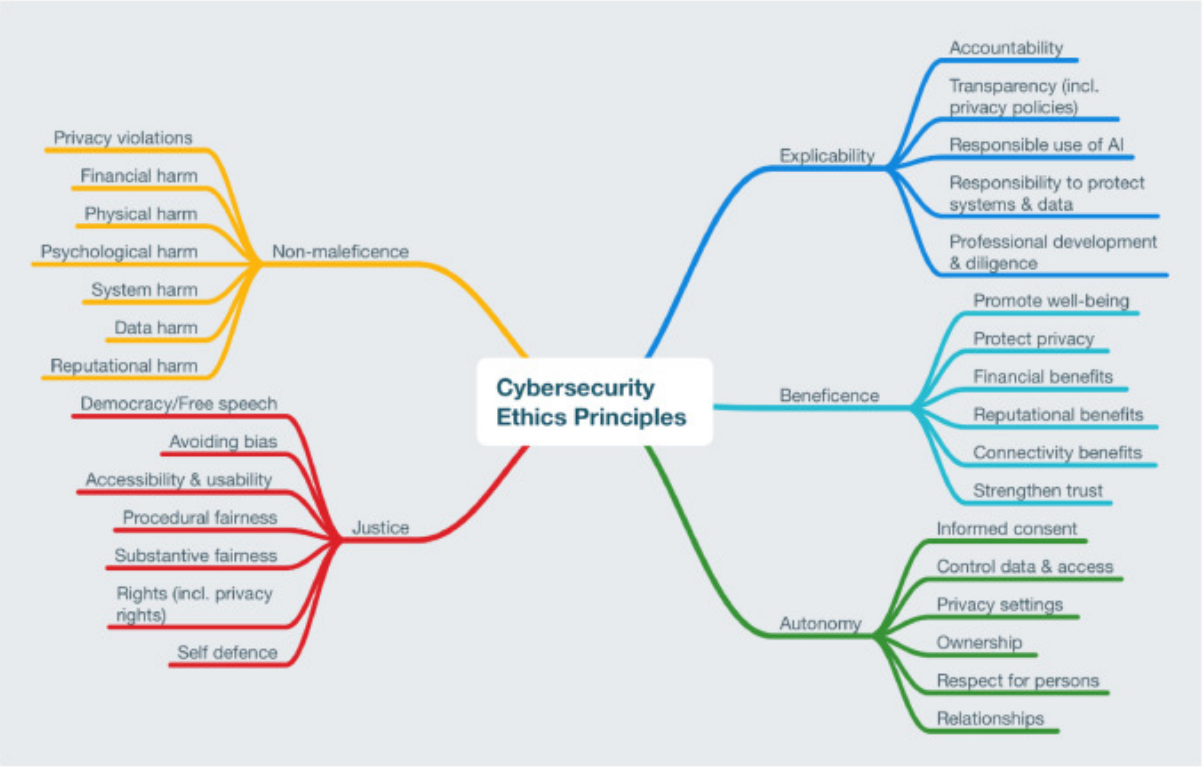


Figure 3: Five cybersecurity ethics principles (Formosa et al., 2021).

All the principles stand on equal footing, but they have different weights in different contexts. An example is where justice is more important in a case than to focus on the well-being of users. Balancing the principles requires sensitivity to the full range of ethical issues covered by the five principles. It is important to have good judgment to discern the relative weight of each principle so that it is possible to resolve an ethical trade-off in the best way possible (Formosa et al., 2021).

Human-right/Right-based Framework

The right-based framework focuses on the human right side of the ethical aspect. The idea of balance, familiar in the context of prima facie duties, is often used to discuss a trade-off

between the extent to which human rights can be respected and security achieved. The existence of trade-off implies the weight of different duties. Such duties can be protecting the security of personal information or preventing criminal attacks. The right-based theories are similar to deontological theories, but they are framed in a manner that shifts the attention to the person's obligations owed to, rather than to the agent who is obligated. If a person has rights, certain things can't be done to them even though the consequences would be good. Other things might be owed to them, no matter what the costs might be. Right-based theories of risk claim that moral agents cant make actions that have more than a null risk in violating the rights of other people (Loi & Christen, 2020).

Some types of cybersecurity technologies that are there to help protect integrity and confidentiality can be both a means to privacy but also a threat. Cybersecurity technologies such as encryption are naturally accompanied by authentication. Authentication involves certification and the management of credentials. This requires the collection of information about individuals, which may expose users to privacy infringement. Another cybersecurity technology can be those involving monitoring web trafficking and fighting cybercrime, which are in more direct conflict with human rights. Monitoring is associated with surveillance and surveillance involves threats of censorship and eavesdropping. Moreover, monitoring is associated with profiling. Profiling “may be used by the police or security agencies to find criminals or terrorists”. Hence, profiling is associated with potential violations of the human rights against discrimination, because in profiling “people are approached, judged or treated in a certain way because these have characterisitics that fit a certain profile and that are associated with certain other traits”. The main ethical issue in profiling is not privacy, although personal information may be used to build profiles. It is the fact that “profiling may inflict all kinds of undeserved harm on people, from nuisance to false accusations to even, in extreme cases, imprisonment of innocent people"(Loi & Christen, 2020).

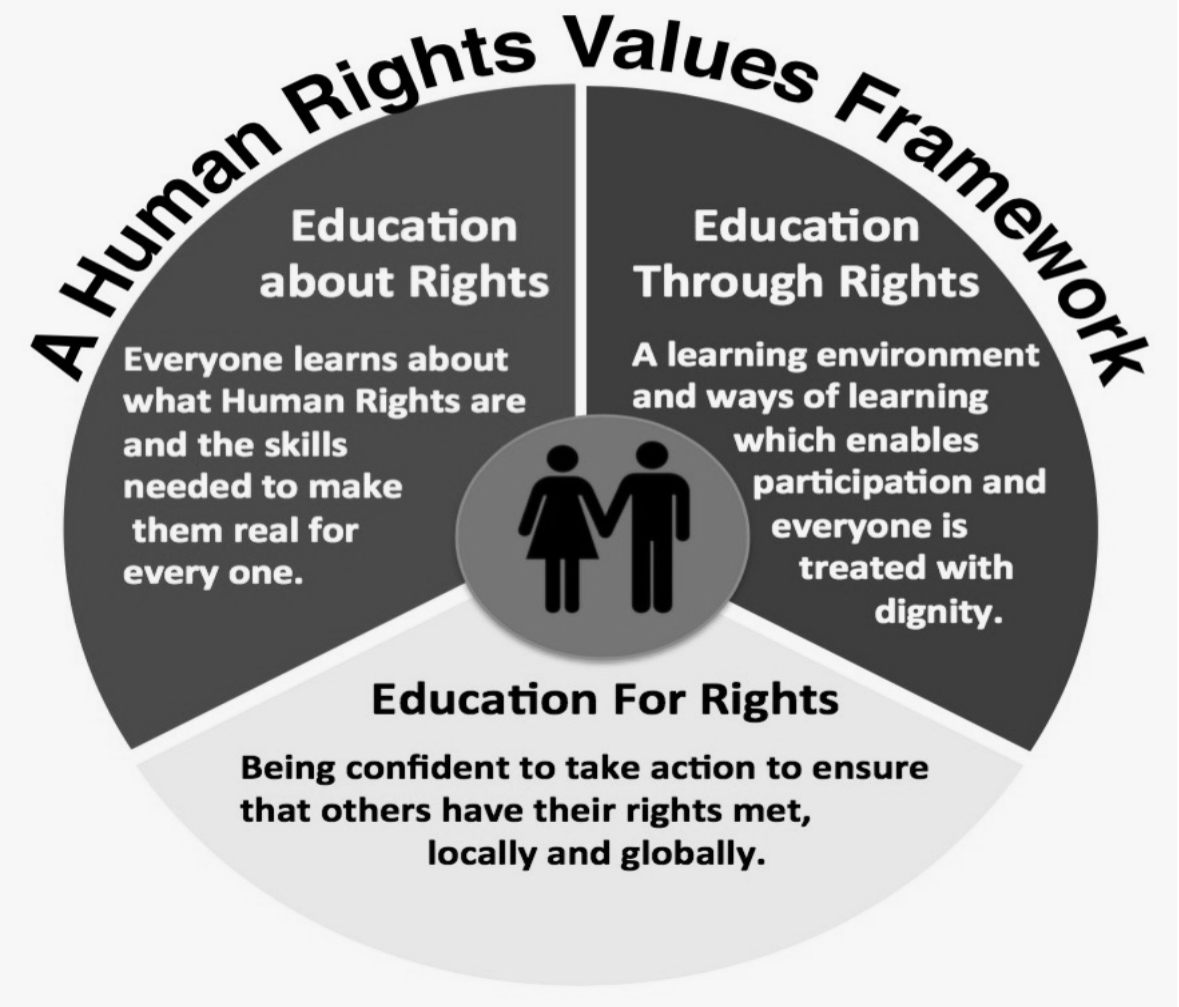


Figure 4: Human rights values framework for education (RealisingRights, 2022).

Methods and Appeals

In this section methods and appeals used to better ethical solutions, decisions and training will be discussed and explained. It will show why the methods and appeals are used and how they might or might not function in an organization.

Ethical Sensitivity Training

Being aware of different ethical principles at play in a specific domain is important for ethical sensitivity training as it helps in making the relevant ethical issues explicit so that they can be recognised in practice, making the ethical principles explicit is also important for training moral focus as it brings home the ethical choices, focusing on balancing conflicts between principles can help us to generate concrete scenarios for training moral judgment, and showing how to resolve ethical conflicts in real-world cases can help to demonstrate morale action. This illustrates the potential utility of the framework as a useful basis for cultivating the ethical expertise of cybersecurity professionals. The necessity of in-corporating "ethical reasoning development into engineering professional preparation" has been previously recognised, and this applies to analogous technical skill sets such as cybersecurity (Hess, Beever, Zoltowski, Kisselburgh & Brightman, 2019). This development requires the ability to reason with ethical principles and goes beyond knowing relevant codes of conduct, since

practitioners need to be able to deal with ethical ‘gray areas’, conflicts, vagueness and incompleteness in ethical guidelines, and novel situations raised by new technologies (Hess et al., 2019). However, there should be more focus on sensitivity as they emphasize the importance of recognising ethical conflicts between principles, rather than arguing how to resolve those conflicts, since the goal is to demonstrate the usefulness of a principlist framework for cultivating ethical sensitivity rather than resolve controversial substantive disagreements about specific cases (Formosa et al., 2021).

Fear Appeal

Fear appeals are used in many domains. Cybersecurity researchers are also starting to experiment with fear appeals, many reporting positive outcomes. Yet there are ethical concerns related to the use of fear to motivate action. Fear is defined as an emotion that moves people powerfully to action, and may tend to make them put more careful considerations of the complex features of a situation aside. A fear appeal usually packages some fear “trigger”, together with an action that the fear appeal designer wants the recipient to take. The theory goes, that the fear appeal recipient will seek to reduce the negative emotion by taking the recommended action. Cybersecurity fear appeals have been used with varying measures of success, either to persuade people to cease or reduce ill-advised behaviors, or to commence secure behaviors (Dupuis & Renaud, 2021).

Ethical Decision Making

While the influence of emotion on individuals’ ethical decisions has been identified by numerous researchers, little is known about how emotions influence an individual's ethical decisions process. Thus, it is not clear whether different emotions promote and/or discourage ethical decision-making in the workplace. There was a model developed by Gaudine and Thorne which integrated research findings that considered the two dimensions of emotions, arousal and feeling state, into an applied cognitive-developmental perspective on the process of ethical decision-making. The model demonstrates that certain emotional states influence the individual’s propensity to identify ethical dilemmas, facilitate the formation of the individual’s prescriptive judgements at sophisticated levels of moral development, lead to ethical decisions choices that are consistent with the individual's perspective judgment, and promote the individual’s compliance with his or her ethical decisions choices. (Gaudine & Thorne 2001). On the other hand, McNamara, Smith and Murphy-Hill looked into how the ACM code of ethics changes software-related decisions with a prior behavioral ethics study with software engineering students, professional software developers, measuring their responses to 11 ethical vignettes. They found that explicitly instructing participants to consider the ACM code of ethics in their decision making had no observed effect when compared with a control group (McNamara et al,. 2018).

Laws, Regulations and Standards Affecting Ethical Adaptations in Norway

This chapter will focus on different laws, regulations and standards that organizations need to consider when it comes to privacy and the ethical frameworks, guidelines and standards in an organization. It will look at the main Norwegian laws that are considered when working with ethics and privacy issues. It also focuses on how ethical dilemmas are considered such as privacy when it comes to AI, and biased decision making when working with AI technologies.

Privacy

Privacy is a concept in disarray. Nobody can articulate what it means. Currently privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations (Solove, 2008).

There is an argument that employees have a prima facie right to privacy, but this right can be overridden by competing moral principles that follow, explicitly or implicitly, from the contract of employment. Normally there is a set of proposed criterias for when intrusion into an employee's privacy is justified. Three types of justification are specified, namely those that refer to the employer's interests, to the interests of the employee her- or himself, and to the interests of third parties such as customers and fellow workers. There are sub-criteria proposed that can be used to determine whether a particular infringement into an employee's privacy is morally justified or not. Technological development has in many cases alleviated work and improved work conditions. But the new technologies have also caused problems such as ethical issues when it comes to surveillance (Persson & Hansson, 2003). That's why it is important to look into how different laws and standards are regulated by the different organizations so that the privacy of the employees and customers are safe in an ethical way. Since the thesis will look into the ethical frameworks used by organizations in Norway it is important to see how they adopt laws, regulations and standards from both the government and EU directives. Some of the laws, regulations and standards the thesis will look into and provide findings on are the Personal Data Act, GDPR and surveillance. This will help give a better insight in how Norwegian organizations adopt the ethical responsibility when it comes to sensitive information.

Personal Data Act

The Personal Data Act contains national rules from Norway as well as EUs privacy scheme (GDPR - General Data Protection Regulation) which is a regulation containing different rules that applies for EU/EØS countries. The Personal Data Act is about how the different organizations are supposed to treat and collect personal data. This law most likely applies to all Norwegian organizations, but there are situations where the law does not apply. It can be split into two different parts:

1. National rules with Norwegian adaptations.
2. EUs privacy regulations which contain two parts, the first one is focused on interpretation assistance who can supplement or explain the articles. The second is articles. This contains privacy rules in The Personal Data Act (Datatilsynet, 2021).

It follows that both the personal data act and EØS-law will follow the privacy regulations of the EU (GDPR) over the Norwegian laws in a conflict. This means that all the Norwegian laws about privacy regulations need to follow EUs privacy regulations to be valid. There are also different national laws from different sectors which help in protecting privacy such as patient record law, the Police Registration Act and similar laws (Datatilsynet, 2021).

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes

obligations onto organizations anywhere, so long as they target or collect data related to people in the EU (Wolford, n.d). When it comes to data security within GDPR it says you are required to handle data securely by implementing "appropriate technical and organizational measures". Technical measures means anything from requiring your employees to use two-factor authentication on accounts where personal data are stored to contracting with cloud providers that use end-to-end encryption.

Organizational measures are things like staff training, adding a data privacy policy to your employee handbook, or limiting access to personal data to only those employees in your organization who need it (Wolford, n.d). With GDPR it enforces all businesses to follow a strict code of ethics when it comes to collect, manage and store personal data. It is designed to put the control of personal data back in the hands of the individual.

Artificial Intelligence for Ethical Decision Making and Privacy

Artificial intelligence (AI) is the concept used to describe computer systems that are able to learn from their own experiences and solve complex problems in different situations - abilities we previously thought were unique to mankind. And it is data, in many cases personal data, that fuels these systems, enabling them to learn and become intelligent (Datatilsynet, 2018).

AI raises a number of concerns when it comes to ethics, security, legal responsibilities, etc. With this in mind Datatilsynet made a report that looked into the concern of the use of personal data in AI and the issue of privacy.

In the report from Datatilsynet they spoke with AI developers and users and the impression they got was that most sectors have adopted AI in a relatively restrictive manner, and that the techniques frequently used are limited. Datatilsynet got their answer whether it was possible to use AI, and protect people's data while doing so and yes, it is possible. It is both possible and necessary in order to safeguard fundamental personal data protection rights.

There are two main aspects of artificial intelligence that are particularly relevant for privacy. The first is that the software itself can make decisions, and the second is that the system develops by learning from experience.
In order for a computer to learn, it needs experience, and it obtains this experience from the information we feed into it. This input may be in several different formats. If a system is sought that will only perform image recognition and analysis, the experimental data will naturally consist of images. For other tasks the input will consist of text, speech or numbers. Some systems utilize personal data, while other systems use data that cannot be linked to individuals (Datatilsynet, 2018).

2.8 Summary of the Literature Review

The literature uncovered and addressed themes and topics related to ethical frameworks for cybersecurity. From the research field, the researchers feel there is a small gap in the previous research about the challenges with the ethical frameworks and how information security personnel implement ethical frameworks in organizations. Based on the literature findings, the researchers see that there are many different ethical frameworks within cybersecurity and see there are disagreements on which ethical framework should be used for understanding

ethical issues raised by cybersecurity practices and technologies. The different literature shows that the ethical frameworks that are used in cybersecurity are usually based on ethical theories such as consequentialist, human rights, deontology, virtue or utilitarian ethics. Some challenges that come when choosing which framework to choose and which ethical theory that it is based on is what type of sacrifices must be made. There are different pros and cons with the different frameworks and what they focus on securing. Principlist framework focuses more on the effect of a decision if the end result is good rather than bad, while human rights and right-based framework focuses on protecting the human users rights rather than the end result being good or bad. So the decision on which framework to choose lies on the management personnel and organization, on what they want their ethical framework to focus on protecting and securing.

The ethical guidelines, laws and regulations is another part to focus on for implementing the ethical frameworks in a good way. In the literature review the researchers can see that Norwegian organizations have to fulfill both EU laws and regulations, but also adapt to national laws and regulations from the government. One of the important rules for organizations in Norway is to follow GDPR and The Personal Data Act which is a national law. Organizations need to adapt to the European and national standards so that the ethical guidelines can guide the employees and users in making the correct decisions and behaviors in decisions that are considered to affect the cybersecurity ethics of the organization.

There is also the discussion on how AI will help with security, AI will have a great impact on the ethics and security of organizations in the future. Therefore it is important for the AI to follow good regulatory frameworks. As such, maybe using one of the ethical frameworks seen in cybersecurity will help the AI make good ethical decisions when working with information security.

2.9 Research Gaps

This section will go through the gaps in the literature. Based on the different literature found in the research part, there were some topics which only had few to none results. The different papers are missing research on how the ethical frameworks are implemented and work in practice in different organizations. The literature is also lacking in the context of the challenges of existing cybersecurity ethical frameworks.

The literature gives insight about different ethical frameworks used in cybersecurity, but the main frameworks which can be seen as best practices are principlist framework, human-right/right-based framework, and consequentialist framework. Those frameworks are mostly debated when it comes to cybersecurity ethics, but there aren't any clearly defined best practice frameworks. It's more important to look at what the organization needs to secure and then use a framework which helps secure those assets or issues and what the organization is fine with sacrificing. Some standards that are found in the literature are the Association for Computing Machinery (ACM) code of ethics, which gives general ethical principles that are used by anyone that uses computing technology in an impactful way. It helps with having guidelines for each principle so it is easier for professionals to apply the principles.

Some of the gaps stated above support the development of the different research questions for the thesis. The first gap that developed the first research question was that there was little to no research on what type of ethical frameworks were used in cybersecurity and in Norwegian context. The only research found was what types of frameworks were seen or linked to cybersecurity.

The other research question was developed because there was not any research on how ethical frameworks were used in Norwegian organizations for cybersecurity. Therefore the researchers wanted to use that gap to study how Norwegian organizations used ethical frameworks, guidelines and standards.

Lack of Focus on Security Culture

In addition the litterature present that was looked at was focusing more on what types of ethical frameworks exist for analyzing ethical questions for cybersecurity. There has not been a lot of research within the topic of ethical frameworks in organizations within cybersecurity. Naturally when looking at an organization and their ethical guidelines and frameworks it would be important to look at the size of the organization and if security is valued in their organization. There is not much literature that mentions how a good security culture has an impact on how employees interpret and follow ethical guidelines for an organization and make decisions based on that security culture.

3. Methodology

This chapter will cover the used methods for gathering primary data in the thesis. In the thesis the researchers used a qualitative approach to the research. The methods used from qualitative approach are an exploratory study and semi structured interviews. The researchers also used the systematic literature review as a method for gathering primary data for the thesis, and can be found in chapter 2. In the chapter there will be explanations on why the qualitative approach was chosen instead of the quantitative approach and some of their differences.

3.1 Research Approach

The research approach is a plan and procedure that consists of the steps of broad assumptions to detailed methods of data collection, analysis and interpretation. It is based on the nature of the research problem being addressed. The research approach is divided into two categories. The approach of data collection which is either qualitative approach or quantitative and the second which is the approach of data analysis or reasoning (Chetty, October 2016). In this section the researchers will write about a hypothetical proposal of a quantitative approach and the actual qualitative approach that was used.

Quantitative Approach

Quantitative methods emphasize objective measurements and the statistical, mathematical, or numerical analysis of data collected through polls, questionnaires, and surveys, or by manipulating pre-existing statistical data using computational techniques. Quantitative research focuses on gathering numerical data and generalizing it across groups of people to explain a particular phenomenon (Babbie Earl, 2010). For the report using quantitative research the steps taken would be carrying out one or several questionnaires to IT employees within companies and analyze the data gathered.

The type of quantitative research method the research would use for data collection and analysis would be to use survey research. Survey research is a systematic investigation conducted via a survey administered to respondents. The possibility of anonymity in surveys allows respondents to answer more valid and candid answers. By using surveys conducted anonymously it can provide more honest and unambiguous responses than other types of research methodologies. By using survey research it would also make it easy to collect numerous information from the respondents. For the research project the researchers would have to decide on what type of questions, the question content, decisions about wording, decisions about response format, and question placement and sequence in the instrument. The research would use a combination of close-ended and open-ended questions, together with a four or five point like scale.

The goal of conducting quantitative research study is to determine the relationship between one thing (independent variable) and another within a population (dependent variable). Quantitative research is either descriptive, which means the subjects are usually measured once or experimental, subjects are measured before and after a treatment.

When doing a quantitative approach for ethical frameworks in cybersecurity the goal would be to gather a lot of data from either questionnaires and surveys and analyze the data. With this approach there would be a clearly defined research question to which objective answers are sought. When conducting quantitative research it is necessary to have hypotheses. The hypotheses would be testable statements linked to the research question. An hypothesis which is related to the research question would be: “Complying with the ethical framework will lead to better cybersecurity”. The use of hypotheses is to make sure that the testing is clear. A hypothesis enables the researchers not only to discover a relationship between variables, but also to predict a relationship based on theoretical guidelines and/or empirical evidence (Davis, 2021).

The challenges and limitations of using a quantitative approach to look at ethical framework in cybersecurity is selecting the correct population for the data collection. Should the data be collected by the people that work with cybersecurity or all who are affected by the ethical frameworks. If the researchers selects only the personnel working with ethical problems in cybersecurity there might be too little data to collect. While selecting all the personnel affected by ethical guidelines and frameworks might give redundant data or information that does not answer the research questions (Chetty, September 2016). Ethical issues that might be problems when it comes to this research design are dishonesty which might leave the research misleading, protecting the integrity and anonymity for the research participant. This is a problem especially if the population is only participants that work with ethical issues in cybersecurity since this is easier to identify (Kaiser, 2019). Quantitative data can also be more efficient and able to test hypotheses, but may miss contextual details.

Another challenge with using the quantitative approach and using questionnaires is that the researchers cannot ask questions open and freely to get more detailed answers back from the attendees. The positives and strengths of using quantitative approach is when collecting quantitative data, the type of results will tell us which statistical tests are appropriate to use. The result of this is that interpreting the data and presenting those findings are more straightforward and less open to error and subjectivity in comparison to a qualitative research approach with interviews. It can allow for a broader study, involving a greater number of subjects, and enhancing the generalization of the results. With a quantitative approach the researchers also avoid personal bias by keeping a distance from participating subjects by using questionnaires. In comparison with a qualitative approach you actually have to make contact with them and speak with them which may involve personal bias by asking leading questions.

For the result part, the findings from the questionnaires and data gathered would then be written objectively in a succinct and precise format. It would be used graphs, tables, charts, and other elements to help us and the reader better understand the data. The researchers would use statistical analysis that would tell how the researchers did analyze the data, what were the key findings from the data and those data would then be presented in a logical and sequential order. There would be a description of the trends or negative results in this part.

Qualitative Approach

Qualitative approach focuses on obtaining data through open-ended and conversational communication. This method does not only focus on “what” people think but also “why” they

think so. Qualitative method is usually designed in a manner that helps reveal the behavior and perception of a target audience with references to a particular topic (Pathak, Jena & Kalra, 2013).

The research project topic is to focus on the ethical framework in organizations for cybersecurity, that's why the research will use a qualitative approach that focuses on the behavior and perception of the organization's managers and IT experts. The interview subjects can provide experience, personal opinion and information regarding ethical frameworks in their organization, challenges and opinions around those topics. Another option and method could be observations of the participants. Observation would not only include participant's observation, but also cover ethnography and research work in the field (Jamshed, 2014). It is a way to gather data by watching people, events or noting physical characteristics in their natural setting. The observations could either be overt (where the subjects know they are being observed) or covert (do not know they are being watched) (Cantrell, 2010).

Arguments for Doing Qualitative Approach

Due to the nature of the problem and characteristics a qualitative research method was found suitable at that stage to gather in-depth insights and data for the research problem and research questions. The research problems are about ethical frameworks in cybersecurity. By using a "qualitative" method the researchers will ask questions and get answers about the experience, meaning and perspective of the participant in a more efficient way than doing a quantitative research approach. The qualitative research will give more in-depth data which will provide research that later on can be used in a quantitative research project. The in-depth data is needed for the quantitative research to be able to do research on a bigger scale. Another reason for using a qualitative approach is to understand how ethics affects the employee and employees. It is important to get an understanding on how much the employees understand and use the ethics in their organizations. In (Ferguson, Thornley & Gibb, 2015) they use a qualitative research approach with focus groups because people with different perspectives will generate richer reflection to their problem. The research will focus on interviewing different employees or managers in IT companies to get further understanding of ethical frameworks within IT companies. This will help the research in getting different perspectives and generate richer reflection to the research questions. By doing this the researchers get to see if different companies use different frameworks and to see if the framework used differs from theory. Also to look at the challenges in ethical frameworks in cybersecurity.

One of the attractive characteristics of the qualitative research method are flexibility to read the research design, modularity, the ability to avoid reliance on the researcher's predetermined assumptions, the ability to focus in the meanings of key issues for participants, especially, any contradictions or inconsistencies in their perspectives (Griffin, 2004). Due to the nature of the topic when it comes to the research questions about ethical frameworks, doing qualitative research is more suitable.

3.2 Research Design

The research philosophy defines in what way the data is gathered. There are different types of research philosophies, the different types are: positivism, interprevisim, pragmatism and

realism. The researchers will focus on a more critical realism approach to the exploratory study. Critical realism focuses on what we know or understand about something that is real and not what is real but that we don't clearly understand or have knowledge about (Archer, Bhaskar, Collier, Lawson & Norrie, 2013).

There are four different types of qualitative research methods usually used: in-depth interviews, focus groups, ethnographic research and case study research. The one method the researchers have chosen to use is exploratory research method which focuses on using in-depth interviews to gather in-depth data from different organizations. The reason for choosing the exploratory research method is that the study is on a topic that has not been researched in-depth before (George, 2022). The research questions are about finding if organizations use ethical frameworks and how they work with ethics. By using exploratory study the researchers will get a better understanding of the existing problem and knowledge on the problem.

The research will be a combination of in-depth interview and exploratory research. The focus of the study is to gather data and information on which types of ethical frameworks different organizations use towards cybersecurity. Look at how they work theoretically and practically, what are the differences from organization to organization and does the type of work that the organization do have any impact on what type of ethical framework they use. The researchers will use different literature on the topic of ethical frameworks to get an understanding on which frameworks are most often used towards cybersecurity. Then the researchers are going to use that knowledge to help design and make interviews which will help gather information on what types the organizations the researchers are interviewing are using, or if they use something that resembles a framework that is already heavily used in cybersecurity. The population for the data gathering will be experts that are working on the ethical guidelines for the organization as well as working on different policies which have an impact on the ethical dilemmas that might surface in the organization. The sampling method that the researchers will use is the non-probability sampling as the researchers will contact different IT experts in organizations that work directly with the ethical aspects of the organization.

3.3 Research Organization Selection

The organizations in this thesis were selected to get a diverse look at how organizations in Norway work with ethics and ethical frameworks towards cybersecurity. The focus was to get different organizations that worked in different sectors. This will give insight about if there are differences in which ethical framework is used in comparison of what sector the organization works in. The most important parameter for the exploratory study was that the organizations were an IT organization with a cybersecurity department. Since there are different types of IT companies and ethical approaches which could influence the data gathered, it was important to map the size, sector and ethical approaches they have. By doing this it is easier to dissimilar the organizations and make it easier to see what type of ethical frameworks the organizations used for cybersecurity and the organization as a whole. The different organization sizes are defined by Norwegian standards, where 1-20 employees are small, 21-100 is medium sized and over a 100 is large sized organization (NHO, n.d). This can be seen in table 7. The researchers wanted to create an overview on how organizations adapt and apply different ethical frameworks or how they look into ethics when it comes to

cybersecurity. As written above the different criteria for the selection of the organizations can be stated as:

1. The organizations needs to be a IT company with an cybersecurity department
2. The organizations needs to be in different sectors in the Norwegian market
3. The size can differ to see if this changes how they work with ethics
4. Get a minimum of six organizations to give an overview on how they are different in applying ethical frameworks.
5. Get organizations from different sectors so that the research can show if sectors affect how they apply ethics.

Organization Profile

The research profiles will give an overview on how the different organizations interviewed are and how the ethical approaches are in their organization. Since the research focuses on how the different Norwegian organizations work with ethical frameworks and approaches for cybersecurity. This will give an easy overview of the differences between the organizations and how they differ in their use of ethical frameworks, approaches and guidelines. The profiles will give information on how big the organization is which is estimated out of the number of current employees in the organization. The information from the organizations have been anonymised as agreed upon with NSD and the informants. The information collected for the research profiles are either gotten from the interviews or information which the organizations post on their public webpages.

Organization	**Field/Sector**	**Size**	**Location**
Education IT	Education, Maintenance, IT	Large	Norway
Knowledge IT	IT, Network and online services	Medium	Norway
Governmental IT	Governmental systems, IT	Large	Norway
Audit IT	Economics, Auditing, Consulting	Large	Norway/International
Research IT	Research, IT	Large	Norway
Retail IT	Retail, Economics, IT and Infrastructure	Large	Norway/EU
Infrastructure IT	Consulting, IT, Economics, Infrastructure	Large	Norway/Scandinavia
Environment IT	IT, Consulting, Oil, renewable energy	Large	Norway/International

Health IT	IT, Infrastructure, Consulting	Large	Norway
Service IT	IT, Infrastructure, Consulting	Large	Norway/Scandinavia
Defense IT	IT Security, Consulting	Large	Norway/International

Table 4: Overview of the organizations interviewed.

The diagram shows which sector the different organizations can be found in. This gives an overview of how diverse the selection of the organizations was.

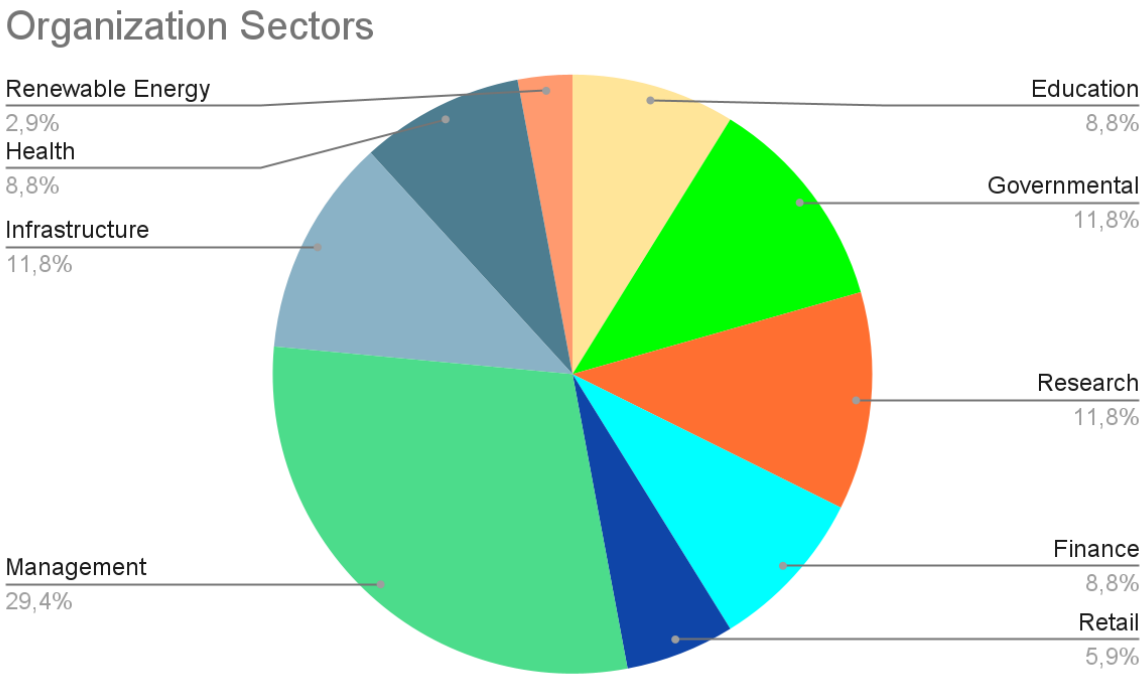


Figure 5: Organization Sectors Figure Created by D, Mikkelsen and R, Zakariassen

Education IT

The first company that was interviewed was a large sized organization which had around 1300 employees working for them. They are responsible for educational servers, users of the systems and IT service. They focus on securing users and information, since they store information about their users and employees. It is also valuable research information which is stored and handled in their IT systems. When looking at their ethical values, guidelines and approaches. Education IT writes that their focus is on trust and is only manageable if the people in the organization have good morals and ethical standards, so that the users and employees which use their systems make the correct ethical choices. The ethical rules used in the organization have two goals. One of them is to give better coordination and to give better organizational order, predictability and efficiency. The other goal with the ethical guidelines is to control and monitor the organization. Some of the central values that are focused on the employees are responsibility, trust and respect.

Knowledge IT

Knowledge IT is a medium size organization with around 90 employees, and operates in the public sector. They operate networks and online services for universities, colleges and research institutions and handle other national ICT tasks. One of Knowledge IT's most important tasks is to strengthen cyber security in education and research. They work with their customers and partners to prevent, detect and deal with security challenges which is why they are an ideal candidate for this study. The company's core values are curious, enthusiastic and customer friendly. All of Knowledge IT companies are co-located and strive for a common working environment. And for them it is appropriate that they have the same personnel policy, ethical guidelines and basic safety requirements. The companies within Knowledge IT meet often as appropriate, but at least four times a year they discuss frameworks for common services, common policy and other matters affecting all companies. They distribute and operate networks for a lot of users and they refer to the users behaving in accordance with generally accepted ethical standards in the use of the network as ethical guidelines are expected from the users. Ethical guidelines are expected for the users and it is valued by the company.

Government IT

Government IT is a large sized organization and they work in the public sector. They are responsible for the operation of IT systems in their municipality and offer the services to their employees and their users. Government IT offers work in customer support, operations, network and projects. Their ethical guidelines focus on that they have things in order. Government IT focuses on values such as honesty, trust and openness, their employees have the task to follow those principles on their own. Their goals with the ethical guidelines are that their employees and users maintain a high standard of ethical principles and values such as professionality, integrity and judgment. The ethical guidelines for Government IT build upon the principles that are found in their policy documents and generally accepted values and norms such as justice, equal treatment, reliability and loyalty. The guidelines are based upon the individual's character and moral values which will affect their reflections on the guidelines and judgment.

Audit IT

AuditIT is a large consulting organization that helps businesses with consulting, auditing, finance and legal services. AuditIT applies the basic principles from International Ethics Standards Board for Accountants (IESBA). Some of these principles are integrity, objectivity, professional competence and due diligence, confidentiality, and professional behavior. In addition to AuditIT values (which are to act with integrity, make a difference, care, work together and challenge and think new), AuditIT have adopted their own network standards. These include a Code of Conduct (ethical guidelines) that describes what behavior is expected of our employees and partners. This is behavior that gives basis for creating trust. Their standards provide guidance for a variety of circumstances, with a common goal - to do the right thing.

Research IT

Research IT is categorized as a large organization. It focuses on research in different fields such as technology, science and social science. Their focus ranges from renewable energy to

health and culture. They deliver laboratories for customers that they can use to do experiments as well as research projects. Their main focus when it comes to IT security is to comply and use the ISO 27001 and NIST frameworks. For their ethics they focus on using an ethical compass which they have made for their organization. The ethical compass is made of different ethical guidelines that the organization needs to follow when doing their work activities.

Retail IT

Retail IT is a large sized international organization which is based in different locations in the EU. They focus on delivering different products and services such as IT consultants, retail systems and security. Their values are based on being entrepreneurial, responsible, dedicated and inclusive. Retail IT also focuses on being transparent and open, they operate in different teams which means that each team's values and guidelines differ from team to team.

Infrastructure IT

Infrastructure IT is an organization which focuses on delivering SaaS products as well as PaaS and IaaS. The organization is categorized as large and focused on giving the customers good products and infrastructure as well as security to those products and services. Their values focus on being forward-looking, responsible and curious. They have their own ethical guidelines and principles that help the employees to make good decisions in situations where they need to make good ethical decisions. Infrastructure IT also uses a code of conduct and information security policies which helps them with how the employees are to work with information security and conduct themselves in the organization.

Environment IT

Environment IT is an organization that focuses on assurance and risk management and they deliver testing, certification and technical advisory services for different industries. Their values are to safeguard life, property and the environment and trust is an important ethical value in their organization. Including having to focus on GDPR they also have to comply with the privacy framework in different countries and NIST framework as they have organizations outside of Europa too. They also have internal guidelines which can be bendable if they are not aligned with the business initiative.

Health IT

Health IT delivers different IT, project, logistics and HR to different hospitals. Their main focus is to drift and manage important IT systems for the hospitals. Health ITs visions and goals is to deliver what is agreed upon, standardize and modernize and lastly digitalizace and streamline. The main focus when securing their systems is to have good access control and least privilege for their employees and users of the systems. When it comes to ethics they focus on being open and confer with colleges and the nearest supervisor about what is right ethically in a decision. They also focus on treating people with respect and integrity, openness and use enough time when difficult decisions are to be made.

Service IT

Service IT focuses on delivering different services such as system development, consultant, UX design and more. Service IT visions, values and goals focus on trustworthiness and good

organizational culture. Other values that are valued are to be down to earth, enthusiasm, sharing culture and freedom. Their culture focuses on training and making sure that the employees understand and focuses on security and complying with their guidelines and policies.

Defense IT

Defense IT is a security service provider supporting businesses. Their values are about making society a safer place and when it comes to their ethics they focus on creating trust and credibility and have integrity in what they do. They also have a strong security culture as they deliver security services to other businesses. Part of this security culture is to pursue education, awareness and training. They also need to follow guidelines based on ISO 27001 ISMS.

3.4 Interviewees Selection

Subjects in this thesis were primarily collected through emails sent from the researchers to different organizations. The focus when contacting different organizations was to get a good overview on how the different organizations worked with ethical aspects when it came to cybersecurity and the organizations as a whole. There were criteria to whom were contacted in those organizations, those criteria was:

1. They have a leadership role within the organization
2. They have responsibilities when it comes to IT and cybersecurity
3. They have responsibilities when it comes to the ethical aspects of their organization.

Several organizations were contacted about being interviewed for this study. The number of organizations that were willing to partake in the interviews were 11 organizations.

The overview of table 4 shows the general profession of the different correspondents that have fulfilled the criterias above. To anonymise them the table will only show what type of role they have and which area they work in the organization they represent. The different subjects have a variation from technical backgrounds to more organizational backgrounds. The variation gave different data and answers to the different questions which gives a good depth. But this also led to some questions that either were not answered or insufficiently answered.

ID	Profession	Area
1	Leadership	IT Management
2	IT/Cybersecurity	IT Security
3	IT/Cybersecurity	IT Security
4	Consultant	IT Security
5	IT/Cybersecurity	IT and Economy
6	IT/Cybersecurity	IT and Research
7	IT/Cybersecurity	IT and Retail

	Management	
8	IT/Cybersecurity	IT and Infrastructure
9	IT/Cybersecurity Management	IT Security Management
10	IT/Cybersecurity	IT Security and Health
11	IT/Cybersecurity Management	IT Security Management
12	IT/Cybersecurity, Incident Response	IT and Infrastructure
13	IT Management	IT, Infrastructure and Services
14	IT/ Cybersecurity Management	IT, Infrastructure and Services

Table 5: Interview subjects

3.5 Data Collection

There are three different types of forms of interviewing to gather information when it comes to a qualitative interview. Unstructured, Structured and Semi-structured. They have different strengths and weaknesses depending on what information that needs to be gathered. The interview guide can be found in Appendix A.

Semi-structured interview is scripted beforehand. Many of the questions are prepared earlier, and the interviewer's role is to ensure that all questions are covered. (Myers & Neyman, 2007).

Unstructured interview is when only a few key questions are prepared beforehand. In this case much more improvisation is required by the interviewer. One of the challenges is to ensure that there are no long pauses during the performance (Myers & Neyman, 2007).

Structured interview. In a structured interview there is a complete script that is prepared beforehand. There is no room for improvisation. These types of interviews are often used in surveys where the interviews are not necessarily conducted by the researcher (Myers & Neyman, 2007).

There were 13 interviews with 16 respondents during the data collection phase. Some of the organizations brought more than one respondent to their interview. Each of the interviews ranged from 30 min to around 60 min. With the respondents consent, the interviews were voice recorded and used for transcribing.

Semi Structured Interviews

For this thesis and research the semi-structured interview (SSI) was used. The goal when conducting the interviews was to have an open discussion and potentially learn things that are beyond the scope of the questions. Semi-structured interviews employ a blend of closed- and open-ended questions, often accompanied by follow-up why or how questions The dialogue can meander around the topic on the agenda. Rather than adhering slavishly to verbatim questions as in standardized surveys. The maximum length is about one hour when conducting SSI to minimize fatigue for both the interviewer and respondent (Adams, 2015, p. 366).

With conducting semi-structured interviews there are both advantages and disadvantages. One of the disadvantages is that SSIs are time consuming and labor intensive. The interviewers need to be smart, sensitive, poised and mimble as well as knowledgeable about the relevant issues. Another drawback is that unless you can support an enormous outlay of time and personnel, SSIs are unlikely to encompass a large enough sample to yield much precision in the estimate of the views of the population from which the sample was drawn. SSI are superbly suited for a number of available tasks, particularly when more than a few of the open-ended questions require follow-up queries (Adams, 2015, p. 367). In addition, using the SSI method allows us interviewers to learn more about the participants' own opinions, experience and perceptions. This allowed and enabled the respondents to speak freely on the topic and later the researchers asked more specific details, if it was needed. Having this method of qualitative interview approach would help to answer the research questions.

3.6 Limitations of Interviews

Using interviews there will be limitations regardless of which type and form of interview that is used. The limitations can affect the outcome and give different answers than predicted. There is a possibility that the differences in social and cultural standings can shape how the interview will be and the outcome of it (Fontana & Frey, 2000). Myers and Newman also writes about the different pitfalls and problems that can be found in qualitative interviews those pitfalls and problems are:

- Artificiality of the interview - The qualitative interview involves interrogating someone who is a complete stranger, it involves asking subjects to give or to create opinions under time pressure.
- Lack of trust - As the interviewer is a complete stranger, there is likely to be a concern on the part of the interviewee with regard to how much the interviewer can be trusted. This means that the interviewee may choose to not divulge information that he or she considers to be “sensitive”. If this is potentially important information for the research, the data gathering remains incomplete.
- Ambiguity of language - The lack of time for the interview may mean that the data gathering is incomplete - The meaning of our words is often ambiguous, and it is not always clear that subjects fully understand the questions (Myers & Neyman, 2007).

Using quality methods can be for gathering data, but it is necessary to understand the limitations and pitfalls of using interviews. When going forward with the interviews it is

important for us researchers to think about these limitations and pitfalls, be aware of them, and try our best to avoid them.

To best try to avoid these limitations above there were created measures to deal with them. To build trust between the subject and the interviewer, a consent form was sent to the subject together with a description of the research topic. They were also given the opportunity to look at the interview guide if they wanted. The consent form gave the subjects information on how the data will be handled, stored and deleted. It also says that everything that is being said will be anonymised and cannot be tracked back to them. The subjects then had more information and knew more about what they were signing and what the interviews involved. With the limitations of ambiguity of language and to avoid the misunderstanding of both interviewers and interviewees it was agreed to highlight anything that was not understandable and clear so it could be further explained. In all interviews there were also two interviewers to attend so if there was any misunderstanding, the other interviewer could notice it.

3.7 Data Analysis

The plan for doing data analysis is to conduct an exploratory research study. Exploratory research in social science can be defined in different ways, but its core consists of an attempt to discover something new and interesting, by working through a research topic. (Swedberg, 2020). This can be helpful to get a better understanding of the research project. Reading many different sources and analyzing other points of view can help us to get more creative solutions.
The research process will involve doing the following:

- Define the objective and explain why we are presenting the subject.
- Determine who will be the right candidates for the exploratory research study. The researchers also need to get permissions, and other features that will make the exploratory research study effective.
- Identify which various consequences could result from the situation,
- Make a list of credible sources and examine them.
- Focus on several key issues and look at why they exist and how they impact the research subject.

The Data Analysis part of the report will show the analysis of the different interviews, which type of method the researchers used, a short summary of the interviews and the different codes and themes found in the different interviews.

Analysis Method

The method used to analyze the interviews is Thematic Content Analysis(TCA), it is a descriptive presentation of qualitative data. In this case the qualitative data will be transcriptions from the different interviews. TCA portrays the thematic content of interview transcripts by identifying common themes in the texts provided for analysis (Anderson, 2007). There are different approaches to thematic analysis, the two different approaches that the researchers looked at were inductive and deductive approaches. An inductive approach involves allowing the data from the interview to determine the themes. While a deductive approach involves coming to the data with some preconceived themes that the researchers

want to find information about. In this qualitative research the researchers have used the deductive approach towards Thematic Content Analysis (Caulfield, 2021).
The TCA can be divided into 6 main steps:

1. Familiarization
2. Coding
3. Generate Themes
4. Reviewing Themes
5. Defining Themes
6. Writing

Step 1: Familiarization of the Transcripts

Transcribing the interviews took a lot longer than expected, since it was more time consuming than expected to listen to the audio files and transcribe what was relevant for the research. In this research there were not any programs used to transcribe the audio files automatically.

Step 2: Coding

Coding of the transcripts were used to look if the different interview objects correlate or if they use similar patterns or data types. There was a table used to get a better overview of the different assets that the researchers think are important in the different interviews. This table will help to look at how the different organizations are similar or differ when it comes to ethics in their organization and towards cybersecurity. The coding table will contain different codes which were found in multiple interviews and that are the most relevant. The different codes can be found in table 6.

Step 3: Generate Themes

By using the different codes found in the coding part, there was identified pattern among them to make different themes which will be shown in the table under:

Codes	**Themes**
Ethical Guidelines	Ethical frameworks , Organizational responsibility
Incident response	Security controls
Least privilege	Security controls
Trust/Trustworthiness	Ethical values
Openness/Transparency	Ethical values
Integrity	Ethical values
Principles	Ethical framework
ISO 27001	Security framework

NIST	Security framework
Whistle-blower channels	Users privacy, Laws
GDPR	Laws, Users privacy
The personal data act	Laws, Users privacy
Access management	Security controls
Security Culture	Culture
Microsoft services	Collaborating partners
ISACA	Ethical standard
NSMs basic principles	Security controls, ethical framework
Management systems	Controls, Organizational responsibility
Compliance	Laws
CIS controls	Security controls
Legal team	Ethical framework, Ethical standard, Laws
Phishing campaign	Simulated attacks
Security measures	Security controls, Security framework, Security responsibility

Table 6: Themes of the codes

Step 4: Reviewing Themes

In this step of the data analysis the research will make sure that the themes are a useful and accurate representation of the data. When looking at the different themes the researchers can see that they fit well with the different codes they are connected to. They describe the codes in an overall good way.

Step 5: Defining and Naming Themes

In this phase, each of the themes that were identified in the previous step were put in a table below with a description explaining the theme.

Theme	Description
Ethical framework	Ethical frameworks include ethical and moral elements such as principles for how to behave in the organization. It gives a foundation for the ethical guidelines to be based on.
Ethical values	Ethical values guide the way the business is done and what is considered acceptable or desirable behavior above and beyond compliance with laws and regulations. Examples of ethical values are trust, transparency and integrity.
Organizational responsibility	When it comes to organizational responsibility the organizations need to comply and follow ethical guidelines, laws and regulations which the state and society puts upon them.
Controls	Management systems for information systems that are built around controls and controlling executive and governing documents.
Simulated attacks	Attack simulated training like phishing and password attacks to test people to see if they open suspicious links.
Users privacy	User privacy focuses on protecting the users data and is law regulated by GDPR. The organizations focus on protecting their employees data and user data from their different systems.
Security controls	Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, or computer systems, or other assets.
Security responsibility	There is a security responsibility when working with the work process. It is important to have meetings and internal collaboration platforms where it is possible to discuss consequences and run ROS analyzes for security level and maintaining privacy.
Collaborating partners	The different organizations have a lot of different collaborating partners. Those partners contribute to the ethical laws, rules and guidelines that need to be followed. They also have different guidelines that the organizations need to follow to be their collaborative partners.

Laws	Laws focus on the different laws and regulations which are put upon organizations when working with security, privacy and ethics.
Security framework	Different frameworks and standards that are used by the different organizations. This is to comply with security laws, regulations and measures to protect the organization.
Culture	Culture is a term which describes the attitudes, behavior, opinions of a particular group of people in a society.
Ethical standard	The theme focuses on different ethical standards that are required by different certifications or organizations. The different ethical standards usually contain different ethical guidelines that need to be followed.

Table 7: Defining and naming themes

Step 6: Writing Up

The write up will conclude the analysis of the data, this can be found in the findings chapter and discussions chapter. The write up will use the most important themes as headers to help describe the findings in the different interviews and help answering the different research questions. There were some themes that were commonly found in the interviews, which was not an important aspect when it came to the research questions.

3.8 Validate Findings

The representation of data and validation of data is a major in qualitative research. The aim of the research is to establish authenticity, credibility, dependability and transferability. In the research the researchers will be using various strategies to validate research findings. One of the methods is to use triangulation with other qualitative findings, either from the research or from others. The researchers are going to interview people in Norwegian organizations so it's important for member checking. Member checking is the process of ensuring that the researchers understood the subjects correctly or that the researchers are accurately interpreting their voices. Another method is to use peer-debriefing. Peer-debriefing may be useful in checking the understanding of the implications of the data, in ways that can add to the credibility.

3.9 Limitations

There are many different factors that can limit the research design. Some limitations to the project can be the formulation of the research aim and objectives. The researchers might have formulated the research aims and objectives too broadly or too small. It's important for us to specify in a way that formulate the research aim and objective to be narrowed so the level of focus of study can be increased. The implementation of the primary data collection method is

also something the researchers don't have much experience with so there is a chance that method is flawed. This is also a master thesis so there are time constraints to it. The time available to study the research problem should be within the time frame of the project. When doing the research, there might be self-reported data which limits the fact it rarely can be independently verified. The researchers have to trust that the accuracy of what people say in the interviews to be true. These self-reported data can also contain several potential sources of bias and can be limitations.

When doing the interviews with the interview subjects there might be challenges regarding the interview form. Doing semi-structured interviews can be time consuming for the respondents and it can be challenging to do that properly. If the interviewee doesn't want the researchers to do any recordings of the meetings too, there might also be challenges when taking notes as it can be difficult to take notes of everything being said.

3.10 Ethical Considerations

This section will give an overview of some potential ethical issues and considerations that can occur related to the project. Dealing with information about an organization's ethical framework and guidelines can be a sensitive topic so thorough discussion it was decided that this study could gather sensitive data. Every participant and interviewer was informed about their right to revoke their consent at any time. One factor that was put in consideration was the Covid-19 pandemic that is still afflicting the country, which led to interviews being digital. The GPR legislation usually requires interviews to be conducted in a physical and offline environment where the device used to record the interviews must not have any network connectivity. With social distancing it made most people having to have home offices and therefore, the interviews were conducted through the internet in the form of online interviews. The Zoom platform has been used to conduct these interviews as Zoom has an agreement with University of Agder (UiA) and is something the researchers have experienced before. Zoom software also comes with encryption technologies and is safe to use for data collection. It was also offered to use Microsoft Teams if any participants wanted to use that platform instead.

To conduct this thesis and study, it was necessary to send an application to the Norwegian Center for Research Data (NSD) for the research intents, data to validate and approve that us researchers are following general rules for data storage and privacy for the respondents. The candidates of this thesis are ensured privacy and anonymity, which means that the data in this thesis should not be able to identify individuals. The candidates will be called informants instead of displaying and calling them by their names as well as the company is anonymised. There were also security precautions and management plans provided to NSD. The data collected is stored and protected in UiA’s own cloud, which is provided by Microsoft and the service used was OneDrive. This process was also approved by NSD in the application.

Voluntary Participation

Participation should be voluntary in all research, and there should be no coercion or deception. The researchers should not be in a position to force respondents to participate. The participants should be invited to participate with a clear understanding that they are under no

obligation to do so and that there will be no negative consequences for them if they do not assist us in the research (Polonsky & Waller, 2011).

Informed Consent

One important issue in the research is to ensure the potential participants fully understand what they are being asked to do and that they are informed if there are any potential consequences of such participation. One way to address the consent issue is through the use of an information sheet, which is provided to all those who are invited to participate (Polonsky & Waller, 2011).

Before conducting any interviews there were sent an email to the participants with a consent form that informed them about the privacy and data collected surrounding the interview. This writing contained information about the contestants rights to insight into their data, the storage and how data is managed. This consent form can be found in Appendix B.

Confidentiality and Anonymity

Within the information sheet, the researchers will have to mention that they will keep respondents' answers confidential and/or anonymous. Confidentiality means that the researchers know who the participants are, but their identity will not be revealed in any way in the resulting report. It is important if the participant wants their identity to be hidden for us to not leak any metadata or anything that can identify the participant based on the level of analysis (Polonsky & Waller, 2011).

Harm

It is important for us to identify any potential for harm and determine how this potential for harm could be overcome. Ideally the research should have minimal, if any, potential for any harm to occur (Polonsky & Waller, 2011).

Plagiarism

Plagiarism related to student work is that the researchers need to be careful that they do not misrepresent someone else's work as our own. There can be temptation to "cut and paste" their work to form new ideas. It is important to appropriately cite their material properly. (Polonsky & Waller, 2011).

Academic Fraud

Academic fraud involves the intentional misrepresentation of what has been done. This would include making up data and/or results from the data or purposefully putting forward conclusions that are not accurate. The temptation to commit academic fraud should be avoided during this research project (Polonsky & Waller, 2011).

4. Findings

In the findings chapter the results and data from the interviews will be presented, which are the main sources of data that were used for answering the research questions. The researchers conducted 12 interviews and came in contact with different organizations. The interview subjects were contacted through emails.

The answers from the interviews, contributed to answering the research questions:

- What type of ethical frameworks are used or connected to cybersecurity?
- How are ethical frameworks, guidelines and standards used in Norwegian organizations for cybersecurity?

As an outcome of the different interviews with the different organizations from the various sectors this chapter will give in depth information about what was found. First off in the findings of the qualitative interviews the researchers uses a table to give an overview of which ethical frameworks that the different organizations most likely relates the most to, the different standards and code of ethics that they informed us about in the interviews and which types of security frameworks that they use in their organizations. Later on in the chapter there will be information regarding what types of ethical standards, ethical frameworks, challenges, security measures and testing, and privacy that the different organizations use.

Company	**Size (S/M/L)**	**Ethical framework / guidelines**	**Standards/ Code of Ethics**	**Security Frameworks**
Education IT	Large	Principlist Framework/ Human-right/Right-based	The European Charter & Code for Researchers, De Facto Standard	ISO 27001 and 27002
Knowledge IT	Medium	Human-right/Right-based Framework	ISACA and FIRST	ISO 27001
Government IT	Large	Principlist Framework	De Facto Standard	N/A
Audit IT	Large	Principlist Framework	ISACA	ISO 27001, ISO 27701
Research IT	Large	Principlist Framework	Internal Ethical Compass	ISO 27001, NIST
Retail IT	Large	Principlist Framework	Maturity Index	ISO 27001
Infrastructure IT	Large	Principlist Framework	Code of Conduct	ISO 27001, ISO 37001, ISO 27002, NIST
Environment IT	Large	Principlist Framework	Information Security Forum(ISF) standard of good	ISO 27001, 9001, NIST,

			practice	SOC 2
Health IT	Large	Human-right/Right-based/ Principlist Framework	ITIL	ISO 27001, NIST, CIS, CCA
Service IT	Large	Principlist Framework	EU Taxonomy GSG	ISO 27001, NIST, ISO 9001
Defense IT	Large	Principlist Framework	Code of Conduct	ISO 27001, ISMS, NIST, CIS

Table 8: Overview of the findings of the interviews

4.1 Ethical Standards

The different interviews gave insight and information about what types of standards and codes of ethics the different organizations had to follow, when it came to their ethical guidelines. In this chapter there will be information about the different codes of ethics and standards found throughout the different interviews.

Education IT did not use a specific ethical standard for their IT systems or cybersecurity, but they do follow a standard called the European Charter & Code for Researchers. The standard is based upon different principles and requirements which helps to specify roles, responsibilities and entitlements of researchers. It constitutes a framework for researchers, employers and funders which invites them to act responsibly and as professionals (Euraxess, n.d). They also use the De Facto standard which often is a result of marketplace domination or practice.

> "No, we have not defined a set of frameworks that define ethics specifically. We relate more to the general guidelines and we have a management system for information security that regulates both rules and what lies in between rules and that is how it is with us. It has been implemented as a de facto standard for our company, but not regulated by law" (Education IT).

De Facto standard can often be described as following the best practice and method for a problem (Carpenter, 2012).

Knowledge IT mentioned many in their organization where certified IT auditors. The certification was from Information Systems Audit and Control Association (ISACA) and the certification they used was called CISA which stands for Certified Information Systems Auditor. Knowledge IT said they were obligated to follow ISACA's guidelines. These guidelines are about IS auditing and assurance standards and define mandatory requirements for IS auditing. "A lot of the people who have worked here for a long time typically have certifications through ISACA. Those certifications have ethical guidelines in which the employees with the certifications need to follow and comply with"(Knowledge IT). They report and inform:

- IS audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- Management and other interested parties of the profession's expectations concerning the work of practitioners
- Holders of the CISA designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate committee and, ultimately, in disciplinary action (ISACA, 2020).

Knowledge IT also mentions that their CERT follows the guidelines that Forum Incident Response Security Teams (FIRST) gives them. FIRST is a forum of incident response and security teams. FIRST brings together a wide variety of security and incident response teams. FIRST uses a CSIRT Services Framework that gives a list of services that a Computer Security Incident Response Team (CSIRT) organization may consider implementing to address the needs of their constituency, and the mechanisms to address gaps in the ability to do so. Some of the services that they recommend are:

- **Incident Management:** Services related to management of cyber-event, to include alerting constituents and coordinating activities associated with the response, mitigation, and recovery from an incident.
- **Incident Analysis**: Services related to identifying and characterizing information about events or incidents such as scope, affected parties, involved systems, timeframes, and status.
- **Information Assurance**: Risk/Compliance assessment, services related to assessing risk or compliance assessment activities. This may include conduc of the actual assessment, to providing support to evaluate the results of an assessment. Typically done in support of a compliance requirement.
- **Situational Awareness**: Sensor/Metric operations, services that focus on the development, deployment and operation of systems and analysis methodologies to identify activities for investigation.
- **Outreach/Communications**: Cybersecurity policy advisory, services that support the development and adoption of cybersecurity policy to positively shape the environment of the CSIRT, its constituency, and other stakeholders by providing subject matter expert advice to inform decision makers.
- **Capability Building**: Training and education, capacity infers some level of capability at some level of maturity. Thus capability is the core building block for CSIRT services. Capability building provides training and education to a CSIRT constituency on topics related to cybersecurity, information assurance and incident response.
- **Research/Development**: Services that help define, identify new capabilities and improve methodologies for performing vulnerability related services or coordinating other organizations or commercial practices that can demonstrate the same (FIRST, 2016).

Government IT did not know of any specific type of ethical standards when it comes to their security department within their organization. It was more of a De Facto standard for following the best practice and method for problems. Even though Government IT did not know any specific standards except de facto standard, they had their own ethical guidelines

for employees in their organization that explained key values for their organization and how they expect their employees to behave.

Audit IT uses the same certification that Knowledge IT uses which is the ISACA certification for Certified Information Systems Auditor. By having this certification their employees are also bound to the guidelines that the ISACA association has.

Research IT uses an internal ethical standard in their organization which they call an ethical compass which was created by an ethic general and an ethics committee. This is also something the HR have and everyone in their organization should know about the ethical guidelines which are in that compass.”We have an ethical compass used in the organization which describes how the employees should conduct themselves and act. That compass is written down and used as guidelines, it is our HR department which owns it”(Research IT). There is also openness in relation to reporting so if an employee sees that something is not right in relation to their own compass, then there should be openness around it and it is easy to report.

Retail IT did not have any specific ethical standard but uses the maturity index as a way to measure how mature their security is. Their maturity index is linked with their security self assessment which tells them what they are doing and the index tells if they are actually doing it. “The manager has access to maturity index and maturity index is measuring for example how many vulnerabilities you have that are critical or not if you are onboarded to different security programs, different security services, because if you are not we don’t know if you are secure or not”(Retail IT). It also helps them measure different organizations that they want to cooperate with. It is used to check if they have different security programs and different security services since they need to know if the organization is secure or not.

Infrastructure IT did not have an ethical standard they based their ethical guidelines on, but they did have code of conducts where ethical guidelines were written and which the employees had to follow. The ethical standard which their ethical guidelines was inspired on was from ISO 37001 which is anti corruption, and NSM when it comes to ethical hacking.

Environment IT follows the Information Security Forum (ISF) standard for good practice, this standard is developed with NIST to create Online Informative References (OILRs) between information security standards and the NIST cybersecurity framework (ISF, 2022). The standard is the most comprehensive information security standard available. It provides complete coverage of the topics set out in ISO 27002, NIST Cybersecurity Framework, CIS Top 20, PCI DSS and COBIT 5 for information security. It is used by many of the world's leading organizations as their primary reference to manage information risk (ISF, 2022). One of the ethical principles that can be found in the standard is that security policy should prohibit making sexual, racist or religious statements, which may be offensive (Siponen, 2006).

Health IT has ethical standards and guidelines when it comes to anti corruption and white washing. They also have ethical guidelines and code of conducts which all employees in their organization needs to follow

Defense IT did not have an ethical standard they based their ethical guidelines on, but they did have code of conducts where ethical guidelines were written and which the employees had to follow. They instead use ISMS which is an information security management system. This system helps them make and maintain their guidelines and the management system is based on ISO 27001 standard.

Service IT relates to the new EU taxonomy and in the GSG direction when it comes to ethical standards. They mentioned that it is not mandatory to have it in the report this year, but they have included it in the year report.

To summarize the different standards found in the organizations the researchers can see that the standards are either ethical or principle based.

- Some of the organizations use De Facto standards which focus on following the best practice and method in that field.
- Other ethical standards found are ISACA and FIRST standards which have ethical values that need to be followed.
- Lastly the organizations have a code of conduct which represents how they should act and work in that organization.

4.2 Ethical Frameworks

In this chapter the researchers will look at the organizations and see if they have heard about ethical frameworks in the context of cybersecurity and if they use it.

Education IT mentioned that they did not have any set of frameworks that defined ethics specially, but they related more to the general guidelines and they had a management system for information security that regulates both rules and what lies in between rules. It had been implemented as a De Facto standard for their company, but not regulated by the law.

Knowledge IT mentioned that the people who work within security in their organization and work with it for a long time have in ways linked it to several external ethical guidelines, plus the fact that those of them who have worked in that organization within information security have long had typical certifications through ISACA as such CISA as an information security auditor and through those certifications they are committed to international ethical guidelines for that organization.

Government IT said that they had never heard about ethical frameworks or heard about it in any formal discussions in any previous jobs. Government IT mentioned that there are some principles that they are trying to establish, but not any formal ones.”I have never heard about

ethical frameworks used in a work situation. There has never been any formal discussions around that theme, but we do use principles which we try to establish"(Government IT). There are more principles that for example you should not have access to more than what you need to do for your job. They are also careful with such things with security when it comes to firewalls and logs. There are also other principles that they want the systems to monitor the traffic, logs and activity and flag what is necessary so they don't need to look at more than what is needed.

Audit IT does not have a specific ethical framework, but they are good at being clear with what values and principles they have."I have a hard time understanding what the ethical frameworks are used for. But I do know a lot about our policies, guidelines and standards when it comes to ethics"(Audit IT). Audit IT focuses on values such as trust and openness, but it is as important to protect the integrity in their work. Those values are used throughout the organization. This can be seen in their procedures and guidelines. The way those values appeal to information security is by following the laws and regulations that are connected to information security.

Research IT was unfamiliar with the concept of ethical framework, but within their organization they use an ethical standard/framework which is called the ethics compass which they use in relation to their projects. Some ethical values Research IT have are transparency towards events in the organization and transparency in relation to reporting if they see that something is not right in relation to their own compass. They also very much stick to policies or choices and policies they should make. Some other values that are in the ethical compass are honesty and trust. Trust is not something one can decide to want or demand, but something one deserves. Therefore, they must conduct business with care and honesty. The ethical compass also mentions generosity, courage and unity.

Retail IT doesn't have anything that can be called an ethical framework, but the ethics are more a part of different other activities that they do. Some of those activities are data protection and privacy or things such as that. Other examples are threat incidents, so they have different parts of the ethical frameworks in their organization but not something that they specifically call an ethical framework. Retail IT focuses on their values which are being entrepreneurial, responsible, dedicated, inclusive and transparent.

Infrastructure IT doesn't mention any ethical framework, but a more general code of conducts they have in their organization and code of conducts that says how to behave in general also we have one which is how to behave within information security. Some values Infrastructure IT mentions they have in their organization are collaboration which is something they work a lot with. Openness and trust are also big keywords. They also have four big keywords in the organization which are future-oriented, responsible and curious and cooperation. They do work with information security and following laws and regulations and which makes them responsible for their actions.

Environment IT they were unsure about what was meant with ethical frameworks. But said that they used an ethical framework in the form of a code of conduct. All the employees need to follow and maintain a relation to the code of conduct, but the code does not point specifically towards cybersecurity. It is important to follow the code of conduct so that the organization is protected against fraud and other things that might harm the organization. The

ethical values that are valued the most in Environment IT is trust, it is important for Environment IT that others can trust them and their work. Other values that Environment IT focuses on are to safeguard life, property and the environment. Lastly they value transparency, when employees or leaders make mistakes they focus on being transparent and the willingness to admit mistakes and learn from them.

Health IT did not mention any ethical frameworks for cybersecurity that they used in their organization, but they said all employees were bound to ethical guidelines which the employees have to follow. They also mentioned openness as a cornerstone of the security work they did. Health IT posts parts of their management systems on the internet so that they are available to everyone in the world so that they can give feedback on things people think Health IT do are good and things they possibly could do better. Health IT has four key values which are respect for their customers and each other. They are predictable and keep their promises. They are competent and deliver quality and they are service-minded and proud of their work.

Defense IT has good control on their policies and guidelines, but as far as they know they dont have a specific framework for ethics. They do use ethical guidelines and policies but nothing that is specifically connected to cybersecurity. “I know very well our policies and our guidelines, but as far as I know we do not have a specific framework for ethics that is linked to those policies then” (Defense IT). The ethical values that they value the most are integrity and trustworthiness.

Service IT did not have its own ethical framework for cybersecurity. They did have ethical guidelines and their own rules for security, security instructions and such things. The ethical values in Service IT are to be credible to customers and suppliers as employers and owners. We will always give advice that is best for the customer, that they follow laws and rules at all times and that they have a respect for dealing with other people both in leisure time, i.e. in both formal and informal contexts.

To summarize the ethical frameworks in the context of cybersecurity the researchers can see that:

- None of the organizations had heard or knew what ethical frameworks were in the context of cybersecurity.
- Instead of an ethical framework for cybersecurity they had ethical guidelines and ethics.

4.3 Challenges with Ethical Guidelines and Ethical Frameworks

In this subchapter the researchers will look at what type of challenges organizations have when it comes to ethical guidelines and ethical frameworks for cybersecurity.

Educational IT mentioned that they tried to run nanolearning where they tried to work with attitudes and attitudes towards safety.

“What is a little difficult is when you use ethical guidelines in cybersecurity because it is much more than just ethics. Ethics governs our norms as well as what we expect to do and of course we avoid challenging employees to a great extent, but we also try to teach them to understand that safety is part of the culture. Therefore, we use this safety month to spread attitudes about a good safety culture and the ethics become in a way a small part of the overall picture”(Educational IT).

Government IT said that they didn’t think there was any challenges, but also said safety is not just about what their department do, but about the whole company and building a maturity in the company which means that you not only need to have a standard framework, but must have a common language, an established consensus that this is the right way to do it. It is a conscious effort to establish these De Facto frameworks/standards.

Knowledge IT mentioned that they had read through them before our meeting, but there was not something that contradicts any thoughts they had about them. They also mentioned one of them had experience from another governmental agency where they were more strict when it comes to their ethical framework.

Audit IT says there are probably challenges all the time when it comes to employees not following the ethical guidelines and frameworks. Audit IT does encourage employees to talk to their closest leader or coaches if they have made the mistake of not following the guidelines. If they don't want to contact their leader or coach, then they can contact either HR or send a message through a messaging channel which is anonymous. Audit IT also mentions that it is hard to know when an ethical line has been crossed, we are humans that try to do our best, but that can be willing to take shortcuts to complete work tasks and do something that they don't know is wrong.

Research IT said that there has not been a lot of challenges when it comes to employees not following ethical guidelines, but also said it was one incident that was very serious, but it had been dealt with afterwards and mentioned it was important for them to follow the laws too. Research IT said there have been some security incidents where some research data from employees were brought with them out of the company when the employee quit. They have guidelines in Research IT which says employees can’t for example bring analysis data that are not open when they quit. It will then be seen as stealing from their company.

Retail IT focuses on individual teams, which means they have different principles and guidelines they follow from one team to another. That's why it is important for the leaders to get their team members to comply with their principles and guidelines. Retail IT does not focus on punishing the employees that don't follow the guidelines, but if there are mistakes made there might be some type of punishment. They have also implemented ways for their employees to tell if they have made a mistake. This can be done through a whistleblower channel if they want to be anonymous.

Infrastructure IT does not mention much about challenges with their ethical guidelines or framework, but mentions they have a whistleblower forum/channel that the employees can contact if they do not want to discuss situations directly with their boss or want to notify on incidents. They also have different guidelines implemented in their organization that are about anti corruption and not getting bribed. They have a code of conduct which says they can fire

the employee if they do not follow it. They have several variants of means, one of which is reprimand that you get feedback from the boss. It is more common to get a letter saying that if you do this again you can get fired.

Environment IT says they are sure that there are some employees that struggle to follow the ethical guidelines all the time. In their management systems there is information about the consequences of not following the code of conduct. They also mention that in some ethical frameworks there are procedures that explain how to follow the guidelines and that it is a requirement to have those procedures. Environment IT have had problems with employees selling information and other more unintentional things such as trying to finish their work task faster by cutting corners.

Health IT uses a metaphor where they describes they have a lot of employees which can be seen as a big norwegian city and there is at least one village idiot, it is their challenge to ensure that the employee is protected from harming themselves and they have said "that they do not leave it to the individual to, for example, take a position on whether an email contains malware or not. That is why they have implemented a bunch of restrictions for the employees on what they can do within the Information communication technology (ICT) area. Health IT also says they use technical tools to a large extent to restrict the employees' ability to do things that may be contrary to the ethical guidelines which can be application restrictions as they have had challenges with that in the past.

Defense IT has an impression that most of their employees follow their guidelines and policies. Our guidelines and policies are generally not a one-size fits all, so there will always be some kind of deviation. But Defense IT thinks that the deviations that are happening are thought through and justified.

Service IT said their job was to pass on this culture to new employees. So they have a relatively comprehensive program, but these values that they have in daily life affect pretty much everything they do. They are about equality and respect for the individual and the fact that they should be allowed to make mistakes, for example. That they never stand with the whip to blame anyone. So if there is someone who comes in and can not identify with the values they have, then they choose that this is not the place for them. Service IT also said that there haven't been many problems with employees not following the ethical guidelines. There have been some situations where some have been put aside and said that this perhaps should not be repeated and done so. They said people live by the guidelines and have understood how to do things and there is openness and even justice and small not deviations, but a direction that is not right with us then they take it.

To summarize this chapter when it comes to challenges with ethical guidelines and ethical frameworks:

- None of the respondents felt there were any challenges when it comes to that topic of area on how they apply the ethical frameworks, guidelines and rules in their organization.
- The organizations do imply that there are or can be challenges with employees following those ethical guidelines and frameworks in their organization.

4.4 Security Measures and Security Testing

When it comes to security testing most of the organizations either outsourced their testing or did it themself. What was interesting was how they did them, some of the organizations did not use phishing campaigns as one of their testing methods. The reason for this is that they did not see the benefits in tricking their employees in clicking malicious links. They meant that there was a big risk in someone clicking something they probably should not have clicked, and that phishing campaigns did not help prevent this. It is also not a good idea to trick the employees as they don't know how they will react. Some might be mad and angry or feel stupid for being fooled. There is also an ethical dilemma in it as if the employee should be punished or not for doing something wrong and being caught. Other organizations which used phishing campaigns were positive about it and said that method is used for learning and not catching someone doing something wrong. If they had some employees that clicked the link then they would go through a course for the employees as a whole to learn more about not clicking something they don't know what is. While other organizations gave out notice to the employee with information that they can learn from.

There were also a lot of the organizations which focused on good access management and least privilege. It is important for them to have a good grasp on who can do what and that they should not have more privileges than needed. The organizations also used a lot of surveillance when it came to endpoint protections, detection and logs. Most had different services that used AI. In the different security technologies there are ethical dilemmas and guidelines that are needed. That's because there might be bias in the algorithms and technology, which makes it so that it focuses more on one type of data traffic or data instead of looking at the whole picture. This might make an organization more vulnerable and the security technology less dependable. That's why it is important to have ethical guidelines for those technologies so that they won't be biased towards different data traffic and data.

4.5 Privacy and Laws

When it comes to privacy and laws, most of the organizations have their own legal department, employees and data protection representatives that work with privacy issues or privacy information that has to be set up and informas what they are going to work with, why they are going to work with it and how they are going to work with it. Some of the organizations also have a data protection officer that works to comply with privacy. For them it is about identifying which relevant laws and rules in the GDPR and the Personal Data Act apply to their organization. To create a good structure for them, it is about what access and privileges you should give to users when it comes to personal data and how long the organization can store and keep the data. The employees in the organizations also get training in a way that the end users must think about what type of data they are handling, either if it is classified information such as sensitive information and personal data or non-sensitive data.
One of the organizations uses a group compliance officer that has the main responsibility of privacy and a global privacy officer that reports to the CTO. It also has a compliance network with data protection managers in different business areas and meetings where they adhere to what datatilsynet says they must do regarding breaches. That they must also follow up in relation to the privacy network.

This section will conclude the findings chapter by stating the most important findings and information that were found throughout the interviews:

- Most of the organizations focuses on values such as integrity, openness, transparency and trust
- Most of the values and the ways in which the organization works with ethics fits into two of the three frameworks. All of the organizations work with ethics which relates to the principlist framework and some of the organizations use a mix between the principlist framework and human-right/right-based framework.
- Some of the ethical standards and ways to work with ethics in the organizations are focused on De Facto standard and principles.
- The ethical standards which were found in some of the organizations were based on other standards that had ethical guidelines that needed to be followed to keep that standard.
- The organizations focus on giving the employees channels to give feedback or inform about mistakes.
- The organizations don't use a specific ethical framework in general or towards cybersecurity, but instead use ethics as values for the whole organization to follow.

5. Discussions

The thesis found out in the different interviews that the organizations were using different approaches to ethics, but had values and concepts which put them under the same ethical frameworks that were found in the literature review. Most of the organization did not use any specific ethical frameworks or haven't heard about it in a cybersecurity context. Throughout the interviews the researchers were able to identify what core concepts and values the organizations use in their ethics as well as cybersecurity, this can be seen in table 9. The researchers were able to identify which types of ethical frameworks the different organizations fit into and use in their ethical guidelines and policies. The most used and common framework that was identified throughout the different organizations was the principlist ethical framework, but there were also other types of framework found through the interviews. Some of the organizations also used a mix of the principlist framework and human-right/right-based framework. Those were identified by the information that the interviews and organizations provided. Table 9 shows an overview of the different organizations in and shows what type of ethical framework or mix that they most likely use in their organization. This is discussed so that organizations can see which ethical framework fits their values and concepts and improve both their ethics and security. In chapter 5.2 the researchers will provide information about the common frameworks found and suggest which one of them organizations can use towards their ethics in their organizations. Lastly in chapter 5.3 there will be provided information on why the findings does not suggest that any of the organizations uses contextual framework for their ethics.

5.1 Key Ethical Concepts, Values and Principles

This chapter will go through which types of ethical frameworks were found in the different organizations throughout the interviews. This is done by looking at key concepts and values for the organizations and comparing them to the core values and concepts of the ethical frameworks. This is done since all the organizations did not have or use a specific ethical framework for cybersecurity. The table below shows what type of key concepts and values the organizations have and which ethical frameworks that fits under those concepts and values the most.

No	Ethical Frameworks	Key Concepts and Values	Organization
1	Principlist Framework/ Human-right/Right-based	Morales and establish attitudes Own values to their institution Pride Humanity Innovation and loyalty Sustainability Diversity Openness Trust Professionalism	Education IT

		Respect, care and seriousness Follow rules and laws	
2	Human-right/Right-based Framework / Principlist Framework	Privacy Leaste privilege Moral values Trust Openness culture Rights consideration Traffic light protocol	Knowledge IT
3	Principlist Framework	Least privilege Systems do the monitoring of traffic Trust Principles	Government IT
4	Principlist Framework	Trust Good behavior Integrity Privacy Care Collaboration Laws	Audit IT
5	Principlist Framework	Openness Honesty Availability Follow the law HMS-security Respect Compete fairly and ethically Trust	Research IT
6	Principlist Framework	Privacy Transparency Principles Responsibility Laws Independent	Retail IT
7	Principlist Framework	Values and humans Cooperation Openness Trust Future-oriented Responsible Curious	Infrastructure IT

		Culture and value-based management Traffic monitoring	
8	Principlist Framework	Anti fraud Trust Safeguard life, property and environment Transparency Principles and policies	Environment IT
9	Human-right/Right-based/ Principlist Framework	Respect Predictable Competent Deliver quality Transparent Traffic monitoring Least privilege Openness Strict access policy Laws and regulations	Health IT
10	Principlist Framework	Trustworthiness Privacy Customer loyalty Freedom Autonomy Sharing culture Principles	Service IT
11	Principlist Framework	Integrity Credibility Trust Security monitoring	Defense IT

Table 9: Ethical frameworks identified for the organizations

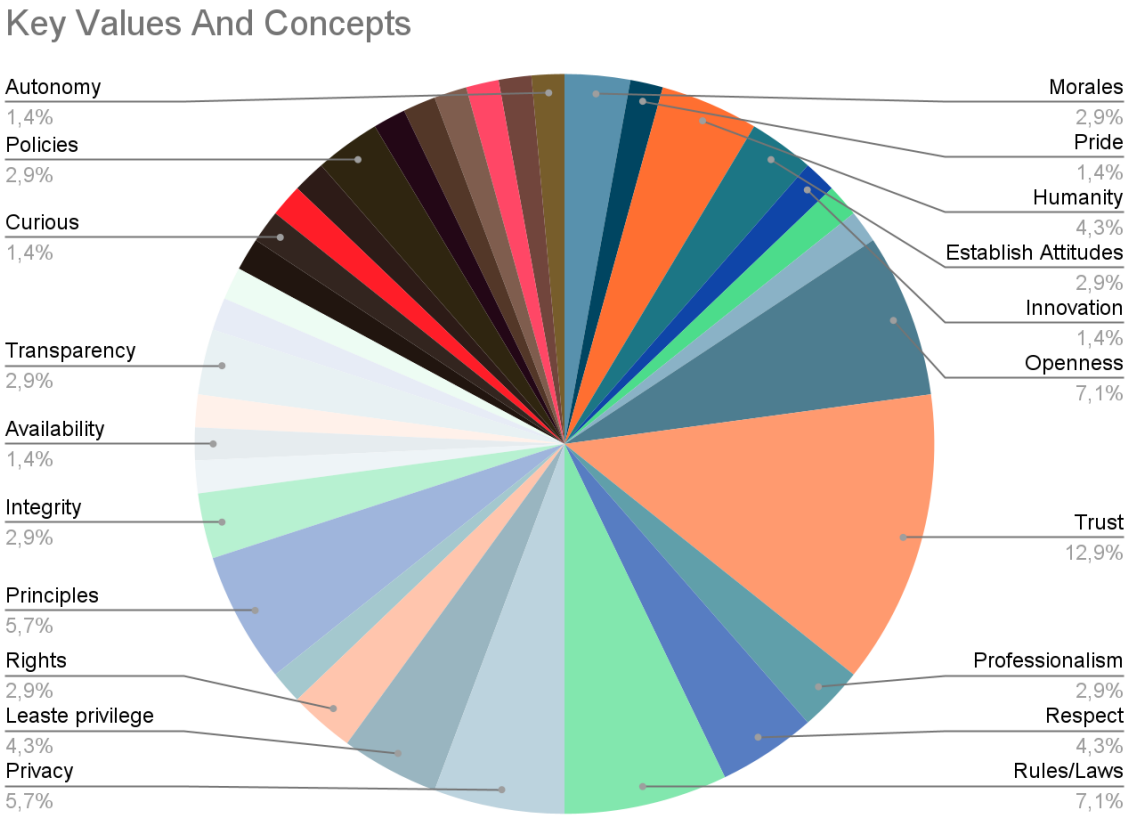


Figure 6: Ethical Key Values And concepts From Interviews

Education IT values and concepts when it comes to ethics fits into the principlist framework and human-rights/right-based framework. The values and concepts which Education IT relates to in the principlist framework are beneficence which focuses on the benefits of cybersecurity technologies towards humans, human well-being, and making lives better. Education IT values and concepts that go well with this principle are morales, established attitudes, humanity, professionalism, respect, care, and seriousness. The next principle which Education IT relates well with is justice. This principle focuses on fairness, equality, and impartiality. The values and concepts that go well with this principle are respect, care, seriousness, professionalism, trust, openness, laws and rules. Another principle which Education IT values and concepts have relations to is autonomy, which focuses on letting humans make informed decisions for themselves. In this case the different values that relate to this principle are their own values to their institutions, and diversity. The last principle in which Education IT relates to is explicability, this principle focuses on cybersecurity being intelligible, transparent and comprehensible. The different values and concepts from Education IT that relate to this principle are openness, trust, morals, established attitudes, sustainability, rules, laws, and professionalism (Formosa et al., 2021). Education IT similarities in their ethics towards human-rights/right-based framework are that they focus on human rights, laws and rules. It is important for them to protect and control the privacy of their employees and users. They have a lot of different guidelines, principles and policies which focus on the rights of the users, employees and the data which they work with.

Knowledge IT values and principles fits into the human-right/right-based framework and the principlist framework. In their organization moral values, trust and openness culture is important. Moral values that fit the human-right framework are laws and rules. They have a balance between humans right on how the systems should monitor the users and how security is achieved within their organization. The systems do not actively analyze every move and report it to the IT department to see when they come and leave the job, but it is used if crime is involved. When it comes to the principlist framework Knowledge IT uses principles such as least privilege, openness, trust and a traffic light protocol. The main principles that Knowledge IT relates to in the principlist framework are beneficence, non-maleficence, autonomy and justice.

Government IT focuses on using principles to run their ethical guidelines, security measures and systems. They focus on principles such as least privilege, system monitoring and trust. By looking at how they work with cybersecurity as well as ethics, there is no mistaking that their way of doing it relates the most to the principlist framework. The principles in which they relate the most to in the principlist framework are beneficence, non-maleficence, justice and autonomy.

Audit IT uses principles like trust, good behavior and integrity when it comes to their ethical guidelines and how they operate in their organization. These values and values like caring for others are important for them. This makes Audit IT relate to the principlist framework when looking at how they work with ethics and cybersecurity. The principles in the principlist framework which they uses are beneficence, non-maleficence, autonomy, justice

Research IT uses a type of ethical compass that relates to all of their ethical guidelines, policies and rules. This compass builds upon different principles and ethical values such as respect, justice, anti corruption, openness, trust and equal rights. They build some of their ethical guidelines upon security standards such as ISO 27001 and NIST. Through the interviews it was clear that the way Research IT works with ethics are closely related to using principles and therefore similar to the principlist framework. Some of the principles that they relate to in the principlist framework are beneficence, autonomy, justice and explicability.

Retail IT focuses on three key principles when it comes to their ethical guidelines in their organization. Those three values are privacy, transparency and responsibility. They also are required to follow guidelines and laws based on the country they operate in. These values correlate to the principlist framework and the values in this framework like beneficence, non-maleficence, autonomy, justice and explicability.

Infrastructure IT uses a lot of guidelines and policies in their organization. One thing they have a big focus on is their code of conduct. This code helps their employees to understand how they are supposed to behave and work in the organization. This code also contains what type of ethics and values that they focus on. The main ethical values that they have are openness and trust, but they also focus on values such as future-oriented and responsibility. Some other values that the code of conduct focuses on are personal conduct values such as integrity, diversity, confidentiality, privacy and sustainability. By looking at Infrastructure IT's code of conduct and the information that was collected through interviews there is a big similarity towards the principlist framework. The reason for this is that the ethical and organizational values that Infrastructure IT has are based upon different principles, rules and

laws. The main principles that Infrastructure IT relates to in the principlist framework are beneficence, non-maleficence, autonomy, justice and explicability. Some cybersecurity services that Infrastructure IT offers are collaboration teams against cybercrime. They have incident response teams which help other organizations to handle incidents such as ransomware or other types of attacks. Infrastructure IT also uses phishing campaigns to test their own employees' security abilities and how easy they are tricked.

Environment IT uses guidelines and code of conducts that implies for everyone in that organization. This code of conduct is used for everything not just cybersecurity, but to reduce fraud and all types of critical factors for their organization. The most important value in Environment IT is trust and that people can trust their organization. They also have other important values which are safeguarding life, property, environment and transparency. These values correlate to the principlist framework and values like beneficence, non-maleficence, autonomy, justice and explicability. They also use phishing campaigns to test the employees for phishing attacks so the employees are better prepared if they are attacked by cyber criminals. They use this technology and method to benefit the employees so they can get training on simulated attacks and the attacks are not there to punish or harm them if they mistakenly click on a link.

Health IT was one of the organizations with the most strict rules, guidelines, principles and policies. Their focus on different values and concepts fits them into two of the ethical frameworks which are human-right/right-based framework and principlist framework. When it comes to the human-right/right-based framework they have a big focus on securing their users' data. Their focus is on protecting human rights over what would enable them to make their work easier. The principles and values which relate to the principlist framework are that they focus on the different principles such as openness, trust, respect, transparency, least privilege and strict access policy. Health IT have strict access policies and have removed social media and other channels on their network to reduce the attack surface for hackers and other aggressors. When it comes to least privilege they use it to reduce the mistakes and ethical dilemmas that their employees can end up in. The main principles in the principlist framework in which Health IT relates their ethics the most towards are beneficence, non-maleficence, autonomy and explicability.

Service IT focuses on different types of principles in their organization for their guidelines and cybersecurity solutions. The values they use are trust/trustworthiness, privacy, loyalty, freedom, autonomy and respect. They also have a sharing culture in service IT and security culture has been a pillar in recent years and put in focus. Service IT also uses phishing campaigns within their organization and they use this technology and method to teach the employees and they simulate phishings attacks on all employees and leaders when they do this campaign. For them they want the leaders to also report deviations and give notice if they have done something wrong so they can benefit from that in the longer run. These values, technologies and methods that are used in Service IT correlates to the principlist framework and values like beneficence, non-maleficence, autonomy, justice and explicability.

Defense IT used an information security management system(ISMS) which contained their guidelines, principles, rules and policies. This system was based on the ISO 27001 security framework, but also had elements from NIST, CIS controlls and GDPR. Their key value in the organization is trust and is seen throughout their work. The ethical framework in which

the researchers have identified that Defense IT relates the most to is the principlist framework. The reason for this is that Defense IT works with a management system that uses documents with principles, policies and rules that shows that they base their work upon different principles. The principles which Defense IT relates the most to in the principlist framework is beneficence, non-maleficence and autonomy.

This table shows the core values and concepts for the different ethical frameworks found in the literature, and which of the values and concepts that were identified in the different organizations throughout the interviews.

Organization	Ethical Frameworks Values and Concepts							
	Principlist Framework					Human-Right/Right-Based Framework		
	Beneficence	Non-mal eficence	Autonomy	Justice	Explicability	Privacy	Rights	Prima Facie Duties
Education IT	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Knowledge IT	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Government IT	Yes	Yes	Yes	Yes	No	Yes	No	No
Audit IT	Yes	Yes	Yes	Yes	No	Yes	No	No
Research IT	Yes	No	Yes	Yes	Yes	Yes	No	No
Retail IT	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Infrastructure IT	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Environment IT	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Health IT	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Service IT	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Defense IT	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Table 10: Ethical frameworks values and concepts

Most of the organizations based on the interviews used ethical guidelines or code of conducts that referred to ethical values and concepts that the employees of the organizations had to follow and adapt. One of the organizations also had created an ethical compass for their values which the people are obligated to follow in the projects they are placed in. The employees of this organization should also know about the guidelines that are placed in this ethical compass. Most organizations have different core values, but most of them are obligated to follow ethics which are based on principles. Some keywords of ethics and values that were brought up during the interviews were trust, transparency, openness, privacy and cooperations. Most of them also used the systems and technologies to not harm the users, but to benefit them in good ways. These are values and principles that correlate to the principlist framework from the literature. There were some organizations that used and followed ethical

standards. Some of those ethical standards had to be followed based on certifications or else they could lose that certification. An example of this ethical standard was the ISACA standard and CISA were they are obligated to follow international ethical guidelines for that organization. Two of the organizations used de facto standards for their companies. Another organization used the EU's charter and code which consist of principles grouped in some main areas like ethical and professional aspects, recruitment and selection, working conditions and social security, and training and development. Another organization used and followed a standard called ISF standard of good practice and built their security controls based on how the standards of good practice is set up, but that standard is more of an information security standard and not so much about ethics.

5.2 Ethical Frameworks Recommendation

This section will focus on suggestions for what type of ethical framework that Norwegian organizations can implement to increase their ethical awareness and better their guidelines, regulations, laws and policies when it comes to cybersecurity. When it comes to an organization's ethical stance Shoemaker et al. (2019) states that “A corporation’s ethical stance has direct bearing on the way an organization defines and executes its commitment to the confidentiality, integrity, availability, non-repudiation and authorization of its information”. That's why it is important for organizations to choose an ethical framework which helps them maintain and protect those values. Shoemaker et al. (2019) also state that “A company’s commitment to cybersecurity can be recognized by their thoughtfulness and adherence to a documented and practical ethical framework.” The two models in which the researchers found out fitted the best with Norwegian organizations and ethics in the context of cybersecurity was a combination of principlist framework and human-right/right-based framework or just the principlist framework. The organizations which should choose the combination of principlist framework and human-right/right-based framework are the organizations which work with a lot of sensitive data and are responsible for it. The reason for this is that it is a lot more important for those organizations to reduce the risk of breaking human right laws and regulations, their main focus will be to reduce the trade off risk of rights to null. These organizations also need good relevant principles which will help them maintain their security abilities and reduce the mistakes made by employees, therefore a combination of the frameworks is a good idea. The other model which is just a principlist framework is for organizations that don't work with a lot of sensitive data. Those organizations do not need to focus that much on human rights and instead can focus on using the principles from the principlist framework. Those principles can be used to define and make good ethical guidelines which makes it easier for employees to make good ethical decisions, when they are put in ethical dilemmas. This helps them make good and decisive decisions which helps maintain the security and reduce the threats.

Model A: Principlist framework/Human-Right/Right-Based framework

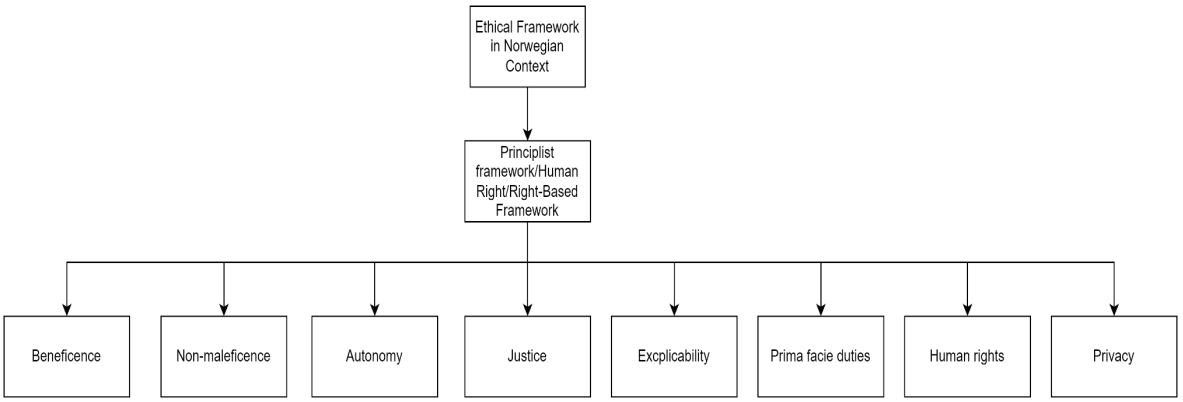


Figure 7: Model A, combination of principlist and human right framework

Model B: Principlist Framework

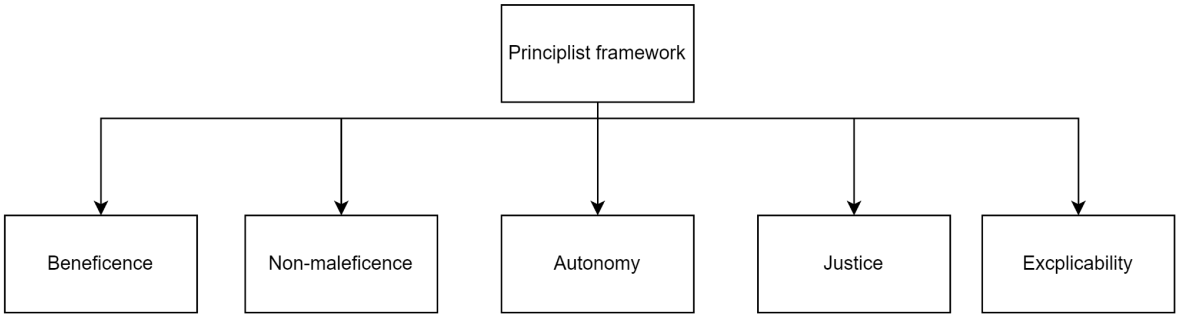


Figure 8: Principlist framework

5.3 Ethical Perceptions in Norwegian Organizations

There were different ways that the organizations that were interviewed adapted ethics into their organizations as well as cybersecurity. Some of the organizations used ethics as a fundamental part of their culture. Since they think this way it is important for them to hire different people who accept and own those ethical values and morals that the organizational culture is based upon. In the Norwegian organizations which were interviewed the culture and ethics were based on deontological systems such as principles, rules and guidelines. The organizations used codes of conduct to tell how their employees work, but it is up to the individual to adapt and understand those codes. While in other parts of the world like many cultures in East Asia, deontological systems may focus more on duties. Those are fixed obligations to others (parents, siblings, rulers, fellow citizens etc.) that must be fulfilled according to established rules of conduct that govern various types of human relationships. Which means that there are more strict duties to how people perceive the rules and norms, this reduces the individual's ability to follow those duties, rules and norms in their own way (Vallor & Rewak, n.d).

No single, detailed code of cybersecurity ethics can be fitted to all contextes and practitioners. Organizations and professions should therefore be encouraged to develop explicit internal policies, procedures, guidelines and best practices for cybersecurity ethics that are specifically adapted for their own activities and challenges (Vallor & Rewak, n.d). However those policies, procedures, guidelines and best practices should be based upon an ethical framework which fits the organizations culture, ethics and values. As seen in the different interviews most of the organizations adopt similar ethical values, but still have different ways to how they adopt those values into guidelines, procedures and policies. This is done because they develop them to fit into their culture and in the area in which the different organizations work. This can be seen as in the organizations that work with sensitive information. They adopt a combination of ethical frameworks because they need to focus on the rights of their users, but still base most of their ethics on principles. While most of the other organizations which don't manage sensitive data focus on principles as their base for ethics, guidelines, procedures and policies.

The third framework that was found in the literature review was the Consequentialist framework which theories derive from ethical principles to guide moral action from the likely consequences of those actions. The most known form of consequentialism is utilitarian ethics, which uses principles of the “greatest good” to determine what the moral obligations are in any given situation. The good in utilirism is measured in terms of happiness or pleasure. The reason that most of the Norwegian organizations do not use this ethical framework, when it comes to cybersecurity is because you can not base your cybersecurity guidelines and principles on what the employee thinks is the morally best in a dilemma or situation. Cybersecurity is based upon following laws, standards and regulations and the decisions in cybersecurity needs to be done in a way that follows these laws, standards and regulations. If the organizations would have every employee decide what is the best decision in a cybersecurity situation based on their ethical morals and what is the “greater good” in their opinion. They might put the organization in a vulnerable state in which criminals may be able to exploit the organization.

6. Conclusion

This thesis work focused on exploring what type of ethical frameworks are connected in the context of cybersecurity and what type of ethical guidelines, standards and frameworks Norwegian organizations use. This research was done using qualitative research to find out what type of ethical frameworks Norwegian organizations use in their organization in the context of cybersecurity. The research has provided information such as which ethical framework the Norwegian organizations interviewed relates the most to, but also found out that most of the organizations don't use any specific framework for their ethics in general and in the context of cybersecurity. The frameworks in which most of the Norwegian organizations related to were the principlist framework and the human-right/right-based framework. The researchers would recommend organizations to learn more about ethical frameworks in general, but also look at the ethical frameworks connected to cybersecurity as this can help them develop good guidelines, procedures, policies and rules that will help them maintain good security and reduce the mistakes that users and employees might make in the context of ethical dilemmas.

The most important findings in the thesis is as follows:

- Norwegian organizations use either principlist framework or a combination of principlist framework and human-right/right-based framework for their ethics.
- Norwegian organizations should look more into adopting frameworks for ethics which can help improve decision making and reduce mistakes.
- None of the organizations interviewed had heard about or knew about ethical frameworks in the context of Cybersecurity.
- Norwegian organizations use ethical guidelines for their ethics and trust, openness, and transparency were key values for the organizations.
- Most of the organizations based their ethics on the organizations as a whole and did not have any specific ethics or ethical frameworks used for only cybersecurity.
- Some organizations use ethical standards and have ethical guidelines they follow, while other organizations use the De Facto Standard.

6.1 Research Contribution

This research work highlighted the lack of knowledge and interest around ethical frameworks used for cybersecurity in Norwegian organizations. When it comes to the literature the ethical frameworks which are connected to cybersecurity was not a deeply studied topic. In this case the research contributed to look at if there were any differences between how different sectors worked with ethics when it came to cybersecurity. The literature stated that the principlist framework was the most used one when it came to cybersecurity, and throughout this research the researchers have found out that this is the case. There are also organizations which use values and concepts which can be found in other frameworks as well. Therefore when it comes to the literature this research contributes by finding out that principlist frameworks is the most used in Norwegian organizations, but that they also use different values and concepts from frameworks such as human-right/right-based frameworks.

The research helps organizations to look more into ethical frameworks and how it can help them make good ethical guidelines and policies which will help maintain their overall security and improve decision making. It will also give suggestions on which framework organizations should use. The research also brings awareness to organizations, to make them aware that ethical frameworks for cybersecurity exist and it can be helpful to look at what ethical frameworks fit for their organization.

6.2 Limitations

Due to the lack of awareness of ethical frameworks in cybersecurity within the Norwegian context, it can impact the quality of the responses and data found in the research. Another limitation is related to the background of the organizations participating in the study, the researchers have not been able to get feedback from policy makers or regulators as they declined the interview request or they have given a generic answer, "we follow all the guidelines". There were also limitations when it came to the subject's understanding of ethics and ethical frameworks in the context of cybersecurity. The reason for this was that they did not have in-depth knowledge about the ethics in their organization, and therefore made it harder to clearly understand how they adopted the values and concepts and how they worked with it.

6.3 Reflection

Due to the novelty of the topic in the cybersecurity area, the researchers are satisfied with the research result as it is something that havent been looked at before. It was interesting to see that no organizations that were interviewed had heard or used any specific ethical framework for cybersecurity. The challenges in which the researchers encountered was firstly that there wasn't much research on ethical frameworks used in cybersecurity context. This made it harder to connect the organizations to the ethical frameworks that were connected to cybersecurity. The second challenge was getting organizations willing to help with the research. Most of the organizations that were contacted either did not respond or did not feel like they could help with answering the research questions or questions for the interviews or they felt they were not the right fit or position in the company to answer to that topic. So some changes that might or should have been done differently were how we informed the organizations about the research and how the researchers structured and made the questions for the interview guide. The approach should have been different to make it easier to understand what the researchers wanted to find out then maybe more organizations would have been more eager to join in on the research. The last problem was that since the organizations did not use any specific ethical frameworks, then the researchers were forced to look at the data they obtained throughout the interviews and information on their websites to look at which ethical framework they related the most to. By doing it this way the researchers might have overlooked something which might have changed which ethical framework some of the organizations would fit into.

6.4 Future Work and Research

The future work for this research would be to interview more organizations and hopefully get a few organizations which use ethical frameworks. If they don't, the research should focus on

going deeper into a few organizations to understand and observe their ethics better so that it would be easier to understand which ethical frameworks the organizations relate to or are similar to. If not then the research could look into how having formal ethical frameworks towards cybersecurity could help and improve the security of the organization and reduce situations where ethical laws and guidelines are broken or ethical dilemmas are solved in a way that is not done correctly. A lot of the organizations that have been interviewed connect their ethical frameworks, guidelines and standards to their culture. Therefore it is important to look at how to develop a good security culture. Developing and sustaining an effective security culture is an essential component of a protective security regime and helps mitigate against a range of threats that could cause physical, reputational or financial damage to organizations. Security culture refers to the set of values, shared by everyone in an organization, that determine how people are expected to think about and approach security. Getting security culture right will help develop a security conscious workforce, and promote the desired security behaviors you want from employees (Center for the Protection of National Infrastructure, 2021). Security cultures' effect on ethical frameworks can be interesting to look at for future research.

References

Adams, W. C. (2015). *Conducting semi-structured interviews*. Handbook of practical program evaluation, 4, 492-505. https://books.google.no/books?hl=no&lr=&id=zntNhoO6gCUC&oi=fnd&pg=PA365&dq=Conducting+Semi+Structured+Interviews%0A&ots=UoilE5fNXV&sig=t_diVnHF9YAT3ersoCDQ1u4X7qg&redir_esc=y#v=onepage&q=Conducting%20Semi%20Structured%20Interviews&f=false

Alleydog. (n.d.). *Ethical Guidelines.* Retrieved 14. February 2022 from: https://www.alleydog.com/glossary/definition.php?term=Ethical+Guidelines

Anderson, R. (2007). *Thematic content analysis (TCA)*. Descriptive presentation of qualitative data, 1-4. http://rosemarieanderson.com/wp-content/uploads/2014/08/ThematicContentAnalysis.pdf

Archer, M., Bhaskar, R., Collier, A., Lawson, T., & Norrie, A. (2013). *Critical realism: Essential readings*. Routledge. https://www.taylorfrancis.com/books/mono/10.4324/9781315008592/critical-realism-margaret-archer-roy-bhaskar-andrew-collier-tony-lawson-alan-norrie

Babbie Earl, R. (2010). *The practice of social research*. Belmont. Social Science, 566. https://libguides.usc.edu/writingguide/quantitative

Beauchamp, T. L., & Rauprich, O. (2016). Principlism. Ten Have H, organizador. Encyclopedia of Global Bioethics. Zurique: Springer, 2282-93. https://www.researchgate.net/publication/305377008_Principlism

Blanken-Webb, J., Palmer, I., Campbell, R., Burbules, N. C., & Bashir, M. (2019). *Cybersecurity Ethics.* Foundations of Information Ethics, 91-101. https://books.google.no/books?hl=no&lr=&id=hUOgDwAAQBAJ&oi=fnd&pg=PA91&dq=ethical+framework+in+cybersecurity&ots=IPaFnOAJ-N&sig=BMPszlhfZJlfmdXTtkR3zxZb9KY&redir_esc=y#v=onepage&q=ethical%20framework%20in%20cybersecurity&f=false

Blanken-Webb, J., Palmer, I., Deshaies, S. E., Burbules, N. C., Campbell, R. H., & Bashir, M. (2018). *A case study-based cybersecurity ethics curriculum*. In 2018 USENIX Workshop on Advances in Security Education (ASE 18). https://www.usenix.org/system/files/conference/ase18/ase18-paper_blanken-webb.pdf

Cantrell, S. (2010). LibGuides: Qualitative Research: Journals. https://guides.library.duke.edu/c.php?g=289813&p=1934020

Carpenter, T. (2012). *Electronic publishing standards.* In Academic and Professional Publishing (pp. 215-241). Chandos Publishing. https://www.sciencedirect.com/topics/computer-science/de-facto-standard

Caulfield, J. (2019). *How To Do Thematic Analysis. A Step-By-Step Guide & Examples.* Scribbr.
https://www.scribbr.com/methodology/thematic-analysis/

Chetty, P. (Sep, 2016). *Limitations and weakness of qualitative research methods.* Project Guru.
https://www.projectguru.in/limitations-quantitative-research/

Chetty, P. (Oct, 2016). *Importance of research approach in a research. Research design strategy.*
https://www.projectguru.in/selecting-research-approach-business-studies/

Center for the Protection of National Infrastructure. (Mar, 2021). *Security Culture.* Retrieved January 12 2022. CPNI
https://www.cpni.gov.uk/security-culture

Datatilsynet. (Oct, 2021). *Om personopplysningsloven med forordning og når den gjelder.*
https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om-personopplysningsloven-og-nar-den-gjelder/

Datatilsynet. (Jan, 2018). *Artificial intelligence and privacy*.
https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

Davis, B. (Apr, 2021). *What is the hypothesis in quantitative research?*. MVOrganizing.
https://www.mvorganizing.org/what-is-the-hypothesis-in-quantitative-research/

Davis, B. (Jun, 2019). *What are the 4 types of qualitative research design?*. MVOrganizing.
https://www.mvorganizing.org/what-are-the-4-types-of-qualitative-research-design/

Duignan, B. (2021). *Utilitarianism*. Britannica.
https://www.britannica.com/topic/utilitarianism-philosophy

Dupuis, M., & Renaud, K. (2021). *Scoping the ethical principles of cybersecurity fear appeals*. Ethics and Information Technology, 23(3), 265-284.
https://link.springer.com/article/10.1007/s10676-020-09560-0#Sec17

Euraxess. (n.d). *The European Charter & Code for Researchers.* Retrieved 10. December 2021 from: https://www.euraxess.no/jobs/charter

Ferguson, S., Thornley, C., & Gibb, F. (2015). *How do libraries manage the ethical and privacy issues of RFID implementation? A qualitative investigation into the decision-making processes of ten libraries.* Journal of librarianship and information science, 47(2), 117-130.
https://journals.sagepub.com/doi/full/10.1177/0961000613518572

Forum Incident Response Security Teams. (2016). *CSIRT Education Services.* FIRST. https://www.first.org/education/first-csirt-services-education-framework-first-final-draft.pdf

Fontana, A., & Frey, J. H. (2000). *The interview: From structured questions to negotiated text.* Handbook of qualitative research, 2(6), 645-672. https://chip.uconn.edu/wp-content/uploads/sites/1245/2019/05/Fontana-Frey-2000-in-Denzin-Lincoln-Eds-The-Interview-From-Structured-Questions-to-Negotiated-Text.pdf

Formosa, P., Wilson, M., & Richards, D. (2021). *A principlist framework for cybersecurity ethics. Computers & Security,* 109, 102382. https://www.sciencedirect.com/science/article/pii/S0167404821002066

Gaudine, A., & Thorne, L. (2001). *Emotion and ethical decision-making in organizations. Journal of Business Ethics*, 31(2), 175-187. http://web02.gonzaga.edu/orgl/orgl503/Articles/Article5.pdf

George, T. (Mar, 2022). *Exploratory Research | Definition, Guide, & Examples.* Scribbr. https://www.scribbr.com/methodology/exploratory-research/

Griffin, C. (2002, January). *The advantages and limitations of qualitative research in psychology and education.* In Proceedings of conference on 'Quantitative and Qualitative Research: Applications in Psychology and Education' organised by The Psychological Society of Northern Greece and the School of Psychology, Aristotle University, Thessaloniki, Greece. https://www.researchgate.net/publication/310480387_The_advantages_and_limitations_of_qualitative_research_in_psychology_and_education

Gotterbarn, D. W., Brinkman, B., Flick, C., Kirkpatrick, M. S., Miller, K., Vazansky, K., & Wolf, M. J. (2018). *ACM code of ethics and professional conduct.* https://dora.dmu.ac.uk/bitstream/handle/2086/16422/acm-code-of-ethics-and-professional-conduct.pdf?sequence=1

Hess, J. L., Beever, J., Zoltowski, C. B., Kisselburgh, L., & Brightman, A. O. (2019). *Enhancing engineering students' ethical reasoning: Situating reflexive principlism within the SIRA framework.* Journal of Engineering Education, 108(1), 82-102. https://onlinelibrary.wiley.com/doi/10.1002/jee.20249

ISACA. (Sep, 2020). *Standards, Guidelines, Tools and Techniques.* https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/standards-guidelines-tools-and-techniques

Information Security Forum. (2022). *The ISF Standard of Good Practice Online Informative References to NIST CSF.* ISF. https://www.securityforum.org/solutions-and-insights/isf-sogp-olir-to-nist-csf/

Information Security Forum. (2020). *Standard of good practice online informative references to NIST CSF*. ISF. https://www.securityforum.org/services/standard-of-good-practice/

Jamshed, S. (2014). *Qualitative research method-interviewing and observation.* Journal of basic and clinical pharmacy, 5(4), 87. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4194943/

Kaiser, M. (March, 2019). *Quantitative methods.* The Norwegian National Research Ethics Committees. https://www.forskningsetikk.no/en/resources/the-research-ethics-library/methods/quantitative-methods/

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering.* https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., ... & Moher, D. (2009). *The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration.* Journal of clinical epidemiology, 62(10), e1-e34. https://www.sciencedirect.com/science/article/pii/S0895435609001802

Loi, M., & Christen, M. (2020). *Ethical frameworks for cybersecurity (Vol. 21, pp. 73-95).* Cham, Switzerland: Springer. https://library.oapen.org/bitstream/handle/20.500.12657/47324/9783030290535.pdf?sequence=1#page=88

Myers, M. D., & Newman, M. (2007). *The qualitative interview in IS research: Examining the craft.* Information and organization, 17(1), 2-26. https://www.sciencedirect.com/science/article/abs/pii/S1471772706000352

Macnish, K., & van der Ham, J. (2020). *Ethics in cybersecurity research and practice.* Technology in society, 63, 101382. https://www.sciencedirect.com/science/article/pii/S0160791X19306840

McNamara, A., Smith, J., & Murphy-Hill, E. (2018, October). *Does ACM's code of ethics change ethical decision making in software development?*. In Proceedings of the 2018 26th ACM joint meeting on european software engineering conference and symposium on the foundations of software engineering (pp. 729-733). https://dl.acm.org/doi/pdf/10.1145/3236024.3264833

Mustajoki, H., & Mustajoki, A. (2017). *A new approach to research ethics: Using guided dialogue to strengthen research communities (p. 254).* Taylor & Francis. https://www.researchgate.net/publication/317266149_A_New_Approach_to_Research_Ethics_Using_Guided_Dialogue_to_Strengthen_Research_Communities

Næringslivets Hovedorganisasjon (NHO). (n.d). *Fakta om små og mellomstore bedrifter (SMB)*. NHO. Retrieved 5. February 2022 from: https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/

Nunns, James. (Jul, 2016). *What is a framework?*. TechMonitor. https://techmonitor.ai/what-is/what-is-a-framework-4945801

Pathak, V., Jena, B., & Kalra, S. (2013). *Qualitative research.* Perspectives in clinical research, 4(3). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3757586/?fbclid=IwAR0BbDvJbnbn65-ATe3iwYX5eUOVHYJ3n7yCPu-Hp8Mk2BW1GKilwYK_KnU

PennState. (n.d). *What are ethical frameworks?*. Retrieved 5. December 2021 from: https://aese.psu.edu/teachag/curriculum/modules/bioethics-1/what-are-ethical-frameworks

Persson, A. J., & Hansson, S. O. (2003). *Privacy at work–ethical criteria.* Journal of Business Ethics, 42(1), 59-70. https://link.springer.com/article/10.1023/A:1021600419449#Abs1

Polonsky, M. J., & Waller, D. S. (2011). *Ethical considerations*. Designing and Managing a research project: A business student's guide. https://www.sagepub.com/sites/default/files/upm-binaries/4999_Polonski_Chapter_5.pdf

Reciprocity. (Feb, 2021). *The Importance of Ethics in Information Security.* Reciprocity. https://reciprocity.com/the-importance-of-ethics-in-information-security/

RealisingRights. (2022). *A Values Framework based on Human Rights.* RealisingRights. https://www.realisingrights.org.uk/index.php/1234

Shoemaker, D., Kohnke, A., & Laidlaw, G. (2019). Ethics and cybersecurity are not mutually exclusive. EDPACS, 60(1), 1-10. https://www.tandfonline.com/doi/full/10.1080/07366981.2019.1651516

Siponen, M. (2006). *Information security standards focus on the existence of process, not its content.* Communications of the ACM, 49(8), 97-100. https://www.researchgate.net/publication/220422725_Information_security_standards_focus_on_the_existence_of_process_not_its_content

Solove, D. J. (2008). *Understanding privacy.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888

Swedberg, R. (2020). Exploratory research. The production of knowledge: Enhancing progress in social science, 17.
https://books.google.no/books?hl=no&lr=&id=vlTMDwAAQBAJ&oi=fnd&pg=PA17&dq=exploratory+research&ots=lTrBh1XaZq&sig=wZKUxjGlixb2gU2J6D9Dt03khfE&redir_esc=y#v=onepage&q=exploratory%20research&f=false

Vallor, S, Rewak, J, W. (n.d). *An Introduction to Cybersecurity Ethics.* Retrieved 5. December 2021 from:
https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf

Wolford, B. (n.d). *What is GDPR, the EU's new data protection law?* Retrieved 21. January 2022 from:
https://gdpr.eu/what-is-gdpr/

Appendix

Appendix A - Interview guide

Vi er en gruppe på to ved navn Daniel Mikkelsen og Robert Zakariassen, vi studerer Master i cybersikkerhet med spesialisering i ledelse ved Universitetet i Agder. Oppgaven vår går ut på å se på hva slags etiske aspekter, teorier og verdier som blir lagt til i etiske rammeverk som brukes av organisasjoner for cybersikkerhet. Vi benytter ulike etiske rammeverk som teoretisk grunnlag for undersøkelsen, og det er viktig for oss å presisere at det ikke gjøres normative betraktninger av om det dere gjør er rett eller galt.

Oppgaven er utarbeidet sammen med våre masterveiledere Devendra Bahadur Thapa og Nadia Saad Noori fra Universitetet i Agder.

Informasjon om lagring av dataene som blir samlet inn, retningslinjer og samtykkeskjema vil bli sendt til deg i et eget dokument. Spørsmålene som blir stilt er basert på litteratur fra fagfeltet. Hvis du av en eller annen grunn ikke vil svare på spørsmålene som blir presentert, og eller hvis du av en annen grunn vil trekke deg ut av forskningsprosjektet, kan du gjøre dette til enhver tid.

Dette intervjuet er et semistrukturert intervju, der du blir bedt om å svare på forberedte spørsmål, men oppfølgingsspørsmål for utdyping av gitte spørsmål kan forekomme.

Anslått tid og varighet på intervjuet er mellom 30 minutter til en time. Dette intervjuet vil ta opp screen recording i form av lyd for transkribering. Har du noen spørsmål før vi begynner?

Introduksjonsspørsmål

1. Hvor lenge har du jobbet i bedriften?
2. Hva er din/deres rolle i virksomheten?
3. Hvor lenge har du jobbet med arbeid knyttet mot cybersikkerhet?
4. Jobber du eller kjenner du til de etiske rammeverk eller retningslinjer for cybersikkerhet og IT innenfor din bedrift?
5. Hva vil du kategorisere som et av bedriftens viktigste arbeidsoppgaver og verdier?
6. Hvilken etiske verdier er viktigst for bedriften?

Etiske verdier og retningslinjer

7. Hva er ditt forhold til de etiske verdiene og retningslinjene til bedriften?
8. Hvilket ansvar har du ovenfor disse verdiene og retningslinjene?

9. Hva slags arbeidsprosess går dere gjennom når dere ser på de etiske verdiene, retningslinjene og rammeverk for bedriften?
10. Følger dere noe spesifikk rammeverk i bedriften om det enten er et eget for cybersikkerhet eller IT systemene generelt?
11. Er de etiske retningslinjene basert på tillit eller prinsipper og moraler som må følges?
12. Hvordan følger de andre ansatte disse verdiene, retningslinjene og rammeverkene?
13. Hvilken roller er med å endre eller opprette etiske retningslinjer?
14. Er det noen bestemte etiske standarder som tas i bruk for bedriften?
15. Har dere noen form for etiske retningslinjer som må følges på grunn av sertifiserings opplegg?
16. Har det vært noen utfordringer når det kommer til deres etiske retningslinjer og ansatte som ikke følger dem?

Privacy and Laws

17. Hvordan jobber Organisasjonen med å opprettholde privacy?
18. Hvordan håndterer Organisasjonen personopplysningsloven og GDPR?
19. Er det noen utfordringer når det kommer til å tilpasse seg personopplysningsloven og GDPR?
20. Bruker dere noe form for overvåking av ansatte eller trafikk?
21. Brukere dere noen teknologier som hjelper med sikkerheten som for eksempel kunstig intelligens?
22. Er det noen etiske retningslinjer som denne teknologien må følge?

Appendix B - Information writing about the project

Vil du delta i forskningsprosjektet
”Ethical frameworks in organizations for cybersecurity”?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å se på hvordan etiske rammeverk er i organisasjoner for cybersikkerhet. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg

Introduksjon

Vi er en gruppe på to studenter ved navn Daniel Mikkelsen og Robert Zakariassen, vi studerer Cybersikkerhet med spesialisering innen ledelse. Prosjektet handler om å se på etiske rammeverk som brukes i organisasjoner for cybersikkerhet. Ideen bak prosjektet er å se hva slags rammeverk brukes av ulike organisasjoner for å sikre systemene, lage retningslinjer for brukere, hvilken prinsipper fra etisk teori brukes og hvordan de rammeverkene funker praktisk i organisasjonen. Prosjektet er veiledet av Dr. Devinder Thapa og Dr. Nadia Saad Noori.

Formål

Forsknings formålet er å se på hva slags etikk som brukes i rammeverk og hvilke teorier innen etikk som brukes når det kommer til cybersikkerhet. Vi vil også se hva som er annerledes fra en organisasjon til en annen når det kommer til hvordan de håndterer det etiske med cybersikkerhet. Forskningsspørsmålene som skal analyseres er:

- What type of ethical frameworks are used in cybersecurity?
- How do ethical frameworks work in practice versus in theory?
- What are the challenges of existing cybersecurity ethical frameworks?
- How do organizations in Norway apply the ethical frameworks for cybersecurity?

Denne oppgaven er først og fremst en studentoppgave, men kommer til å bygges videre på og gjort om til en masteroppgave.

Hvem er ansvarlig for forskningsprosjektet?

Oppgaven er utformet i samarbeid av våres masterveiledere i prosjektet, Devendra Bahadur Thapa og Nadia Saad Noori fra Universitetet i Agder fakultet for teknologi og realfag.

Hvorfor får du spørsmål om å delta?

Masteroppgaven har behov for 5-15 respondenter med ulik tilknytning og erfaring opp mot forskjellige fagfelt som har relevant tolkning til etiske rammeverk. Det kan være behov for IT-personell, HR, eller eventuelt ledere for et bredt og mangfoldig perspektiv på fagfeltet.

Hva innebærer det for deg å delta?

Som følger av restriksjoner og lover knyttet til Coronaviruset, vil intervjuene bli gjennomført digitalt, via video- og ringetjenesten Zoom.

Hvert intervju er av omlag en times varighet. Intervjuene er semi-strukturelle, som betyr at det er forberedte spørsmål, men må man være beredt på at oppfølgingsspørsmål kan forekomme for ytterligere utredning. Det vil gjøres lydopptak og tas notater sånn at det er mulig for oss å gå over intervjuet senere.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Dataene som blir samlet inn har ingen interesse eller intensjon om å identifisere deltakere i forskningsprosjektet. I intervjuene kommer det til å bli tatt i bruk digitalt lydopptak via screen recording for transkribering. Dataene som blir innhentet vil bli analysert og presentert i masteroppgaven, disse dataene vil da være i en anonymisert fremstilling, hvorav alt innhentet rådata via screen recording og eller via diktafon vil bli slettet. All innsamling og behandling av intervjudata vil være i tråd med retningslinjene til UiA og Norsk senter for forskningsdata (NSD).

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Dataene som blir behandlet i denne studien vil kun være tilgjengelige for prosjektansvarlig, Devendra Bahadur Thapa, Nadia Saad Noori, samt oss studenter og og databehandlingstjenesten Zoom.
- Videre er også iverksatt tiltak for å sikre at ikke uvedkommende får tilgang til data under og etter intervjuene:
    - Møte linken vil ikke deles åpent.
    - Møtet vil være passordbeskyttet

- Det vil benyttet lobby/venterom for å slippe inn riktige personer i møtet.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 10 juni 2022. All rådata vil bli destruert underveis i prosjektet, videre skal annen data fremstilt i prosjektet anonymiseres innen prosjektslutt.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke. På oppdrag fra Universitet i Agder har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Masterstudent, Robert Zakariassen ved Universitet i Agder, kontaktes på epost (roberz17@uia.no), og eller på telefon: +4793861471.
- Masterstudent, Daniel Mikkelsen ved Universitet i Agder, kontaktes på epost (danielmik@uia.no), og eller på telefon: +4748047381 .
- Professor, Devinder Bahadur Thapa ved Universitetet i Agder, kontaktes på epost (devinder.thapa@uia.no), og eller på telefon: +4795256430
- Førsteamanuensis, Nadia Saad Noori ved Universitetet i Agder kontaktes på epost (nadia.saad.noori@uia.no), og eller på telefon: +4793888245

- Vårt personvernombud: Ina Danielsen ved Universitet i Agder, kontaktes på epost (ina.danielsen@uia.no), og eller på telefon: +4738142140.

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Daniel Mikkelsen og Robert Zakariassen,

Masterstudenter

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju innen 30 april.

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Appendix C - Exclusion Table of Literature Review

Citation: Number and Title	Title Exclusion	Abstract Exclusion	Full-text exclusion	Criteria
6: Ethical framework for Artificial Intelligence and Digital technologies	✔	✔	✗	✗: Setting outside the scope
7: Paradoxes of artificial intelligence in consumer markets: Ethical challenges and opportunities	✔	✔	✗	✗: Setting outside the scope(AI)
8: DeTER Framework: A Novel Paradigm for Addressing Cybersecurity Concerns in Mobile Healthcare	✔	✗		✗:Setting outside the scope ✗: Content to technical and specific
9: Cybersecurity in Active and Healthy Aging Era	✔	✗		✗:Setting outside the scope
11: Ethical and Privacy Considerations in Cybersecurity	✔	✗		✗:Setting outside the scope ✗: Uses a framework for evaluating
12:A framework for competence development and assessment in hybrid cybersecurity exercises	✔	✗		✗:Setting outside the scope
13: A systemic framework for addressing cybersecurity in construction	✔	✔	✗	✗:Setting outside the scope ✗: Does not focus on the ethical aspect
14: Smart Information Systems in Cybersecurity: An Ethical Analysis	✔	✗		✗:Setting outside the scope (Telecommunication)
17: The Ethics of AI Ethics: An Evaluation of Guidelines	✔	✗		✗: Setting outside the scope(AI guidelines)
18: Ethics of Cybersecurity and Biomedical	✔	✔	✗	✗: Focuses on a

Ethics – Providing Ethical Guidelines for the SHAPES Project				project called Shapes and uses mostly the same ethical literature.
19:Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security	✔	✔	✗	✗: Setting outside the scope
20:Compliance, Ethical and Professional Issues in Cybersecurity	✔	✔	✗	✗: This article is not peer-reviewed
21: Where computer security meets national security	✗			✗: Setting outside the scope
24: Ethical Aspects in Cyber Security	✔	✔	✗	✗: Content was short and some was outside of the scope
25: A Framework for Ethical Cyber-Defence for Companies	✔	✗		✗: Setting outside the scope
27: Ethical and Privacy Considerations in Cybersecurity	✔	✔	✗	✗: Content was short and it was outside of the scope
31: Creating a Culture of Enterprise Cybersecurity	✔	✗		✗: Content was short and it was outside of the scope
32: Ethics of AI and Cybersecurity When Sovereignty is at Stake	✔	✔	✗	✗: Setting outside the scope
33: From defense to offense: The ethics of private cybersecurity	✔	✗		✗: Setting outside the scope
34:The Ethics of Hacking: Should It Be Taught?	✔	✗		✗: Setting outside the scope
35:Cyber-noir: Cybersecurity and popular culture	✔	✗		✗: Setting outside the scope
36: Cybersecurity in Educational Networks	✗			✗: Setting outside the scope

37: More than the individual: Examining the relationship between culture and Information Security Awareness	✔	✗		✗: Setting outside the scope
39: Cybersecurity Culture, Norms and Values	✔	✗		✗: Setting outside the scope
40: Privacy and Cybersecurity Insights	✔	✗		✗: Setting outside the scope
41: The Ethical Use of Machine Learning in Cybersecurity	✗			✗: Setting outside the scope
42: Socio-technical systems cybersecurity framework	✔	✗		✗: Setting outside the scope
46: An Ethical Framework for Guiding the Development of Affectively-Aware Artificial Intelligence	✔	✗		✗: Setting outside the scope(AI)
47: Cyber Ethics in Education	✔	✔	✗	✗: Locked behind a paywall
49: Assessment of Ethical Performance of Organization Members: A Conceptual Framework	✔	✔	✗	✗: Locked behind a paywall
50: Ethical Principles and Processes Guiding Dialysis Decision-Making	✔	✗		✗: Content was short and it was outside of the scope
51: Ethical standards and principles	✔	✗		✗: Setting outside the scope
52: Putting Principles into Practice: Developing Ethical Leadership in Local Government	✔	✗		✗: Contents publication date to old
54: Cybersecurity Curriculum Design: A Survey	✔	✗		✗: Setting outside the scope
55: Cybersecurity and Cyber Warfare: The Ethical Paradox of 'Universal Diffidence	✔	✗		✗: Setting outside the scope

Table A1: Exclusion of literature

Appendix D - Inclusion Table of Literature Review

Research Question	Citation: Number and Title	Synthesis Type	Rank 1-10 (Relevance)	Justification
1 and 2	1: A principlist framework for cybersecurity ethics	No primary data, used existing literature	10	Discusses different approaches and values used in ethical cybersecurity as well as frameworks used in cybersecurity.
1 and 2	2: Ethical Frameworks for Cybersecurity	No primary data, used existing literature	8	Shows the different types of ethical frameworks used in Cybersecurity
1 and 2	3: Ethics in cybersecurity research and practice	Qualitative (Case Study)	5	This paper shows ethical issues faced by researchers and criticises existing governance in cybersecurity ethics
1 and 2	4: An Introduction to Cybersecurity Ethics	Qualitative (Case Study)	7	The paper discusses what ethical framework can guide cybersecurity practice and what are ethical best practices in cybersecurity.
1 and 2	5: ETHICS AND CYBERSECURITY ARE NOT MUTUALLY EXCLUSIVE	No primary data, used existing literature	5	This article outlines ethical factors related to cybersecurity as recommended by a model called CSEC2017
1 and 2	10: A Case Study-based Cybersecurity Ethics Curriculum	Qualitative (Case Study)	5	This paper discusses use of different ethical frameworks in western philosophical tradition, but also meta-ethical frameworks.
1 and 2	15: ACM Code of Ethics and Professional Conduct	Qualitative (Case Study)	6	It focuses on how to build code of ethics when working with cybersecurity issues.
1	16. Foundations of Information Ethics	Qualitative (Case	6	Outlines cybersecurity practice and two main overarching professional

		Study)		organizations who have established codes of ethics for the engineers who belong to their organization.
1	22: Scoping the ethical principles of cybersecurity fear appeals	Qualitative (Analysis)	6	The paper focuses on the fear appeal that can be used in Cybersecurity. Fear is used so that it is a higher chance for users to follow guidelines and dont ignore rules.
1 and 2	23:Does ACM's Code of Ethics Change Ethical Decision Making in Software Development?	Qualitative (Case Study)	7	ACM has a code of ethics and this paper focuses on how this affects the ethical decision making for developers.
2	26: Emotion and Ethical Decision-Making in Organizations	No primary data, used existing literature	6	This paper looks at how emotion can influence the employees ethical decision making.
1	28: Importance of Morality, Ethical Practices and Cyber Laws as Prelude to Cybersecurity	No primary data, used existing literature	6	Uses moral theory to define what is right and wrong as well as looking at how ethical practice is important to secure information technology.
2	29: Cybersecurity culture as an element of IT professional training	Qualitative (Case Study)	5	Look at how IT training is an important aspect to understand and work well with ethical aspects in organizations, which will help cybersecurity.
1	30: Ethical Aspects in Cyber Security	No primary data, used existing literature	4	Look at how including ethics in the cybersecurity curriculum increases the capabilities of students.
1 and 2	38: The Introduction of Ethics into Cybersecurity Curricula	No primary data, used existing literature	6	This article focuses on the importance of teaching professional ethics to future cybersecurity specialists.
1 and 2	43: Fostering the Culture of	Qualitati	6	This case study focuses on

	Cyber Security	ve (Case Study)		fostering the culture of Cyber Security and takes in awareness, education, and live training.
1 and 2	44: Cybersecurity and the Ethics of Care	No primary data, used existing literature	6	Proposes a focus on the ethical aspect of care towards cybersecurity using it as a philosophical framework.
2	45: The Effect of Organizational Culture and Ethical Orientation on Accountants' Ethical Judgments	Qualitati ve (Case Study)	5	Look at the relationship between organizational ethical culture between two big companies.
2	48: The impacts of organizational culture on information security culture: a case study	Qualitati ve (Case Study)	6	Looks into how Information security culture is believed to be influenced by an organization’s corporate culture.
1 and 2	53: Cybersecurity and Ethics	White paper	8	The White Paper focuses on ethical disclosure on cybersecurity developed in scientific literature.
1 and 2	56:Privacy at Work – Ethical Criteria	White paper	5	Focuses on monitoring and privacy issues when it comes to ethics.
2	57: Artificial intelligence and privacy	Report	6	Look at how AI can help with decision making and improve privacy.

Table A2: Inclusion of literature

Appendix E - Data Set for Key Concepts and Values

Morales	2
Pride	1
Humanity	3
Establish Attitudes	2
Innovation	1
Sustainability	1
Diversity	1
Openness	5
Trust	9
Professionalism	2
Respect	3
Rules/Laws	5
Privacy	4
Leaste privilege	3
Rights	2
Traffic light protocol	1
Principles	4
Integrity	2
Honesty	1
Availability	1
HMS-security	1
Transparency	2
Responsibility	1
Independent	1
Future-oriented	1
Curious	1
Anti fraud	1
Safeguard life, property and environment	1
Policies	2
Predictable	1
Competent	1
Deliver quality	1
Strict access policy	1
Freedom	1
Autonomy	1

Figure 9: Key concepts and values data set