Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Joachim Ulven

High level information security risk in higher education

Master's thesis in Information Security
Supervisor: Einar Snekkenes & Gaute Wangen
July 2020

NTNU
Norwegian University of Science and Technology

Joachim Ulven

High level information security risk in higher education

Master's thesis in Information Security
Supervisor: Einar Snekkenes & Gaute Wangen
July 2020

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Preface

This master thesis in Information Security at NTNU carried out during the spring semester of 2020. I was approached by the Digital Security Section at NTNU and offered collaboration on an extensive risk assessment of NTNU, where I had the opportunity to write a master thesis along with the assessment. The idea for the thesis was provided by Gaute Wangen, who is my external supervisor. This collaboration would enrich me with hands on experience on risk assessment and management. I immediately accepted the offer. The COVID-19 virus did add substantial challenges to the risk assessment work and caused cancellation and delays for the data collection. However, postponing of the submission date for the master thesis was approved.

The paper is written for those who are interested in information security risk regarding higher education. It is constructed to be an informative document. The reader can either be familiar with information security risk or possess minimal knowledge of the subject.

20th July 2020
Gjøvik, Norway

Acknowledgement

I want to thank the following persons for their help during this master thesis.

First of all, I am very grateful to Prof. Einar Snekknes and Prof. Gaute Wangen, who has supervised on the project since January 2020 and provided helpful and valuable feedback and reading material. Those motivated and encouraged me to overcome the challenges.
I will also give at special thanks to the risk assessment team and Digital Security Section at NTNU for this interesting and educational journey this master thesis has provided.

Thank you, Randi Utstrand, for assisting in document recommendation and interview sampling.

Thank you, Vebjørn Slyngstadli, for insights on the subject matter and supplement of documents relevant to the master thesis.

I am also grateful to all participants in both the survey and the interview who generously gave their time answered my many questions. Their contribution was highly valued.

–Joachim B. Ulven

Abstract

Identifying assets, threats and vulnerabilities is essential when assessing therisk in an organisation. Several of the most renowned information security risk assessment frameworks like ISO/IEC 27005, NIST SP 800-39 and OCTAVE has this assessment in their framework. The purpose of this master thesis is to evaluate what information security risk currently threatening higher educational institutions and assess the information security risk perception of the managerial level at the Norwegian University of Science and Technology (NTNU).

This master thesis utilized qualitative and quantitative research methods like literature study, survey and interviews to identify valuable information assets, threats and vulnerabilities that are prominent in higher educational institutions. The literature study conducted 82 reviewers of different literature sources including academic papers, articles, websites and white papers. The survey had 107 participants which included deans, institution leaders and other managerial support personnel at faculty level at NTNU. The interview had 13 participants from the top administrative management who manage the core tasks at NTNU. This project was done in collaboration with personnel from the Digital Security Section at NTNU, which conducted an extensive risk assessment of NTNU, in the spring of 2020. Some of the result presented in this thesis will also be featured in their final risk assessment.

The findings from this project show that the overall information security risk identified in the literature study and at the managerial level at NTNU shares a high degree of likeness and similarities. Threat based on “Organized criminals” and “Human error” were among the topmost prominent threats in higher education. These threats can exploit prominent vulnerabilities in higher education which includes: Lack of information security knowledge, awareness, attitude, culture and insufficient resources. Valuable information assets in higher education relating to “Graduation measures”, “Stakeholder satisfaction”, “Employee & HR” and “Enrollment” were identified as the most valuable and abuse of these would be critical to higher education institutions. The combination of these three factors illustrate an overview of the information security risk relevant for higher educational institutions.

Sammendrag

Identifisere verdier, trusler og sårbarheter er avgjørende når du vurderer risikoer i organisasjoner. Flere av de mest kjente informasjonssikkerhetsrisiko rammeverkene som ISO/IEC 27005, NIST SP 800-39 og OCTAVE bruker dette i sine rammeverk. Hensikten med denne masteroppgaven er å evaluere hvilke informasjonssikkerhetsrisikoer som truer høyere utdanningsinstitusjoner og vurdere oppfatningen av informasjonssikkerhetsrisiko på ledernivå ved Norges teknisk-naturvitenskapelige universitet (NTNU).

Denne masteroppgaven benyttet seg av kvalitative og kvantitative forskningsmetoder som litteraturstudie, spørreundersøkelse og intervjuer for å identifisere verdifulle informasjonsverdier, trusler og sårbarheter som er fremtredende i høyere utdanningsinstitusjoner. Litteraturstudien gjennomførte 82 gjennomlesninger av forskjellige litteraturkilder fra akademiske artikler, nyhetsartikler, nettsider og rapporter. Spørreundersøkelsen hadde 107 deltakere som inkluderte dekaner, institusjonsledere og annet leder støttepersonell på fakultetsnivå ved NTNU. Intervjuet hadde 13 deltakere fra den øvre administrative ledelses nivået som administrerer kjerneoppgavene ved NTNU. Dette prosjektet ble gjort i samarbeid med personell fra seksjonen of Digital Sikkerhet ved NTNU, som gjennomførte en omfattende risiko- og sårbarhets analyse av NTNU, våren 2020. Noe av resultatet som blir presentert i dette prosjektet vil også bli inkludert in deres endelige sluttrapport.

Resultatene fra dette prosjektet viser at den generelle informasjonssikkerhetsrisikoen som er identifisert i litteraturstudiet og på ledernivå ved NTNU, deler en høy grad av likhet. Trusler basert på “Organiserte kriminelle ” og “ Menneskelig feil ” var blant de mest fremtredende truslene i høyere utdanning. Disse truslene kan utnytte aktuelle sårbarheter i høyere utdanning som inkluderer: Mangel på informasjonssikkerhets kunnskap, bevissthet, holdning, kultur og manglende ressurser. Verdifulle informasjonsverdier i høyere utdanning relatert til “Graduation measures”, “Stakeholder satisfaction”, “Employee & HR” og “Enrollment” ble identifisert som de mest verdifulle og misbruk av disse ville være kritiske for høyere utdanningsinstitusjoner. Kombinasjonen av disse tre faktorene illustrerer en oversikt over informasjonssikkerhetsrisikoen som er relevant for høyere utdanningsinstitusjoner.

Contents

Figures

Tables

Abbreviations

CLR	=	Comprehensive Literature Review
KPI	=	Key Performance Indicators
NTNU	=	Norwegian University of Science and Technology
ROS	=	Risiko- og Sårbarhets analyse (Risk assessment)
SOC	=	Security Operation Center
STO	=	Strategic Tactical Operational

Chapter 1

Introduction

Universities and academic institutions rank among the most attractive targets for cyber-attacks, according several news outlets. The Wall Street Journal[1] and The New York Times [2] all reported in 2019 a rising trend in cyber-attacks targeting academic institutions in the United States. Universities and academic institutions are managing large amounts of valuable research and sensitive personal data which makes academic institutions a lucrative target for cyber criminals[3]. Everything from low level individuals who seek financial gain, to heavily founded state sponsored actors who intend to steal confidential research data might be in the loop. The constant influx of new students, external guest and employees does also add challenges to the information security work at universities.

According to the Head of Programme, Cyber and National Security at TechUK, Talal Rajab: "The higher education sector in the UK has long been a target for cyber criminals, tempted by the world-leading academic research that universities produce in sensitive areas such as medical and defence research. As the cyber threat evolves, and attacks become more sophisticated, it is imperative that universities invest heavily in their cyber defences and protect the professional and personal data of the 2.5 million students and staff learning and working in universities across the UK."[4]

This threat is also present at Norwegian universities. The Norwegian Police Security Service (PST) documented in its' 2020 annual National Threat Assessment[1], that Norwegian universities be a attractive target for abuse. It addressed that many research communities are working closely together with actors in business environments. This might appeal to foreign intelligence services who seeks to steal important information and technology, to achieving their goals of tech-

[1]https://www.wsj.com/articles/schools-brace-for-cyberattacks-11566379800 (Accessed: 17.03.20)

[2]https://www.nytimes.com/2019/07/28/us/hacker-school-cybersecurity.html (Accessed: 17.03.20)

[3]https://www.fireeye.com/blog/executive-perspective/2019/04/higher-education-faces-a-unique-cyber-threat-landscape.html (Accessed: 08.02.20)

[4]https://www.computerweekly.com/news/252464169/Hackers-targeting-UK-universities-a-threat-to-national-security (Accessed:15.06.20)

nology development. The report address that Norwegian businesses and Norwegian researchers manages knowledge, expertise, personnel and equipment that other foreign states might utilize to development weapons programs. This will make Norwegian research environments regarding nuclear physics, underwater and deep-water technology, control systems, autonomous vessels, artificial intelligence, engineering design, nanotechnology, satellite and missile technology, as well as technology suitable for arctic conditions targeted for infiltration. Some of these disciplines are also relevant for developing of weapons of mass destruction.

However, even though academic institutions are facing substantial information security risk at their institutions, the initiative of implementing information security measures might not exist. The chief information security officer at Purdue University, David J. Shaw stated in an article in The New York Times that: "A university environment is very different from a corporation or a government agency, because of the kind of openness and free flow of information you're trying to promote," said David J. Shaw. "The researchers want to collaborate with others, inside and outside the university, and to share their discoveries." [5] Academic freedom and open source are strong norms in the academic environment. This culture can make the of information security work at higher educational institutions challenging.

1.1 Topic covered by the project

Topics covered in this project will evaluate the assets, threats and vulnerabilities in higher educational institutions.
Information security risk is often associated with the relationship between values, threats and vulnerabilities. If one of these factors does not exist, there wouldn't be any risk present in an organisation. However, employees at academic institutions are managing more sensitive and critical information than ever before and the number of threats and vulnerabilities has only increased due to the connectivity of the internet.

Valuable information in an organisation are often related to the information assets that are directly or indirectly contributing with the objectives or core tasks in an organisation. These information assets can be linked to strategic objectives and therefore be identified by examining the Key Performance Indicators(KPI) at an organisation. Actors who pose harm or threat to these information assets should be labeled as the most dangerous threats, depending on their level of occurrence. Vulnerabilities in an organisation might also contribute to the exposure and loss of valuable information assets. These vulnerabilities can also be attributed to social elements like: Lack of risk awareness, inadequate security culture or lack of knowledge and competence.

The first security strategy addresses in the information security policy at the

[5] https://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all&_r=0 (Accessed 03.05.20)

Norwegian University of Science and Technology (NTNU) states that: "Managers need to have a clear understanding of risk and an overview of the information assets that the unit handles, so that they can make informed choices and set priorities for the introduction of security measures."[6] It is therefore crucial to identify these critical elements that are present in an organisation either by conducting literature- and quantitative studies. This can be extremely applicable and beneficial to managers in an organisation who manage information related to core tasks and objectives in the organisation. By studying and assess the risk associated with information security one can implement proactive measures and mitigate potential cyber incidents that can have serious consequences to key academic processes.

1.2 Keywords

Information Security, Information Security Risk, Risk Perception, Higher Education, Threats, Vulnerability.

1.3 Problem description

The book from Whitman and Mattord[2] describes the following: "To protect your organization's information, you must: (1) know yourself; that is, be familiar with the information assets to be protected, their inherent flaws and vulnerabilities, and the systems, mechanisms, and methods used to store, transport, process, and protect them; and (2) know threats you face."[p.11] Identifying assets, threats and vulnerabilities in an organisation can be challenging. Information assets are constantly created, processed and stored. The threat environment in cyber space are constantly changing, where new methods and tools makes it is hard to identify, evaluate and map threat actors and attacks that are likely to inflict harm to an organisation. Changes in organisational structure can unveil new vulnerabilities that hasn't been accounted before, which might need immediate assessment. It can therefore be challenging to conduct a holistic risk assessment that accurately addresses the values, the threats and the vulnerabilities present in an organisation. Information relating to information security risk for higher education institutions are scarce, inaccurate or unavailable to the public. This might be due to the possibility of potential bad press or damage of educational reputation. A study which utilizes qualitative and quantitative methods to assessing the perception of information security risk by identifying valuable information assets, threats and vulnerabilities in higher educational institutions can therefore be desirable.

However, assessing information security risk perception at managerial level in higher educational institutions can also be beneficial. The "*How safe is your data? Cyber-security in higher education*" from John Chapman[3] addresses that it is a mistake that cyber risk is being manage solely by the information technology

[6]https://innsida.ntnu.no/wiki/-/wiki/English/Policy+for+information+security(Last visited: 17.06.20)

function in an organisation. Information security risk affects all operations and needs to be included and addressed by the wider governance and management process across the organisation. He continuous and states that, cyber risk cannot be delegated away from the governing body and the executive management. They need to be held accountable for ensuring that informed and appropriate decisions are being made which meets or exceeds the expectations of any organisation's stakeholder and the law.

1.4 Justification, motivation and benefits

It is critical to protect assets at higher educational institutions. Universities and higher educational institutions are constantly conduction teaching, research and development which is highly beneficial for society. Companies in private and public sector are also collaborating and investing huge amounts of resources in research and development at higher educational institutions. It is therefore pivotal to assess and mitigate all risk that might be of threat to these assets related to the core processes at higher educational institutions. Findings in this project might assist in future risk assessment at higher educational institutions to protect critical information assets. Finding from this project may also increase information security awareness level and make personnel at institutions more aware of the information security risks which is present at a university.

1.5 Research questions

1. Which information security risks threatens higher education according to literature?
2. Which information security risks threatens higher education according to the managerial level at NTNU?
3. How do the information security risk identified in literature overlap with risk identified at the managerial level in NTNU?

1.6 Planned contribution

This master project has been a collaboration with a small team from the Digital Security Section at NTNU, which as of January 2020 where tasked of conducting an executive risk assessment (Risiko- og Sårbarhets analyse) of NTNU. The purpose of the risk assessment was to identifying information assets relating to core task and other potential threats relating to the managerial level at NTNU. This included collecting data from deans and leaders with managerial support. This master thesis has contributed to this risk assessment by collecting quantitative and qualitative data which will be featured in the final risk assessment. Some of the findings from the risk assessment will also be presented in this report.

This master thesis will present findings from a literature study where identification of:
(1)Valuable information assets in higher educational institutions based on Key Performance Indicators(KPI).
(2)Threats applicable to higher education, from other studies.
(3)Vulnerabilities documented in literature which is applicable to higher educational institutions.

The project will also conduct a case study where qualitative methods are used to identify which valuable information assets, threats and vulnerabilities are present at NTNU.

Finally, the project will also conduct a survey and interviews to identify the most prominent information assets, threats and vulnerabilities present at the managerial level at NTNU. This will include deans and leaders with managerial support and top administrative personnel managing the core tasks and processes at NTNU. This project will therefore present a rich and valuable set of information that will give an overview of the information security risk present in high education and how the managerial level in higher education perceive the current risk.

1.7 Limitations

The case study in this master thesis will be limited to the Norwegian University of Science and Technology. This includes the three campuses in Norway: Trondheim, Gjøvik and Ålesund. No other higher education institution will be featured in the case study. However, literature from other international higher educational institutions will be featured in the general literature study.

1.8 Thesis structure

This section will present a brief summary of the content presented in this thesis. The list will be presented the chapter and it content.

- Chapter 2 presents a study context to give the reader sufficient knowledge of the coming research topic. Topics includes definitions of general information security risk and managerial levels in an organisation.

- Chapter 3 presents the methodology of this project. The chapter will address considered research methods and the applied research method that were used in the project.

- Chapter 4 presents the literature finding of the information assets, threats and vulnerabilities prominent in general higher education institutions.

- Chapter 5 presents the case study of NTNU, which will address valuable information assets, threats and vulnerabilities at NTNU.

- Chapter 6 presents the results and analysis of the survey and interview done on the managerial level at NTNU.

- Chapter 7 presents the discussion of each research questions and potential future work.

- Chapter 8 presents the conclusion of the master thesis.

Chapter 2

Study context

The purpose of this chapter is to give the reader sufficient knowledge and background to better understand the coming research topic. This chapter will address definitions regarding general information security risk and the managerial levels in an organisation.

2.1 Introduction to information security

The international standard, ISO/IEC 27002:2013[4], defines information security as the preservation of the confidentiality, integrity and availability of information.

Whitman and Mattord[2] define information security as "protection of information and the characteristics that give it value, such as confidentiality, integrity and availability, and includes the technology that houses and transfers that information through a variety of protection mechanisms such as policy, training and awareness programs and technology"[p.5]. However, information security is not exclusively limited to these three characteristics. Whitman and Mattord[2] continuous and address that "present-day needs have rendered these characteristics inadequate on their own to conceptualize InfoSec because they are limited in scope and cannot encompass today's constantly changing IT environment, which calls for a more robust model. The C.I.A triad, therefore, has been expanded into a more comprehensive list of critical characteristics and processes, including privacy, identification, authentication, authorization, and accountability."[p.8]. Solm and Niekerk[5] states in their paper that: "The aim of information security is to ensure business continuity and minimise business damage by limiting the impact of security incidents"[p.98].

2.2 The three factor model for information security risk: Assets, Threat and Vulnerability

Information security risk assessment can be conducted by several frameworks. The most renowned information security risk assessment frameworks are ISO/IEC 27005, NIST SP 800-39 and OCTAVE to name a few. However, they all share the similarity of first, identifying valuable assets in an organisation either through qualitative or quantitative methods. Then identify internal and external threats that might potentially cause harm to these assets. Then finally identify and evaluate vulnerabilities that are present in organisation.

The book from Landoll[6] describes security risk as the "loss potential to an organization's assets that will likely occur if a threat is able to exploit a vulnerability" [p.30]. The book from Whitman and Mattord[2] explains information security risk as the following: "a threat represents a *potential* risk to an information asset, whereas an *attack*, sometimes called a *threat event*, represents an ongoing act against the asset that could result in a loss. Threat agents damage or steal an organization's information or physical assets by using *exploits* to take advantage of a *vulnerability* where controls are not present or no longer effective. Unlike threats, which are always present, attacks exist only when a specific act may cause a loss."[p.11] The definition from Whitman and Mattord can be illustrated in figure 2.1 as the following: A hacker(threat) exploits a zero-day (vulnerability) to get access to an organisations confidential database(assets). This assumption is echoed in every information security incident and are is why information security risk frameworks are focusing on identify all threats, vulnerability and valuable assets that are present in an organisation.

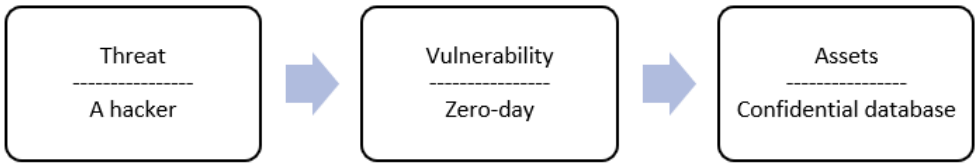


Figure 2.1: Illustration of information security risk by Whitman and Mattord[2].

The book by Landoll[6] continuous "The overall objective of all security risk assessment analysis processes is to determine and convey the security risk to the organization's assets.[...]The security risk determination therefore is dependent upon the identified threats and vulnerabilities measured, and based on the probability of the threat/ vulnerability pair, the value of the asset affected, and the impact that the threat/ vulnerability pair will have on the asset."[p.365] This assumption is illustrated in figure 2.2 in a Venn-diagram of the three-factor perspective of risk(assets, threat, vulnerability), with the likelihood multiplied with the impact in the centre. The likelihood and impact is equal to risk of a threat using a vulnerability to affect an asset:

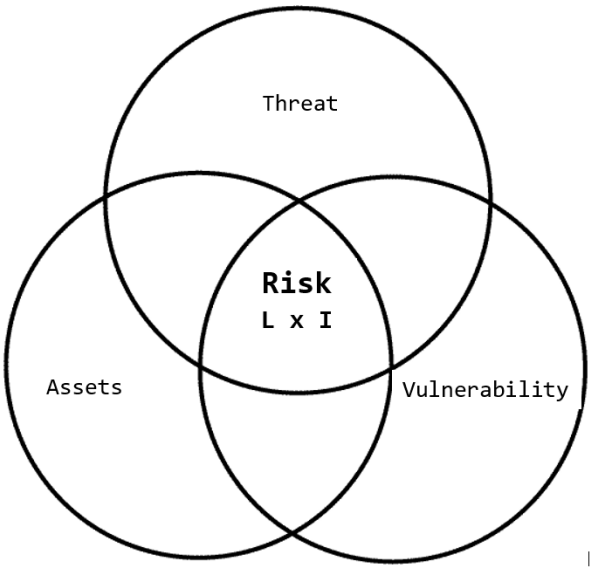


Figure 2.2: A Venn-diagram of the three-factor perspective of risk.
[1]

$$Risk = Assets * Threat * Vulnerability \tag{2.1}$$

2.2.1 Assets

The book by Landoll[6] describe assets as information, resources or other items that is considered to be valuable by an organisation. This includes buildings, equipment, personnel, organization reputation, business documents and other tangible and intangible assets. Whitman and Mattord [2] describe assets as the following: "An organizational resource that is being protected. An asset can be logical, such as a Web site, software information, or data; or an asset can be physical, such as a person, computer system, hardware, or other tangible object."[p.2]. Information assets on the other hand is "any asset that collects, stores, processes, or transmits information, or any collection, set, or database of information that is of value to the organization "[2][p.320]

It is important to identify and enumerate the assets within a given organisation before conducting the risk assessment according to Landoll[6] and ISO/IEC 27005[7]. This will help to scope the security risk assessment and further determined the countermeasures and controls that is needed to be employed.

[1]Source: Adapted from https://innsida.ntnu.no/wiki/-/wiki/Norsk/informasjonssikkerhet+-+risikostyring(Accessed:07.07.2020)

2.2.2 Threat

Whitman and Mattord[2] describes threats as "Any event or circumstance that has the potential to adversely affect operations and assets."[p.11] The book also address that terms like *threat source* and *threat* are commonly used interchangeably. Even though the two terms are technically distinct, the term *threat* might also describe treat source. While a threat agent is "The specific instance or a component of a threat"[2][p.11]. The book from Landoll[6] describes a threat as an event with an undesired impact, while a threat agent is the entity that may cause a threat to happen. Threats are always present.

2.2.3 Vulnerability

Whitman and Mattord[2] describes vulnerability as "A potential weakness in an asset or its defensive control system(s)"[p.11]. While the book from Landoll[6] describes a vulnerability as "a flaw or oversight in an existing control that may possibly allow a threat agent to exploit it to gain unauthorized access to organizational assets."[p.29]. The book from Landoll[6], continuous to state that vulnerabilities are a very important element of a security risk assessment. Vulnerabilities are instrumental in determining current risk, and risk that remaining after control measures have been implemented. Without vulnerabilities, there would not be any risk. However, there is no such thing as a "vulnerability free system". It is therefore important to identify and assess the vulnerabilities in the existing systems and those vulnerabilities that still might be present after safeguard recommendations have been implemented.

2.3 Introduction organizational management levels

Figure 2.3: Organisational management levels, illustrated by the STO framework [2]

The Strategic Tactical Operational(STO) framework is a holistic representation of the organisational management level, in most organisation. It was first used as a illustration for supply chain management (eg. [10] [11]), however it has been adapted to illustrate where managerial tasks are conducted and who's responsible for them (eg.[8][12][13] [14]). Everything is connected from the top down.

2.3.1 Strategy level

The strategic level is where senior/top level management plan and make decisions that sets or impact the long-term direction of the entire organization. These decisions are visionary and future oriented. External data like the economy, markets, stakeholders, competitors, and business trends are essential to their analysis, planning, and decisions.[8][p.272] One of the most critical contributions from the top level is strategies and strategy planning. The strategy plan is constructed by the organisational mission and objectives, which assist in the construction of the strategy formulation. The goal of a strategy planning is to guide the organizational effort and allocate necessary resources towards established and defined goals, while adapt to the environment [12] [p.71] and [2][p.129]. An organization's strategy usually describes how it intends to create value for its shareholders, customers and citizens. It is senior managers task to construct and maintain the most suitable strategy for the organisation. They must assure that the rest of the organisation are complaint and follow the strategies created for them. They are managing the core task in the organisation.

The paper from Darmalaksana et la. (2018)[15] address that the strategy in higher educational institutions consist of three core processes. These include:

[2]Source: Adapted from[8][p.273] and [9][p.20]

- Education and Teaching
- Research
- Community Service

The paper also addresses that universities needs supporting activities to effectively perform the three processes.

- Academic Administration
- Finance and accounting
- Human resources
- Campus infrastructure
- Relationship with industry
- Student Service

Employees at the strategic level occupying these core processes by assisting in allocating their resources in order to support the vision, mission and goals that have been planned to accommodate the strategy in higher educational institutions.

2.3.2 Tactical level

The tactical level is largely concerned with medium-term planning. Managers in this level are monitoring the performance of the organisation, control budgets, allocate resources and set policies. They assess how to beat out competitors and generate revenues and profits to accomplish the organization mission, strategy and objective. External and internal data are therefore important for decision making at this level, which often has a one- to three-year time horizon. [8] [p.272] and [9] [p.20].

The tactical level can refer to the academic faculties at higher educational institution. Faculties are independent departments of learning in academic institutions[3], where deans and management support contribute to the academic institution core task in their faculty[4].

2.3.3 Operational level

The operational level usually consists of workers and sub-managers who deal with short-term planning and the day-to-day control of organisation activities. The decisions taken at this level are directed at the organisation's effort to meeting the medium-term goals by abiding the budgets, policies and procedures set by the tactical level. Operational decisions tend to be highly structured and have little impact on the organisation as a whole. Examples of decisions taken at the operational level might be setting a daily or weekly production schedule. [9] [p.20]. Academic departments can refer to as the operational level in higher educational

[3]https://www.dictionary.com/browse/faculty?s=t (Last visited:18.06.20)

[4]https://uwaterloo.ca/secretariat/policies-procedures-guidelines/policy-45 (Last visited:18.06.20)

institution. They are subgroups in faculties and are conducting education and research on specific topics.

2.4 Managements levels relation to information security

Information and data assets are valuable to all organisations. Executives and managers are becoming more aware of the potential security breaches that may occur. The importance of preserve the confidentiality, integrity and availability of their information assets has become more necessary. Board of directors, executives and managers should therefore be more involved in information security to undertake responsibility regarding information security issues in the organisation. This is important, because they contribute to strategic planning which needs to be informed of the effectiveness of general information security strategies and the overall performance and efforts in the organisation[16, 17].

The paper from McFadzean et al.[17] address three reasons why greater managerial and board of director involvement in information security are beneficial. The first reason is because: "directors are responsible, often legally, for their organisation's risk management system and internal controls."[p.624]. It addresses that organisations must be compliant with legislation and regulations that addresses information security and privacy. The General Data Protection Regulation (GDPR) is a legislation in EU on data protection and privacy. The law was implemented on the 25 of May 2018 and incorporate all organisations and companies that manage and store personal data. Organisations can be fined if they violate these regulations[5]. The second reason described in [17] is that leaders and managers may also gain a competitive advantage through good IT governance, by taking greater interest in information security matters. Aspect like, better communication may contribute to competitive edge. The third reason for why information security matters, is that "it could be a factor that affects the success of an organisation's information security initiative"[17][p.624]. Information security policies reflect business objective and implement approaches that support commitment from management. This will contribute to future benefits.

Information security conducted at top management level, will also give executives ability "to evaluate the organisation using a holistic approach as well as having the power to ensure that new systems and procedures are implemented in a timely manner."[17][p.622]. This is also applicable to higher educational institutions. The information security policy at NTNU states that leaders(Deans and university administration managers) are: "responsible for compliance with the information security requirements, including the processing of personal data" at their unit and "responsible for ensuring that employees at the unit have adequate training in information security and can fulfil the duty to assess the risk of new projects and processing, as well as for reporting nonconformities in the event of

[5]https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en(Last visited:18.6.20)

information security breaches"[6] By having the management level engaged in information security work, one will contribute to a holistic and profound risk awareness in an organisation.

[6]https://innsida.ntnu.no/wiki/-/wiki/English/Policy+for+information+security (Last visited:18.06.20)

Chapter 3

Methodology

This chapter will address the methods used in this master thesis to conduct this research-based project. Topics include considered research methods and the applied research method.

3.1 Considering research methods

"Research is a logical and systematic search for new and useful information on a particular topic." [18][p.2] it is therefore imperative to evaluate the most sufficient research methods to collect adequate data for this master thesis. There are mainly two approaches to gather research data: Qualitative research and quantitative research.

3.1.1 Quantitative research

Quantitative research is based on the measurement of quantity or amount. Quantitative research possesses unique characteristics that differentiate it from qualitative research. The following list from Rajasekar et al.[18] address characteristics of quantitative research:

- It is numerical
- Non-descriptive
- Applies statistics or mathematics and uses numbers.
- It is an iterative process whereby evidence is evaluated
- Results are often presented in tables and graphs
- It is conclusive
- It investigates the *what*, *where* and *when* of decision making

A common method for conducting quantitative research is through surveys. Survey enables researches to obtain data on several pre-determined subjects through questions to collect data which cannot be obtained through systematic observations. The survey form needs to be formulated in a cohesive manner while being apprehensible to participants. Communication and formulation of the questions

featured in survey should therefore be comprehensible. The benefits of a survey are that it can reach and collect data from a wide audience in a cost-effective manner. Participants may also be able to can control their answer, which makes their answer more valid. Some disadvantages with survey are the possibility of a low responses rate. Other disadvantages could be the that participant don't understand the question or give inaccurate answers. It is therefore not recommended to feature objectives that may change over time in the survey. Asking participants questions related to illegal acts, religious beliefs and other sensitive information is also not desirable [19].

The downside with surveys is the lack of in-depth information gathered from the subjects, in which qualitative research methods do. The accuracy and the usefulness of the data obtained in a survey depends on several factors. The paper from Gürbüz[19][p.142] addresses factors that might contribute to the accuracy and usefulness of the data obtained in a survey. The following list address these factors:

- The researcher has conceptualized all the variables to be measured in an understandable form
- The pollsters have no effect on the survey
- The respondents give correct answers to all questions
- The respondents perceive all the questions correctly
- The respondents do not know the hypotheses, purpose and problems of the research
- The interview status and the interviewers do not affect the respondents

3.1.2 Qualitative research

Qualitative research relates to qualitative phenomenon's involving quality. Qualitative research possesses unique characteristics that differentiate it from quantitative research. The following list is from Rajasekar et al.[18] address characteristics of qualitative research:

- It is non-numerical
- Descriptive
- Applies reasoning and uses words
- Its aim is to get the meaning, feeling and describe the situation
- Qualitative data cannot be graphed
- It is exploratory
- It investigates the *why* and *how* of decision making

Qualitative research methods are used when a problem or issue needs to be explored deeper, where quantitative measures and the statistical analyses simply do not fit the problem. This can be studying a group or population or to identify variables that cannot be easily measured. We can use qualitative research if we need a complex, detailed understanding of a topic or an issue. Some of these details can only be acquired by (eg.) talking directly with individuals, in their homes

or at their work place, and allowing them to tell their stories accurately[20].

Qualitative research usually conducts and utilizes multiple forms of data collection methods. A common method for conducting qualitative research is through case studies. Case studies are strongly connected to qualitative research methods. Defining features of a case study is that it uses multiple data collection methods from different perspectives and accounts within a structured context, to create an in-depth understanding that is holistic, comprehensive and contextualised of the subject matter[20, 21]. These structured context can range from processes or organisational context like schools and institutions[21]. “Case study is defined not so much by the methods that you are using to do the study, but the edges you put around the case”[20][p.125]. Data collection methods used in case studies may vary. However, the most used forms include interviews, observations, documents and audio-visual materials [20] [p.127]

Benefits of qualitative research is the flexibility of conducting and collecting data. It gives the research the freedom of examining the research topic according to preferences. However, qualitative research can be tedious endeavour when trying to achieve satisfying results. The amount of data collected, can make the analysis challenging and tedious if the researcher lack experiences of conducting qualitative research.

3.2 Applied research methods

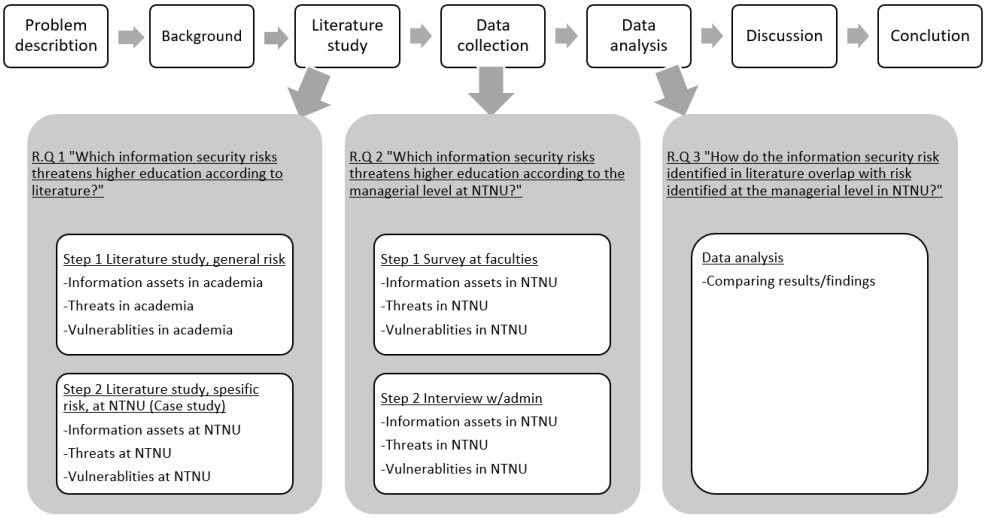


Figure 3.1: Methodology and process overview of this Master Thesis

We will in this project use literature study and a case study to acquire sufficient knowledge about information assets, threats and vulnerabilities applicable to higher educational institutions. We will also conduct a survey and interviews to assess valuable information assets, threats and vulnerabilities that are prominent to managerial level at NTNU. The figure 3.1 presents the applied research method that will be used in this project.

3.2.1 Literature study

A literature study is a review of as much literature as possible around a particular research topic. We will first conduct the literature study on general valuable information assets based on Key Performance Indicators that are present in higher education institutions. Identify sources of literature that depict statistics of threats to higher educational institutions, and identify which vulnerabilities are currently present at higher educational institutions.

The literature study will follow the seven-step Comprehensive Literature Review(CLR) model from the book from Onwuegbuzie and Frels[22]. It is a step-by-step model that gives the researcher the freedom to reiterate steps, but still keeping the process structured. This model will be used when acquire literature about valuable information assets, threats and vulnerabilities for general higher education and for the case study of NTNU.
The process is grouped into three main phases: *Exploration phase*, *Interpretation phase* and *Communication phase*. The following figure illustrates the seven-step model:

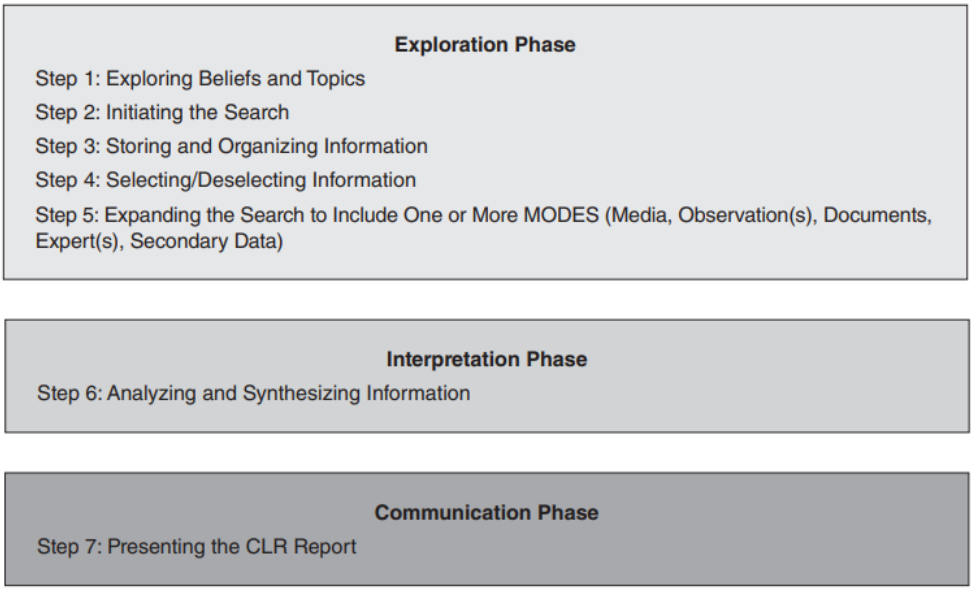


Figure 3.2: The three phases of the Comprehensive Literature Review, from the book [22][p.56]

The three phase of the seven-step model will now be briefly introduced and described, together with details regarding the execution.

Exploration phase

We will start the literature study by following the steps depicted in the *Exploration phase*. We will start acquiring knowledge from personnel working at the Digital Security Section at NTNU, to achieve first-hand knowledge of threats that may exploit vulnerabilities to abuse valuable information assets. It was essential to identifying valuable information assets that were relevant to strategic objectives at higher education and to NTNU. The conversation and dialogues from these individuals will give us a holistic overview of the topics, and access to further literature that were highly relevant. After receiving knowledge and insight on the topic, we'll shift our attention to news articles and published report.

This will give us further knowledge and insight and deepened our knowledge. All initial findings will be sorted and organized in folders, which shall be uploaded and synchronized with the cloud service application MEGAsync. This is a highly convenient solution due to the level security and flexibility. All types of literature relevant to the topic will be selected. This included webpages from academic institutions, academic papers, books and white papers. The academic papers will be acquired from online academic databases such as Researchgate, Scopus, ScienceDirect and Google Scholar. Books will be acquired from both online academic databases and Google searches. White papers will be acquired from Google search.

Interpretation phase

The second phase of the literature review depict the interpretation of the information that will be extracted during the *Exploration phase*. The literature search might accumulate a large number of results. A big part of the work after will be to investigate potential information and literature. All types of literature will be considered when we acquired data on the topic. We wanted to achieve a holistic understanding of the topic by widening the spectre. Literature and information from websites related to academic institutions, academic papers, books and white papers will be included. Results from websites and academic papers will be weighted more, than books and white papers. This is because websites on academic institutions and academic papers goes through long processes of certification and review before publication. They are therefore less bias. Books are generally less review by a board of expert before publishing and are primarily created for financial gain. White papers are usually created by companies seeking financial gain. They can therefore be tuned to accentuate in the company's favour. Though, they can contain legitimate data, they might be presented to promote or advertise a service.

Communication phase

The final phase of the of the comprehensive literature review is the communication phase. It illustrates how results from the previous steps shall be presented. Literature findings relating to general "Valuable information assets", "Threats events" "Threat agents" and "Vulnerabilities", in higher education will be presented in chapter 4. Findings related specifically to NTNU will be presented in chapter 5.

3.2.2 Case study

This project will include a case study on the Norwegian University of Science and Technology, by using qualitative methods to achieve a holistic understanding of the values, threats and vulnerabilities related to information security risk present at NTNU. These qualitative methods include literature study of web pages, academic papers and former bachelor- and master thesis relating to the subject. We will also conduct dialogues with personnel from the Digital Security Section at NTNU to identify valuable information assets, threats and vulnerabilities present at NTNU. This will give us an in-depth understanding of the current information security risk at NTNU.

3.2.3 Data collection method: Survey

The purpose of this survey is to collect data from the managerial level regarding information assets, threats and vulnerabilities at NTNU. Participants in the survey will only include deans, institution leaders and other managerial support personnel from each of the 9 faculties at NTNU. This survey will be done in collaboration with the Digital Security Section at NTNU. They were tasked with conducting an

extensive risk assessment to map information assets at each faculties.

Their assignment was to map "primary" information assets. Primary information assets included valuable information assets that is created, processed and manage in the organisation which assist the core tasks and strategies in an organisation. These primary information assets can be unstructured information (eg notes, documents, publication, video- and audio recordings etc), structured information (eg student data in administrative systems, data in research databases, results from survey's etc) or information in raw form (eg research data that hasn't been analysed or possessed information). "Secondary" information assets, on the other hand, include tools, computer resources, application, systems, databases, network and other assets that transmits information were not part of the scope.
Our collaboration enabled us to add additional questions in the survey. This made it possible to collect data and identify information assets, threats and vulnerabilities at managerial level at NTNU. The survey managed to collected data for both this project and their research.
The development of the survey shared the same design as depicted in OECD[23][p.31-43]. It consisted of a 6 steps-by-step guide on how to create a perception survey. It is important that these steps are followed chronologically.

Step 1. Define survey objectives, use of results and target population
This step describes that the initial phase of developing a survey. It addresses the objective and goal that shall be achieved in this survey. One should also address the target population in this step. The Digital Security Section had received their assignment, to map valuable information assets that assist NTNU in core tasks and strategies. We added additional questions relating to threats and vulnerabilities at NTNU. This survey targeted only deans, institutions leaders and administrative personnel at faculties.

Step 2. Draft survey questions
This step describes the construction of the questions that shall be included in the survey. After identifying the key issues, we will begin drafting questions and the introduction letter. We will make great effort to create question that is easy enough for all respondent, regardless of previous knowledge, while simultaneously cover our objective. The sequence of the questions will be taken into consideration. The construction of these questions is based on findings from the literature study, along with expert knowledge input from the members from the Digital Security Section. The survey will consist of fourteen questions, where seven of the questions will be free-text questions, one "Yes/No/Do not know" question and six ranking/Likert-scale questions. The ranking/Likert-scale questions will be designed with five or six alternatives. They will have four ranking alternatives and one for "Do not know" and "Not relevant". The survey will be in Norwegian. We will strive to make the survey as sort as possible for making the survey more appealing. The number of questions will be determined by the research issue. We aim for a 10-

minute survey.

Step 3. Pilot and re-adjust questionnaire
After constructing a draft of the survey, we will conduct a pilot test to learn how respondents will interpret the questions. It is essential to adjust and redesign poorly phrased questions, to improve the quality of the questions, which will further improve the quality of the results. We will select three individuals we know we'll receive good feedback from. This will be done one week before the initial launch of the survey.

Step 4. Select respondents and the data collection method
This stage confirms the number of respondents and the way they are selected. We will request a list of managerial personnel at each faculty and make clear that this list will be used to forward our survey to each participant. We will receive a list from each of the 9 faculties at NTNU. The following table illustrates the overall planned number of participants from each faculty:

Faculties at NTNU	Number of survey recipients
Faculty of Architecture and Design (AD)	12
Faculty of Humanities (HF)	19
Faculty of Information Technology and Electrical Engineering (IE)	17
Faculty of Engineering (IV)	13
Faculty of Medicine and Health Sciences (MH)	23
Faculty of Natural Sciences (NV)	35
NTNU University Museum (VM)	12
Faculty of Social and Educational Sciences (SU)	22
Faculty of Economics and Management (OK)	16
Total	169

Table 3.1: Total number of participants receiving the survey from each faculty

The survey will be sent by e-mail, which requires minimal resources and reaches a widely dispersed sample group. This will give the participants the flexibility to answer the questions when they had time.

Step 5. Running the survey
The survey will be presented on Nettskjema.no, due to their level of security and level of user friendliness. The survey will be launched on the morning of 16.04.20 and be online until the evening of 08.05.20. Three follow-up emails will be sent to non-respondents during the period.

Step 6. Analysing the results
The data from the survey will be analysed by the IBM SPSS Statistics 26 software. We will use this software to conduct a descriptive statistical analysis of our findings. This will include analysing the frequency, median, variance and range of our results. Methods like standard deviation and mean will not be conducted, because the questions analysed in this study feature a Likert scale design. It is synonymous

with Likert-scale and ordinal data to not conduct standard deviation and mean, because it will be inaccurate to measure the distance between two alternatives in a Likert-scale. We will then conduct a univariate analysis where we presented the results in a stacked histogram where the distribution will be illustrated in percentage of each individual variances. Bivariate analysis of the data will not be conducted in this project.

We will also analyse one free-text question where we will categorize the results into specific topics and quantify results. Tables and figures which illustrate the results are depicted in chapter 6.

3.2.4 Data collection method: Interview

We will use semi-structured interview as the qualitative research method to collect data from top administrative personnel managing the strategies at NTNU. The goal of the interview is to explore and get an in-depth understanding of valuable information assets, threats and vulnerabilities at higher educational institutions, which the survey could not. This project will used the "Seven stages of an interview inquiry" from Brinkmann[24].

Stage 1: Thematizing
This stage addresses the *why* and the *what* for conducting this study. First, we will need to formulate the purpose for conducting the interviews. The purpose of the interview is to strengthen the findings from the survey and assess the research question described in section 1.5. We will therefore conduct interviews to achieve an in-depth and holistic identification and evaluation of (1)valuable information assets, (2)threat and (3)vulnerabilities based on the perception of managerial personnel who govern the core task and strategies at NTNU. We will therefor identify people which create, process and manage these core tasks at NTNU[1]. These key personnel will be recruited from:

- Research
- Education and learning environment
- Art and Innovation
- Dissemination and outreach
- Independent managerial group

Secondly, we will need to identify the *what* of the study. This involves developing a conceptual and theoretical understanding phenomena to be investigated. This will be done though the literature study, which will uncover general information assets, threats and vulnerabilities both in general higher education institutions and at NTNU.

[1]https://www.ntnu.edu/strategy(Accessed 10.06.20)

Stage 2: Designing
This stage addresses the *how* the study should be conducted. This involves planning the procedures and techniques of the interview study. Sampling and selecting interview subjects are critical. We will use insight knowledge from the Digital Security Section to map potential interview subjects. We will also use resources like intranet at NTNU to identify members of the 5 different managerial groups. After selecting possible prospects, we will send invitation out by mail. If individuals are unavailable, a new invitation will be sent to another person within the same department. Recommendations from unavailable individuals will also considered. The interviews will be conducted over a 6-week period, from 25.03.20-08.05.20. The interview will be conducted on Skype for Business. This will give the interview subjects a familiar software, which might minimize errors.

Stage 3: Interviewing
This stage address how a semi-structured interview shall be constructed. It is therefore essential to develop a script or an interview guide that can be used at the interviews. The interview will consist of 14 questions, which is similar to the questions featured in the survey. The 14 questions will consist of 1 relating to valuable information assets, 6 relating to threats and 7 relating to vulnerabilities present in higher education. The interview guide will be used at each interview and will start with an introduction. The introduction will present the purpose of the interview, the research topic, and the interview subjects' contribution to the study. They will be also informed that the interview will be recorded and that he/she must consent to this. The interview guide will also contain all question that are featured in the interview. Each question will be brief and have a small introduction. The questions will be almost identical to the questions in the survey; however, they will be formulated to engaged and trigger the interview subject to elaborate on the topic. The interview guide will be structure after the interview guide, however follow-up questions and deviation from the interview guide can occur to achieve an in-depth view of the topic.
A pilot test will be conducted before the first interview. This will give valuable feedback on the formulation of the questions and the time used during the interviews.

Stage 4: Transcribing
This stage addresses how the transcription shall be done. This interview study will conduct an audio-recorder during the interview, to aid in the development of a transcription. We will use the application *Taleopptak 10.2004.1202.0 © 2018 Microsoft* to record the interview. This will increase the validity and reliability of the data collected. The transcription will be constructed with the assistant of the "Voice typing" -feature in Google Docs. Additional edits and read through will also be done with the audio-record to spell check. The transcription of the interview will minimize oral language, and still preserve the authenticity of the interview.

The final transcript will be sent to the interview subject for evaluation, which will further increase its validity. After receiving the final transcription from the interview subject, the audio recordings will be deleted.

Stage 5: Analyzing
This stage addresses how the transcriptions will be analysed. This project will use the "Meaning coding" method to analyse the transcript[24] [p.122]. We will read through the transcript evaluating and categorize the answer based on their statements. This will be done to every transcript. Categorization will entail a more systematic conceptualization of a statement and open the way for quantification. This will make further work more manageable.

Stage 6: Verifying
This stage addresses the validation and generalization of interview knowledge by evaluating other sources of information. As mention in section 3.2.3 we will conduct a survey of deans and managerial personnel presented from each faculty at NTNU. This might validate our findings from the interview and further establish a statistical generalization of the valuable information assets, threats and vulnerabilities that are present at managerial level of the population in higher education institution.

Stage 7: Reporting
This stage addresses how the results of the interview will be presented. We will present each question according to topic(information assets, threats and vulnerability), with interview quotes rendered in a readable style. This will make it more pleasant for the reader. Elements and themes that are frequently mentioned will also be highlighted. A collective summary will also be presented to give the reader a holistic understanding of the findings. The interview will be conducted in Norwegian but will be presented in English. Translation will be conducted manually. The findings will be presented with key quotes and a holistic summary of the statements in chapter 6.

Chapter 4

Literature study: Assets, threats and vulnerabilities in higher education institution

We will in this chapter present findings from the literature review, which address valuable information assets, threats and vulnerabilities in regards information security risk in higher education institutions. A total of 71 sources of literature has been reviewed regarding information security assets, threats and vulnerabilities related to general higher education. The following were the most adequate based on validity and accuracy.

4.1 Assets in higher education

Assets in higher education can range from equipment used in research, personnel(eg. professors, student ect) to information assets. Higher education shares the unique characteristic that it produces large quantities of research data and sensitive data about students and employees. The large quantity of data makes higher education institution an attractive target for cyber criminals. The paper from Pinheiro[25] states that an educational institution "store thousands of information from each student, teacher and staff. Bank accounts, addresses, school transcripts and other valuable data"[p.43]. "In an educational institution there are hundreds of students, dozens of teachers, dozens of employees and collaborators, and the greater the number of people, the riskier and harder to monitor the cyber security gets." [25][p.44]. The following sections will highlight some of the valuable information assets in higher education.

4.1.1 Information assets in higher education

"Colleges and universities collect data from donors, trustees, board members, alumni, students, parents, applicants, faculty, staff, medical patients, consumers, and vendors. The type of data they collect and maintain is wide spread as well, including, sensitive research, financial, medical, employment, personal, and tax data. Colleges and universities also are not only institutions of higher education – they are financial institutions, medical institutions, and retail establishments, and subject to the state, federal and international regulations related to those industries."[26] [p.2]

Listing all information assets in a higher educational institution is a tedious endeavour. There are too many factors that go into creating value in an organisation and listing all is not eligible[6]. Currently, there is a lack of literature sources that list information assets related to higher education institutions. However, the Queensland University of Technology has created a formal inventory of possible information assets at their institution. The following table is a compressed list of information assets depicted from the list from Queensland University of Technology[1]:

Category	**Information assets from Queensland University of Technology**
Student information	-Personal/sensitive information (eg. name, e-mail, address) -Admission details -Class registration information -Student financial information -Student results (eg. exam results) -Records of student support services -Student communications platforms -Study records of course completion and achievements
Learning and teaching information	-Curriculum information -Information associated with curriculum -Online learning information -Course information -Exam information -Library learning resources -Meta data about resources
Research information	-Research management data (eg. resources, business and industry engagement) -Research results and publications -Contract management -Intellectual property (patent)

	-Funding information
Facilities management information	-Campus infrastructure information -Security infrastructure
Financial management information	-General corporate finance information -Management information regarding budget, costing, pricing and report
Governance, strategy and policy information	-Committees management data -Meetings schedules -Legislative documents -Audit and risk management -Strategy documents
IT support information	-Communication and collaboration information -Infrastructure information -Identity and access information (eg. username and password) -Technology procurement information -Technology support information
Human resources information	-Staff and employee records -Recruitment information -Records of Health, Safety & Environment
Alumni information	-Records of personal detail -International partner agreement information -Partnership
Market and Media	-Websites -Market management information -Intranet -Social media information

Table 4.1: Compressed table from Queensland University of Technology inventory of information assets

[1]https://www.qut.edu.au/about/governance-and-policy/information-asset-register(Accessed:15.04.20)

As seen in table 4.1 the compressed list of information assets from Queensland University of Technology illustrates a vast variety of information assets in higher education. Categories like: “Student information”, “Learning and teaching information”, “Research information” are among them.

However, we wish to identify the most critical and valuable information assets in higher institution. The purpose for this is to root out non-crucial assets and to minimize the list to make it more comprehensible. This can be done in several ways. The book from Whitman[2] addresses how to identify information assets, that is critical to the success of an organisation. “When determining the relative importance of each information assets, refer to the organisation’s mission statement or statement of objectives. From this source, determine which assets are essential for meeting the organisation’s objectives, which assets support the objectives, and which are merely adjuncts”[p.328]. Whitman[2] addressed that we need to identify which information assets are critical to the success of the organisation. This can be accomplished by examining the Key Performance Indicators (KPI) and evaluate which information assets that directly and indirectly support these KPI in higher education institutions.

4.1.2 KPI in Higher education

Higher education is relying heavily on government funding in many nations, to maintain educational processes. The pressure is mounting on higher education institutions to make efficient and effective use of these public funds. One method to demonstrate prudent management of these funds, to relevant stakeholders, is through the use of Key Performance Indicators[27][p.983].

Key Performance Indicator (KPI) represents a set of measures that focus on the performance of an organisation, which can determined the current or future success of an organisation[28][p.34]. It gives organisation quantifiable unit to measure growth in the organisation. Another definitions from Ahmed et al.[29] defines KPI as “a measurable value which explains the effectiveness of an institution and how it is achieving key objectives. Institutions use KPI for ensuring that they are going on the right way or not.[...] KPI are the most comprehensive goals for the organization which guide the managers’ activities for making them obtainable”[p.37]. KPI can be used to track progress on specific business objectives and can aid and evaluate if an organisations business strategy is sufficient. Examples for KPI include yearly revenue, new signed deals or costumer increase.

The article from Asif and Cory[27] explains that KPI in higher educational institutions needs to be developed through review and adaptation of the institution’s mission and core academic processes. All dimensions of higher education including research, teaching, and service to the profession must be considered. KPI in higher educational institutions can therefore be anything from the amount of research points the institutions achieves to the number of students completing their studies.

The paper from Asif and Cory[27] provides a comprehensive list of KPI in higher education based on an extensive literature study from 11 different authors. The results are in the following table:

Academic processes	**KPI**
Research performance indicators	Number of research publications
	Number of research projects
	Number of patents
	Number of monographs
	Number of spin-offs from main research stream
	Number of patents addressing local needs
	% of faculty winning academic grants
	Number of technology projects
	Number of research projects addressing local needs
	%of faculty attending conferences and seminars
	Research impact
Teaching performance indicators	Students and other stakeholder satisfaction
	Employer satisfaction with graduates skills
	Number of students completing the program
	Student progression rate
	Dropout rate (Number of dropouts/No. of students enrolled)
	Median score of students
	% of students with a particular GPA
	Course rating – median evaluation of the course by students
	Graduates employment rate
Service performance indicators (university, profession, and community)	Number of academic programs designed
	Participation in curriculum development
	Participation in academic committees
	Students counselling
	Community service
Financial performance	*Revenues*
	Income generated from research projects
	Income generated from consultancies
	Income generated from spin-offs/ patents
	Sponsorships/endowments
	Income generated from tuition
	Expenses
	Total teaching and research cost
	% of budget allocated to the research

Table 4.2: KPIs in higher education from Asif and Cory[27][p.993]

As seen in table 4.2 the list of KPI in higher education provided by Asif and Cory[27], include KPI in academic processes like research performance, teaching performance, service performance and financial performance.

The number of KPI in higher education can also be overwhelming and obscure. There are many types of KPI that can be present in higher education institutions. Ballard[28] managed in his doctoral paper to identify the most valuable KPI in higher education by analysis the content of the system portfolios submitted from 34 higher education institutions. He identified 2139 different KPI's related to these institutions. Ballard created 24 categorize or "Areas Measured" for covering the varying theme of the KPI identified in his work. The following list illustrates the ranking of the top KPI categories based on the Academic Quality Improvement Program in his doctoral thesis[28][p.120]:

KPI category in Higher Education	**Score by %**
Graduation measures	100
Stakeholder satisfaction	100
Employee & HR	97
Enrolment	94
Retention	94
Financial	88
Student success	88
Student engagement	85
Strategic planning	82
Admission	76
Course measures	76
Alumni	70
Advancement	68
Other	68
Grants and Research	62
Community connection	59
Peer comparisons	59
Athletics	41
Facilities	41
Library	32
Business connection	29
Financial aid	29
Connection with other educational institutions	21

Table 4.3: Overall list of KPI's categories ranked by critically. Source: Ballard[28][p.120]

As seen in table 4.3 the list provided by Ballard[28] manage to rank KPI in higher education based on their value. Even though some the KPI categorize or "Areas Measured" attained similar scores, the top four KPI categorize were related

to “Graduation measures”, “Stakeholder satisfaction”, “Employee & HR” and “Enrolment”. We can now identify the most valuable information assets from Queensland University of Technology[2] from Ballard’s list of the most valuable KPI in higher education. This is illustrated in section 4.4.

[2]https://www.qut.edu.au/about/governance-and-policy/information-asset-register(Accessed:15.04.20)

4.2 Threats in higher education

Pinheiro[25] address in his paper that educational institutions are facing a unique security challenges unseen in other sectors. Education institutions are continuously growing and evolve digital solutions to check a student's performance, schedules or even monitor tasks and organize them. This may generate information that may be attractive to hackers and organised criminals. Singar and Akhilesh[30] addressed in his paper, some of the information assets that might be targeted:

- Students' personal data such as email id, contact number and financial information
- Students' educational data such as projects and marks
- Admission details
- Examination details
- Administration details
- Institute's employee details
- Financial data of the Institution

This type of information are attractive to organised criminal, and can be abused. This can contribute to consequences like disruption of learning, loss of intellectual property, identity theft and financial cost[30].

4.2.1 Threats events in higher education

As mentioned in section 2.2.2, threat events or attacks are acts committed by threat agents to gain access to assets. These agents might utilize a wide range of attack methods to gain access into systems in higher education. The following sections will presents sources of literature which illustrates an overview of the most common attacks and threat events to higher education institutions.

Ncube and Garrison(2010), "Lessons Learned from University Data Breaches"[31]

Ncube and Garrison[31] conducted a study which analysed reported data breaches at universities and colleges in the US. The data was obtained from the Privacy Rights Clearinghouse[3]. This data was collected from 165 universities with a total of 290 incidents. The study analysed how data records were stolen during the period 2005 to 2009. The following table and figure illustrates their findings:

[3]https://privacyrights.org/ (Accessed: 02.05.20)

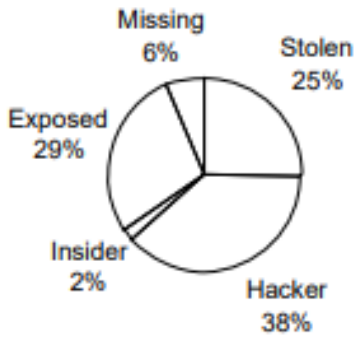


Figure 4.1: Pie chart from Ncube and Garrison,[31][p.32] depicting total breach incidents per category from 2005-2009

TABLE 4. NUMBER OF INCIDENTS PER YEAR						
TYPE	**2005**	**2006**	**2007**	**2008**	**2009**	**TOTAL**
STOLEN	9	15	16	21	12	**73**
HACKER	38	20	16	14	22	**110**
INSIDER	1	1	0	3	1	**6**
EXPOSED	5	13	25	28	12	**83**
MISSING	1	5	6	6	0	**18**
TOTAL	**54**	**54**	**63**	**72**	**47**	**290**

Figure 4.2: Table from Ncube and Garrison[31][p.33], of the number of incidents per year.

As seen in figure 4.1 the percentage of incidents contributing to the most record breaches are "Hacker" incidents. Ncube and Garrison[31] defined the category *Hacker* as "unauthorized remote computer break-ins"[p.28]. These incidents contribute to 38% of the total 290 recorded incidents at universities in the period 2005-2009 and contribute to the largest number of records compromised for four of the five years and the highest number of incidents for three of the five years. Other frequent incidents were "Exposed" which Ncube and Garrison defined as "unprotected data that may be publicly accessible and includes records exposed in e-mail, regular mail, online and through disposal."[p.28], and "Stolen" which Ncube and Garrison defined as "stolen hardware such as desktop computer, laptop, server, flash drive, and hard drive."[p.28]. These incidents may contribute to loss of confidential or personal information in higher education.

Grama(2014), "Just in Time Research Data Breaches in Higher Education"[32]

This research was conducted as a response to EDUCAUSE Higher Education Information Security Council (HEISC)[4] requested to identify the attribution over

[4]https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/about-heisc (Accessed: 02.05.20)

data breaches in higher education. The data presented in this research paper was use from the Privacy Rights Clearinghouse(PRC)[5]. The data set from PRC included 727 breaches from all types of educational institutions between 2005 to 2014. However, the EDUCAUSE Center for Analysis and Research (ECAR) sorted the data set from PRC to only include data breaches from higher education. This resulted in a data set of 562 reported breaches at 324 unique institutions in the US between 2005 and April 25, 2014. 63 % of all breaches were reported from doctoral institutions, however they make up only 7 % of all US institutions. The following pie chart in figure 4.3 illustrates the findings in [32], with breach classification originating from the PRC Chronology of Data Breaches:

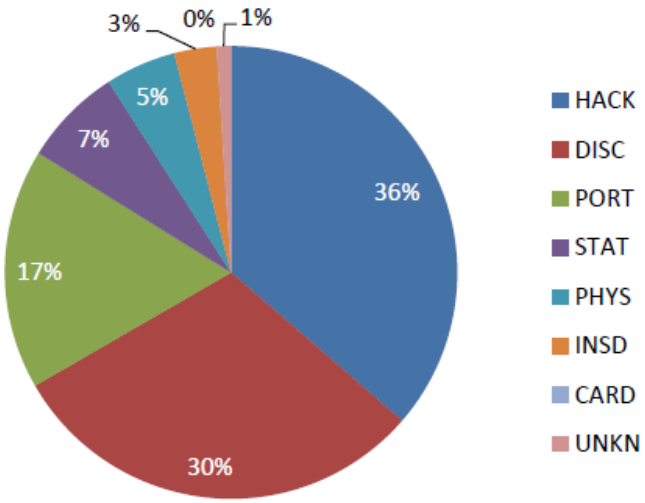


Figure 4.3: Types of data breaches in higher education, 2005-2013[32][p.4]

- **Payment Card Fraud (CARD)**: Fraud involving debit and credit cards that is not accomplished via hacking.
- **Unintended disclosure (DISC)**: Sensitive information posted publicly on a website, mishandled, or sent to the wrong party via e-mail, fax, or mail.
- **Hacking or malware (HACK)**: Electronic entry by an outside party; data loss via malware and spyware.
- **Insider (INSD)**: Intentional breach of information by someone with legitimate access (e.g., an employee or contractor).
- **Physical loss (PHYS)**: Lost, discarded, or stolen non electronic records, such as paper documents.
- **Portable device (PORT)**: Lost, discarded, or stolen portable devices (e.g., laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.).
- **Stationary device (STAT)**: Lost, discarded, or stolen stationary electronic device such as a computer or server not designed for mobility.

[5]https://privacyrights.org/ (Accessed: 02.05.20)

- **Unknown or other (UNKN)**: Breaches that do not fit into the above categories or where a root cause has not been determined.

As seen in in the pie chart from Grama[32] the largest proportion of the reported breaches fell into the "Hacking/malware" classification, which accounted 36% of all breaches. Grama[32] address that these breaches were outside parties accessing records via direct entry, malware, or spyware. The second most reported breaches were the result of "Unintended Disclosures", which where sensitive information which had inadvertently been made publicly available on a website or sent to an unintended recipient via e-mail or fax. The third largest proportion of the reported breaches were due to the loss of a portable device, such as a lost or stolen laptop or memory device.

Payment card fraud were the least likely data breach classification seen among the reported breaches at higher education institutions according to Grama[32]. Only one breach was classified with this tag, which occurred in 2012.

Grama[32] addressed in his paper that potential direct financial costs of data breach in higher education could include legal representation, fines, and the expense of notifying affected individuals. He continued to address that organizations like higher education might face, losses in reputation and consumer confidence. Reputation is very important to higher education institutions. Defacement and reputational consequences could result in a loss of alumni donations and even a reduction in the number of students choosing to apply to or attend the institution.

Verizon inc.,"Verizon annual Data Breach Investigation Report"(2017-2019) [33–35] *(White Paper)*

The Verizon annual *Data Breach Investigation Report*, is created by Verizon Inc., which is one of the largest communication technology companies in the world[6]. The company releases annual reports on data breaches and security incidents that occurred in the biggest industries, including the educational industry. The report from 2019 addresses 41 686 security incidents, of which, 382 incidents occurred in the educational service. The purpose of the study is to raise awareness and provide the ability to learn from the past. Verizon receives data from 73 data sources, 66 of which are organisations external to Verizon. They represent an international group from 86 countries of public and private entities willing to support this annual publication.

The Verizon report from 2019 had 382 incidents, 99 of which were confirmed data disclosure; 2018 had 292 incidents, 101 of which were confirmed data disclosure; 2017 had 455 incidents, 73 of which were confirmed data disclosure. The following table and figure illustrate the number of breaches occurring in the year 2017, 2018 and 2019 systematized into 6 categorize and a histogram, sorted after frequency:

[6]https://www.verizon.com/about/our-company (Accessed 20.04.20)

Threat Events(Action)	2017	2018	2019	Sum
Error	19	16	37	72
Hacking	43	46	42	131
Malware	26	14	16	56
Misuse	5	3	9	17
Physical	2	8	1	11
Social	32	41	38	111
Total number of breaches	127	128	143	398

Table 4.4: Number of security beaches sorted by action and year from Verizon Data Breach Investigation report 2017-2019

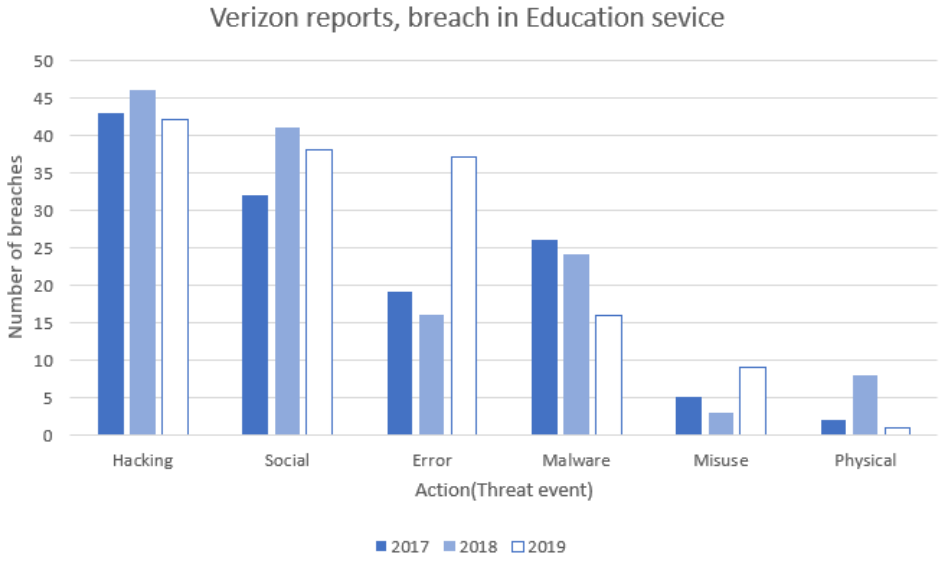


Figure 4.4: Histogram of breaches in Higher education from Verizon annual Data Breach Investigation reports 2017-2019

As seen in table 4.4 and figure 4.4, "Hacking" is the most frequent data breach action conducted in the educational industry. Closely followed up by "Social" methods and "Errors". The least frequent action relating to data breaches in the educational industry is "Physical" action, which had only one case in 2019 according to [35].

The 2019 edition of the "Verizon annual Data Breach Investigation Report"[35] had also added a taxonomy of *patterns* associated with the incident or breach in the educational industry. The *pattern* gives an in-depth illustration of the level of sophistication and attribution which contributed to the incident or breaches. The table 4.5 illustrates the pattern of incident or breaches in the educational industry from the 2019 report[35][p.38]:

Pattern	Miscellaneous Error	Web Application attacks	Everything Else
Precentage	35%	24%	20%

Table 4.5: Patterns that contributed to breach and incidents in educational services from 2019[35][p.38]

As seen in table 4.5, "Miscellaneous Error", "Web Application attacks" and "Everything Else" were the top three patterns present in the educational industry. According to the Verizon report, *Miscellaneous Errors* are "Incidents in which unintentional actions directly compromised a security attribute of an asset"[p.25]. *Web Application attacks* are "Any incidents where an information asset went missing, whether through misplacement or malice"[p.25]. Everything else is "incidents types we frequently encounter but that do not provide enough granularity for us to place in one of the other patterns. [...] About half or more of these breaches could be attributed to social engineering attacks via phishing."[p.39]. These patterns were also present at the top of the 2017 and 2018 edition.

Hackmageddon.com, *Information Security Timelines and Statistics*,[36, 37] (*Website*)

Hackmageddon.com is a website that collect public reports on global cybersecurity attacks and convert them into timelines and graphs. This website creates statistics for four different industry categories. These include: "Public admin, defence, social security", "Human health and social work activities", "Financial and insurance activities" and "Education". The following table and figure illustrates, the number of breaches occurring in the year 2018[36] and 2019[37] systematized into 11 categorize and a histogram, sorted after frequency:

Attacks(Threat Events)	**2018**	**2019**
Account Hijacking	30	26
Brute-Force	0	2
DDoS	2	0
Defacement	0	1
Malware/Pos Malware	16	71
Malicious Script Injection	0	1
Malicious Spam	0	1
SQLi	1	0
Targeted Attacks	4	4
Unknown	20	20
Vulnerability	1	2
Total number of threat events	**74**	**172**

Table 4.6: Threat events from 2018 and 2019, reported by Hackmageddon.com

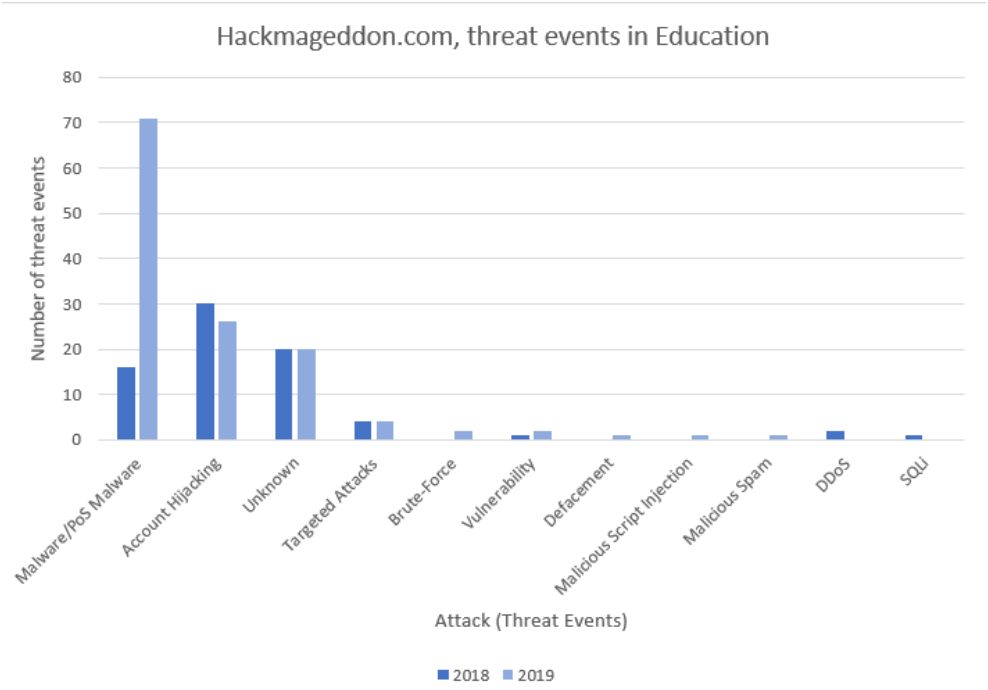


Figure 4.5: Histogram of attacks(threat events) in higher education from Hackmageddon.com, Statistics from 2018 and 2019

As seen in table 4.6 and figure 4.5, "Malware/PoS Malware" is the most frequent cyber-attack in the educational industry according to statistics from 2018[36] and 2019[37] from Hackmageddon.com. Other frequent attacks were "Account Hijacking" and "Unknown". The least frequent cyber-attack to the educational industry were "Brute-Force","Vulnerability", "Malicious Script Injection" and "SQLi" to name a few. The table gives a representation of which attacks and threat events which targets the educational industry. However, Hackmageddon.com usually relays of *attack submission*. Classification of attacks can therefore be subjective and the amount of work regarding follow ups and fact checking is unknown.

4.2.2 Threat agents in higher education

It is hard to attribute the origin of a cyber security attack. Methods like VPN, proxy servers and compromised systems may aid the threat agent in obfuscating his true identity. As of 2019, 4.1 billion people are using the internet[38]. The threat agent can range from a state sponsored group with intentions of stealing information, to a curious "script kiddie" sitting in his basement. The following sources of literature address which threat agents are targeting the educational industry.

Hackmageddon.com, *Information Security Timelines and Statistics*,[36, 37] (*Website*)

Hackmageddon.com is a website that collects public reports on global cybersecurity attacks and convert them into timelines and graphs. Data is based on submission from the public, which the website creates graphs and timeline. In addition to creating statistics on the different information security threats in the industry, it also creates statistics on the possible motivation of these attacks. The following table illustrates, the number of breaches categorized by threat agents in 2018[36] and 2019[37]:

Threat agents(Motivation)	2018	2019
Cyber Crime	70	122
Cyber Espionage	3	5
Hacktivism	1	1
Total	74	128

Table 4.7: Threat agents from 2018 and 2019, reported by Hackmageddon.com

As seen in table 4.7 "Cyber Crime" is the most frequent threat agents in the educational industry according to statistics from 2018[36] and 2019[37]. This data address that the majority of threat agents that attack educational institutions are seeking financial gain and can be labelled as cyber criminals. Other motives addressed by Hackmageddon.com include "Cyber Espionage" and "Hacktivism". However, Hackmageddon.com usually relays of *attack submission*, and classification of the motivation of a cyber-attack can be subjective to the submitter. Human errors can occur and the amount of resources to conduct follow ups and fact checking is unknown.

FireEye Inc. "Cyber Threats to the Education Industry" (2016) [39]
(Whit Paper)

FireEye Inc, is a traded company, which provides software, hardware and services to investigate cybersecurity attacks[7]. They create annual cyber threats intelligence reports for several industries. The latest report from FireEye[39], in regards to

[7]https://www.fireeye.com/ (Accessed: 28.05.20)

cyber threat agents to the education industry was published in 2016. It addresses that the most severe threat agents to higher education is:

- **Advanced persistent Threats** (APT) which are frequently trying to gain access to sensitive intellectual property.
- **Enterprise-like cybercriminals** seeking to steal and profit from sensitive personal and financial information from student, faculty and staff.
- **Hacktivists** trying to deface and disrupt websites, as a method of protest or way to call attention to a cause.

The report[39], addresses that education institutions will likely continue to face different cyber threats from different threat agents, due to the amount of valuable information stored on school networks, along with the ability to launch operations on other targets from the school networks. The report also highlights challenge for administrators at educational institutions to secure school networks due to the size of users and the constant need for internal and external users to access and share information.

4.3 Vulnerabilities in higher education

The amount of general literature regarding information security vulnerabilities in higher education was limited. This might be due to level of sensitivity and possibility of defacement by going public with this information. Only one paper provided a holistic overview of vulnerabilities that might be present to higher educational institutions. However, several papers documented factors that might be present or were highly relevant to vulnerabilities in higher educational institutions. The following section will present vulnerabilities present in higher educational institutions.

4.3.1 Common vulnerabilities in higher education

Lack information security awareness and knowledge
The weakest link in every information system is the user. According to the 2019 Verizon, Data Breach Investigation Report[35] 33% of all cyber breaches in 2018 utilized social attacks. Phishing emails is regarded as the most successfully tactic to gain entrance into an information system. It doesn't matter if our organization has the most sufficient and secure system in the world, as long as the user doesn't exhibit proper awareness regarding information security. This is essential in higher education institutions. The constant influx of student each year makes it challenging to uphold information security awareness in higher education. The paper from Al-Janabi and Al-Shourbaji[40] conducted a study of cyber security knowledge and awareness in an educational environment. The study involved a questionnaire with 760 participants, which included personnel from academic staff, researchers, undergraduate students and employee within educational environments in the Middle East. The result from the study indicated a clear lack of knowledge regarding information security and a low level of awareness within the educational environment. A other paper from Metalidou et al.[41] conducted a study to investigate the association and cause of lack of awareness and other human factors regarding threats to "computer" security in higher education. The study included 103 employees, namely teachers, administrators and working postgraduate students from the academic society of the TEI of Athens. They fund that the root cause of information security awareness in higher education correlated to: Lack of motivation to follow security procedures, lack of general knowledge about attacks, users' risky belief, users' risky behaviour, and inadequate use of technology, all correlated with lack of awareness in higher education. These factors can also affect security measures like password management. The paper from Nyblom et al.[42] conducted a study assessing the root cause of compromised accounts at universities. They concluded in their study that reuse of password across multiple services, weak password strength and general low awareness were the largest contributors to the root cause of compromised accounts at universities.

Awareness and knowledge regarding information security is also crucial in higher educational institutions. Yilmaz and Yalman[43] conducted a comparative analysis of the information security effort at universities. They concluded that "the human factor directly affects every stage" of information security work at higher educational institutions. Information security awareness were addressed as a key element for information security in higher education. The paper also addresses information security awareness as very relevant for adapting the ISO/IEC 27001 framework at an institution. The paper highlights the importance of information security awareness presence at top management level. This was essential for implementation and maintaining the information security policies in the organisation. A other study that substantiates the study by Yilmaz and Yalman[43], is the paper from Rezgui and Marks[44]. They concluded that "The lack of application to information system security awareness has a direct relationship with how the university's information system assets are viewed and valued. In addition, it leads the misalignment of information system goals and objectives with the institution's overall mission and strategic objectives." [p. 249].

The papers in this section has highlighted the lack of information security awareness in higher education and the level of contribution it might provide to general information security effort in higher education. The 2020 paper from Singar and Akhilesh[30] addresses the challenges of have lack of information security awareness in higher education, exceptionally: "Cyber-security awareness plays a substantial role in securing the information of any organization. Nevertheless, cyber-security managers focus more on providing solutions that are technical in nature such as installing routers and firewalls, while they focus less on the threats, as there is the absence of cyber-security awareness among end users." [p.253] The paper also addresses that cyber-security awareness at higher educational institution in developing countries are more absent than in developed countries[p.254].

Lack of resources and finance

Lack of resources and finance are also a root cause to several vulnerabilities in higher education. Ismail and Widyarto (2016)[45] conducted multiple case studies that unveil that colleges and universities in Malaysia had insufficient resources to adapt and implement insufficient security policies. They concluded that the cause of this where be due to limited finical budgets which were allocated to information security in higher education in Malaysia.

However, this problem is not limited to developing countries, but also western countries. The 2015 report from FireEye *"Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do About It"*[46] does also cites financial challenges as present in higher education institutions. The report states that: "The central IT department [at higher educational institution's] share of research grant money is often not enough to secure the data from that research. Despite this mismatch, central IT is still tasked with providing the right level of network security controls. The lack of funding has two negative results. First, it's simply

not enough funding to do the job. Second, it means that most schools can't afford to hire the experts they need to fill critical security roles—especially those who can fight APT attacks. As a result, many university IT departments can't detect and prevent advanced attacks—let alone analyze and respond to them." [p.8] As addressed in the 2015 report from FireEye[46], employment and recruitment of skilled IT and information security managers is essential. It will make it easier to implement and adapt sufficient information security policies in higher educational institutions.

However, the 2019 Cyberthreat Defense Report[47] from CyberEdge, unveiled that the educational industry suffer the biggest IT security skills shortage among 19 different industries. Approximately 91.3% of participant from educational industries experienced of shortage of qualified IT security talents. This is an increase from the 2018 report[48], where the educational industry reported an 87.1% shortage of qualified IT security talents. The 2019 survey included 19 industries from 17 countries with 1200 respondents who manly consisted of qualified IT security workers.

The paper from Pinheiro[25], does also highlight the higher educational industry as under founded. The paper summaries that: "One of the reasons why there is such a high vulnerability in educational institutions that the risk of cyberattacks is so significant is that there is a high exposure to external users."[p.50]. He continuous and address that: "Several institutions have limited budgets for information technology infrastructures and teams. Universities and schools focus budgets on equipment needed for school and labs, for example, and not to protect the network from hackers because they store thousands of sensitive and extremely valuable data for them." [p.50]. Sufficient distribution of resources to essential processes and assets is always challenging, however this section has highlighted that information security resources might not be distributed sufficiently in higher education.

Poor attitude and culture

Academic freedom is a strong norm in higher education. Knowledge should be available for all and not be restricted. Values like openness and transparency are present in higher educational institutions. However, some of these values might generate conflict regarding establishing security controls at higher educational institutions. The 2015 report from FireEye *"Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do About It"*[46] addresses some challenges with higher educational institutions. One is the cultural challenges. The white paper addresses that universities might be reluctant to incorporate any changes that may impede research. Security tools or anything that might limit access to information or communication might be undesirable. It can therefore be challenging to implement security controls to protect valuable information. The report also addresses that IT roles in higher education aren't always separated into different roles. Duties between IT operators and IT security personnel might not be established. This might cause "corruption and collusion between employees, and

inherent conflicts of interest abound. An IT administrator may be reluctant to report incidents or faults in his or her own area of responsibility, for example."[p.7]

Some argue that the present of openness and transparency at higher education might encourage reporting and complains with already established information security policies. However the paper from Grama(2014)[32] might address otherwise: "Many speculate that higher education's culture of openness and transparency encourages breach reporting by institutions, even when such reporting is not legally necessary. This culture does not exist in other industry sectors, where breach reporting could damage an organization's ability to be competitive in that industry. In these instances, a breach may only be reported when it is required by a law or some other regulation, and even then, only when the breach circumstances clearly fall within the purview of the underlying regulation."[p.6]

UNIT- "Tilstandsvurdering av informasjonssikkerhet og personvern blant de statlig eide universitetene og høgskolene" report (2019)[49]

The *Unit - Directorate for ICT and joint services in higher education and research*, in Norway, conducted a report that evaluates of the status of the information security and privacy of university institutions in Norway. The 2019 edition of the *"Tilstandsvurdering av informasjonssikkerhet og personvern blant de statlig eide universitetene og høgskolene"*[49] featured 21 of the state-owned universities in Norway. The purpose of the report was to map the scope and procedure of the information security and privacy work at these institutions. The report addressed several potential vulnerabilities that were present/relevant to the universities in Norway. The following list address the main vulnerabilities these institutions:

Limited human resources and capacity
19 of the 21 institutions described that the human resources that had been invested into managing information security and privacy were not sufficient to meet the demand, despite improvements over the last years. There was also a demand to increase the initiative among "common worker" in several organisations. The lack of resources had also cause work relating to information security to be done partially and insufficiently.

Lack of expertise in information security and privacy
A lack of practical competences relating to information security, were also a reoccurring topic in the report. Concerns regarding violation of information security or incompliance of policies were regarded as frequent. The report also addressed that personnel were unsure of the content of the policies, especially regarding safe storage of research data.

Insufficient implementation of information security management systems
The report addressed that several institutions had implemented or where about to implement information security management systems. However, several institu-

tions had not operationalized the information security management systems, due to lack of personnel, resources and limited knowledge of practical information security and privacy work.

Insufficient overview of information assets in certain types of research
The effort to achieving a holistic overview and mapping of sensitive information assets (eg personnel data) has been conducted and improved due to the implementation of GDPR. However, the report addresses that a repetitive theme in all institutions, were the lack of achieving a complete and holistic overview of sensitive research data, which did not have personnel information. This did not necessarily indicate that all research data had insufficient secure storage, however the report addressed that the details regarding the security measure on how they were implemented was unclear.

Significant technical and organizational complexity
Several institutes did also refer to an increase in technical complexity, which made information security and privacy work more challenging. The report addressed that duplication of applications regarding storage were a problem. This made it challenging for personnel to locate data or knowing which type of actors had access to the information. This increase the possibility of human errors and information leakage to other systems.

Lack of plans for handling major information security incidents
Few institutions had reported of contingency plans to restore operations of systems or IT-infrastructure; however, several institutions had started developing and implementing this. The report also addressed that some institutions had implement mitigation method to limit the damage of a cyber-attacks by conducting backups. IT exercises related to cyber-attacks had also been absent, however several institutions had planned events and exercises to simulate cyber-attacks in 2019.

4.4 Summary of findings from the literature study

This section will present a short summary of the literature study findings regarding general valuable information assets, threats and vulnerabilities present in higher education.

4.4.1 Valuable information assets

As addressed in section 4.1.1 we can determine the importance of information assets, based on their relationship with an organisation's mission statement or statement of objectives. We can therefore identify valuable information assets based on their relationship with an organisations KPI. By combining the table 4.3 from Ballard[28] and the list from Queensland University of Technology (table 4.1), we can synthesised that the following table illustrates the most valuable information assets in higher educational institutions:

Top 4 KPI from Ballard[28]	Information assets categories from QUT
Graduation measures	Student information Learning and teaching information Financial management information
Stakeholder satisfaction	Research information Facilities management information Financial management information IT support information
Employee & HR	Human resources information
Enrollment	Market and Media

Table 4.8: Proposition of the most valuable information assets based of KPI from Ballard[28]

As seen in the table 4.8 information assets categorize like: Student information, Learning and teaching information, Financial management information, Research information to name a few might be ranked as the most valuable information assets. As illustrated in table 4.1, "Student information" might include information assets like: Personal/sensitive information (eg. name, e-mail, address), Student financial information, Student results (eg. exam results), Records of student support services, to name a few. Other information assets that might be included in Learning and teaching information, Financial management information and Research information, might be: Curriculum information, exam information, general corporate finance information, research management data (eg. resources, business and industry engagement) and intellectual property, to name a few.

4.4.2 Threats events and threats agents

The literature study unveiled 4 distinct sources of literature relating to the threat events and 2 distinct sources of literature relating to the threat agents. Only Ncube and Garrison[31] and Grama[32] specified their data set as exclusively from higher educational institutions. Verizon[33–35] and Hackmageddon[36, 37] address threats from the educational industry. We might assume that these sources of literature include data from higher educational institutions and other academic institutions as well. None of these data set were specifically targeting the managerial level at higher educational institutions. The following table illustrates the overview of threat events according to the litterateur findings, rank after occurrence:

Rank	Ncube and Garrison[31]	Grama[32]	Verizon[33–35]	Hackmageddon[36, 37]
1	Hacker	Hacking or malware	Hacking	Malware/Pos Malware
2	Exposed	Unintended disclosure	Social	Account Hijacking
3	Stolen	Loss of portable device	Error	Unknown
4	Missing	Loss of stationary device	Malware	Targeted Attacks
5	Insider	Physical loss	Misuse	Brute-Force
6		Insider	Physical	Vulnerability
7		Payment card fraud		Defacement
8		Unknown or other		Malicious Script Injection
9				Malicious Spam
10				DDoS
11				SQLi

Table 4.9: The rank of the threats present in the educational industry according to literature

As illustrated in table 4.9 “Hacking” and “Malware” appears to be the most occurring threat event to educational institutions. This can be attributed to the rising of malware and ransomware describes in the paper from Singar and Akhilesh[30]. A report from BitSight[50]does also highlights the rise of ransomware, which target educational institutions. It described 2016, as the worst year for educational institutions regrading ransomware attacks. Table 4.9 also illustrates that “Social”, “Error”, “Misuse” and “Unintended disclosure” are also occurring frequently in educational institutions. This can be attributed to human errors in educational institutions. Other threat events like: “Physical loss”, “Stolen”, “Insider”, “Payment card fraud”, “Defacement” are also present threats in educational institutions but occur in minor quantities. However, these events can cause loss of confidential information.

Section 4.2.2 addressed threat agents that targets educational institutions. Hackmageddon.com[36, 37] and the FireEye report “Cyber Threats to the Education Industry”[39] addresses that the following list are the most pressing threat agents to educational institutions:

"Cyber Criminals", who can be groups or individuals, who are using their IT expertise and computer knowledge to steal information and sell it for financial gain.
"Cyber Espionage", who can be state sponsored groups, who is tasked with information gathering of organisations. They can also be classified as Advanced Persistent Threats. Their motivation is to steal classified and valuable information.
"Hacktivist", who are hacker group with political agendas. Their motivation is to push forth their political ideology.

This list of threat agents might also give an indication of the resources and capabilities the threat agent has. The data from Hackmageddon.com[36, 37] reveal that the majority of the threat events can attribute to the category "Cyber crime", as illustrated in table 4.7.

We can therefore synthesis based on our literature findings that the most present threats to higher educational institutions can be attributed to the following categorize:

Organised cyber criminals with financial motives, which might utilize threats events like "Hacker"/"Hacking or malware", "Social", "Payment card fraud" which is motivated by "Cyber Criminals" as cited in Ncube and Garrison[31], Grama[32], Verizon[33–35] and Hackmageddon[36, 37]
Human error, which might cause by threats events like "Exposed", "Unintended disclosure", "Error" and "Misuse", as cited in Ncube and Garrison[31], Grama[32] and Verizon[33–35]
Espionage from state actors, which might utilize threat events like "Hacking" and "Social" which is motivated by "Cyber Espionage" as cited in Verizon[33–35] and Hackmageddon[36, 37].
Loss of confidential information, which might include threat events like "Stolen", "Missing", "Loss of portable devices", "Loss of stationary devices", and "Physical loss" as cited in Ncube and Garrison[31] and Grama[32].
Sabotage from activists which might include threat agents like "Hacktivist" who conduct "Defacement" as cited in Hackmageddon[36, 37].
Insiders, which include the threat event "Insider" as cited in Ncube and Garrison[31] and Grama[32].

4.4.3 Vulnerabilities

The findings in section 4.3 addresses several vulnerabilities that are present in higher education. By examining common vulnerabilities in higher education and the topics addressed in the UNIT report[49], we can categorize present vulnerabilities in higher educational institutions into the following categories:

Lack of information security awareness and knowledge, which has been addressed in the papers Al-Janabi and Al-Shourbaji[40], Metalidou et al.[41], Nyblom et al.[42] and the UNIT report[49]
Lack of resources and finance, which has been addressed in the papers FireEye inc.[46], the 2019 Cyberthreat Defense Report[47] and the UNIT report (2019)[49]
Poor attitude and culture, which has been addressed in the papers FireEye inc.[46] and Grama(2014)[32].

All of these vulnerabilities attributed to social vulnerabilities. According to the 2019 Verizon, Data Breach Investigation Report[35] 33% of all cyber breaches in 2018 utilized social attacks to gain entrance into a system.

4.5 The three factor information security risk in higher education

As illustrated in the sections above there are several elements that incorporates in the assets, threat and vulnerabilities relating to higher educational institutions. As addressed in section 2.2 by Whitman and Mattord[2] we can determine an overview of the information security risk by identifying the **threat** that exploits a **vulnerability** to gain access to **assets**.

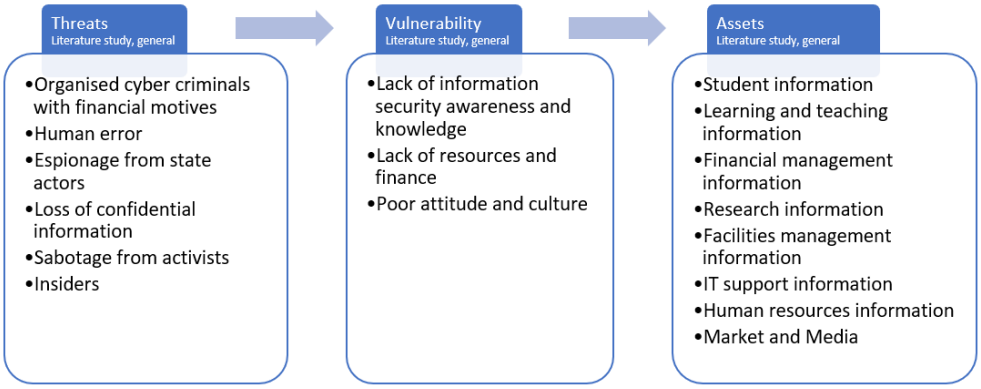


Figure 4.6: General information security risk in higher educational institutions

Figure 4.6 refers to an overview of information security risk in literature where the present threats might exploit vulnerabilities that might gain access to valuable information assets in higher educational institutions.

Consequences of these risks may vary. Singar and Akhilesh[30] list potential consequences as: Disruption of learning, identity theft, loss of intellectual property and financial cost [30]. The paper from Grama[32] addressed that potential consequences of data breach in higher education could include legal representation, fines, and the expense of notifying affected individuals. Other consequences might include loss in reputation and consumer confidence. He states in his paper that reputation is very important for higher education institutions. Defacement and reputational consequences could result in a loss of alumni donations and even a reduction in the number of students choosing to apply to or attend the institution. This can cause long-term effects and is critical for a higher educational institution.

Chapter 5

Case study and literature findings of NTNU

We will in this chapter presents the case study approach that were employed in this research project. The case study is represented through the Norwegian University of Science and Technology and consisted of an excessive literature study of NTNU. A total of 11 sources of literature has been reviewed regarding information security assets threats and vulnerabilities at NTNU. The following were the most adequate based on validity and accuracy.

5.1 Introduction to NTNU

Norwegian University of Science and Technology(NTNU) is a university that specialises in natural science, engineering and technology. It also conducts research topics like arts, health sciences, humanities, medicine social sciences. It is the largest university in Norway per student enrollment and consist of 8 faculties and a university museum. The university has three different campuses in Norway. One in Trondheim, one in Gjøvik and one in Aalesund. The university has a total of 41 965 students and 7 60 employees(2019)[1]. The university was first established in 1910 as Norwegian Institute of Technology (NTH), and later change name to Norwegian University of Science and Technology in 1996[2]. The university is ranked 401-500 in the world, according to the to The World University Rankings[3]. The CWTS Leiden ranking of 2018 ranked NTNU 218th relating to the number of publications[4]. NTNU has also been rewarded the Nobel Prize in Physiology and Medicine in 2014, where John O'Keefe, May-Britt Moser and Edvard I. Moser was rewarded for their discoveries of cells that constitute a positioning system in the

[1]https://dbh.nsd.uib.no/statistikk/ (Accesses:07.07.2020)

[2]https://www.ntnu.edu/about (accessed: 10.06.20)

[3]https://www.timeshighereducation.com/world-university-rankings/norwegian-university-science-and-technology (Accessed:10.06.20)

[4]https://www.leidenranking.com/ranking/2018/list(accessed 10.06.20)

brain in neuroscience[5] The core tasks of NTNU is: Research, Education and learning environment, Art and Innovation and Dissemination and outreach[6] The following figure represents the organisational structure at NTNU:

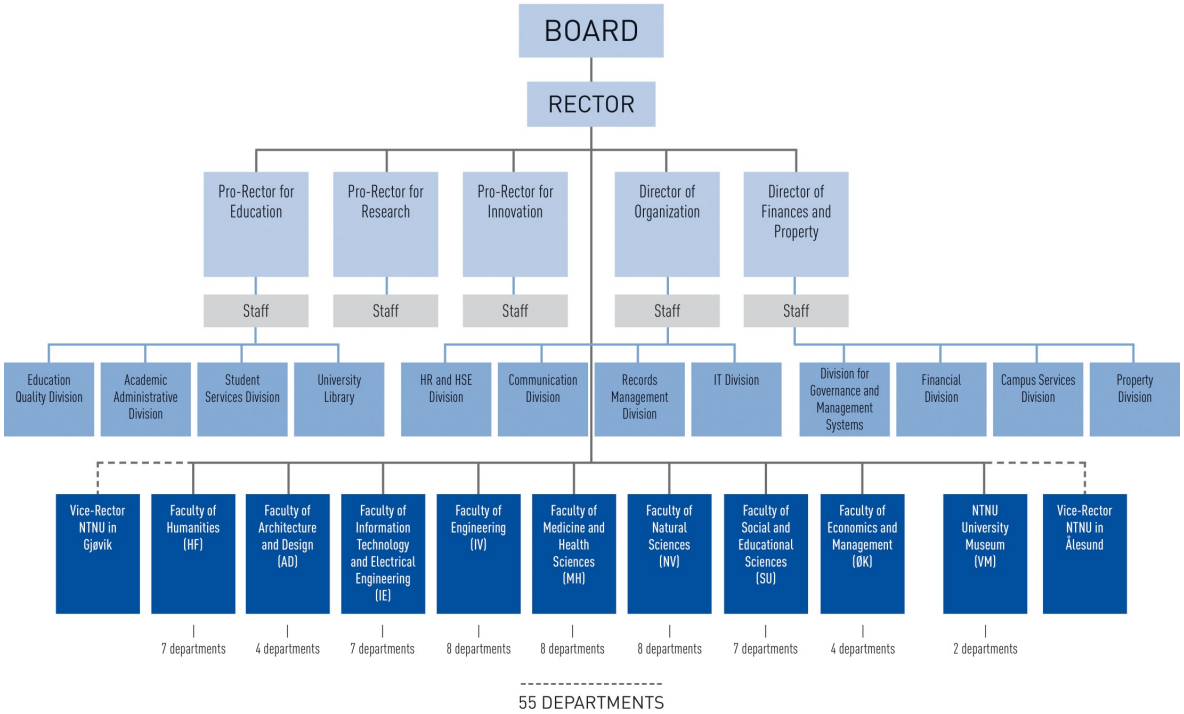


Figure 5.1: Organizational chart of NTNU
7

As illustrated in figure 5.1, the light blue presents the administration and its' sub departments at NTNU. While the dark blue presents the 9 different faculties and the additional two campuses(Gjøvik and Ålesund). These faculties represent a vast range of studies and areas of research and education. The following table list the 9 faculties at NTNU[8]:

[5]https://www.nobelprize.org/prizes/medicine/2014/summary/(Accessed 10.06.20)
[6]https://www.ntnu.edu/core-tasks (Accessed: 17.06.20)
[7]Source: https://www.ntnu.edu/organizational-chart (Last visited:18.06.20)
[8]https://www.ntnu.edu/faculties (Accessed:13.06.20)

Faculty	A.D.	Reasearch & Education details	Number of students(2019)[9]
Faculty of Architecture and Design (AD)	4	Architecture, urban planning, design and visual arts.	1350
Faculty of Humanities (HF)	6	Philosophy, history, media, literature and language.	4205
Faculty of Information Technology and Electrical Engineering (IE)	7	Mathematics, computer science, cybernetics, nano and micro electronics.	7715
Faculty of Engineering (IV)	8	Energy, geology, petroleum, marine technology and mechanical engineering.	6485
Faculty of Medicine and Health Sciences (MH)	8	Medicine, neuroscience, public health and nursing.	6055
Faculty of Natural Sciences (NV)	8	Biology, physics and chemistry	3540
Faculty of Social and Educational Sciences (SU)	7	Pedagogy, geography, social work and psychology	8360
Faculty of Economics and Management (OK)	4	Economics and international business	4190
NTNU University Museum (VM)	2	Natural history, archaeology and cultural history	N/A

Table 5.1: Faculties at NTNU with details (A.D.=Academic Department)

5.2 Literature study: Assets, threats and vulnerabilities at NTNU

The following section presents findings from the literature study, which address valuable information assets, threats and vulnerabilities in regards information security risk at NTNU. A total of 11 sources of literature has been reviewed, and the following were the most adequate based on validity and accuracy.

5.2.1 Valuable information assets at NTNU

Like any other university, the Norwegian University of Science and Technology, does possess the same valuable information assets as depicted in table 4.8. However, NTNU might value some information assets more than others. A 2017 article from Times Higher Education World University Rankings[10], ranked NTNU as number 1 in the world among universities with the biggest corporate links. NTNU had the highest proportion of research in collaboration with single partner from industry. This was due to its research collaboration with SINTEF, which in total co-authored 1711 papers. SINTEF is one of Europe's largest independent research organisation with 2000 employees from 75 countries. It conducts contract research and development for private and public sector in the fields of natural sciences, technology, medicine and social sciences [11].

[10]https://www.timeshighereducation.com/features/universities-with-biggest-corporate-links (accessed 10.06.20)

[11]https://www.sintef.no/en/this-is-sintef/(Accessed:10.06.20)

This might indicate that NTNU have a substantial amounts of information assets that can be linked to corporations. This might imply that NTNU might value the following information assets more than other universities:

- Research management data (eg. resources, business and industry engagement)
- Research results and publications
- Contract management
- Intellectual property

However, the literature study did not identified any other sources of literature that added or subtracted, to the assumptions presented in section 4.4.1.

5.2.2 Threat relevant for NTNU

NTNU, like all other higher educational institutions, are targeted by threat agents. However, NTNU has established a Security Operation Center (SOC), which can handle and manage cyber security incidents for the university. The NTNU SOC is a sub department in the Digital Security Section at NTNU and assess and manage cyber incidents at NTNU. Statistics and data collection from NTNU SOC have given researchers at NTNU the opportunity to conduct research and analysis the information security risk at NTNU. This accumulated in several papers.

Wangen(2019), "Quantifying and Analyzing Information Security Risk from Incident Data"[51]

The paper from Wangen[51] categorize, quantify, and apply an organization's information security incident register for risk analysis. The paper includes data of cyber security incidents assessed by the NTNU SOC between November 2016 and October 2017. 550 incidents where registered in this period. The following figure illustrates the main causes of data incidents at NTNU:

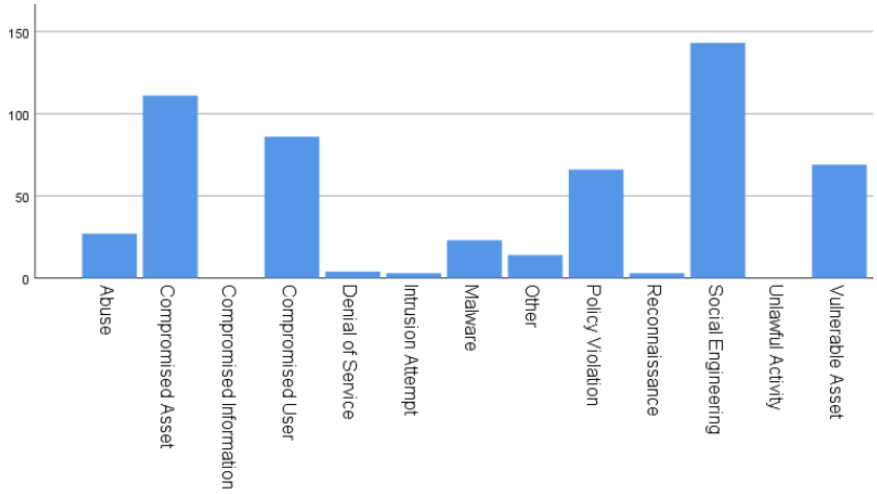


Figure 5.2: Incident causes in the NTNU SOC(Nov 2016- Oct 2017)[51] [p.9]

As seen in figure 5.2 the events that cause the most incidents were Social Engineering(eg. phishing, spear phishing, and whaling/CEO frauds), Compromised Assets, and Compromised Users. The events that caused no incidents were Unlawful Activity and Detection and Compromised Information. This shows that lack awareness and knowledge might be the main cause of data incidents at NTNU.

Ringdalen et al.(2018), "Trusselprofilering og etterretning i åpne kilder"[52]

The bachelor thesis "Trusselprofilering og etterretning i åpne kilder"[52] from 2018 conducted a threat profiling which prepared a detailed description of characteristics and capability of threat actors relevant to NTNU. This thesis feature and presented data of threat actors targeting NTNU and their frequency. This data was originally obtained from the Digital Security Section at NTNU. It is unknown when this data was sampled. The following tables illustrates the table 8 [52][p.30] and table 9 [52][p.30] in their thesis, translated into English.

ID	Threat	Frequency
TA01	Internal and external opportunist	Very likely
TA02	Chaotic actors/activists	Likely
TA03	Competitors	Less likely
TA04	Organised crime	Very likely
TA05	State actors (Sabotage and espionage)	Unknown
TA06	Terrorist	Unlikely
TA07	Unfaithful servant/insiders	Less likely

Table 5.2: Illustration of different threat agents targeting NTNU and their frequency

Likelihood grading	Written description	Likelihood description	Frequency intervall (P)
4	Very likely	Occur once a month	P>13/365
3	Likely	Once to twelve times a year	1/365 to 12/365
2	Less likely	Once every second year	.9/365 to .5/365
1	Unlikely	More rare then every second year	P<.5/365

Table 5.3: Description classification of likelihood of table 5.2

As illustrated in table 5.2 "Internal and external opportunist" and "Organised crime" are the most prominent threats related to information security at NTNU according to the report. The report defines "Internal and external opportunist" as individuals who will seek every opportunity to achieve unjust gain. While "Organised crime" were defined as threat agent with ties to criminal networks who is actively trying to steal information or conduct fraud to achieve financial gain. The bachelor thesis describes "Competitors" and "Unfaithful servant/insiders" as the least frequent threat. "State actors (Sabotage and espionage)" were classified as unknown.

NTNU(2019), "Threat assessment of cyber security at NTNU"[51]

Other sources of literature that highlights the information security threats at NTNU, are the 2019 "Threat assessment of cyber security at NTNU"[53]. This document is not publicly available but provides a holistic overview of the different threat events and threat agents that might be present at NTNU. Sources in this report are gathered from internal and external agents. The following list are threat depicted in the report, order after threat perception:

Organised Criminals
The report address "Organised Criminals" as actors how are motivated by financial gain. They wish to obtain credit card and personnel information which they can easily sell to others. Methods utilized by these agents might include ransomware, which is malware that encrypts data/information and render it useless. Victims are therefore forced to pay a ransom to restore their information. Other methods include phishing/spear phishing which utilizes social engineering through e-mail to reveal information(eg username and password) or click on links. This method is frequently targeting managers and CEO, which is referred to as "Whaling". The NTNU report[51] describes "Organised Criminals" as one of the most persistent threats at NTNU.

State sponsored threats(APT)
The report address "State sponsored threats" or Advanced Persistent Threats(APT) as actors how are motivated by sabotage or theft of important information and technology at NTNU, to achieve technological development goals in their home country. Recruitment of actors inside NTNU is also cited as a potential threat at NTNU. The NTNU report[51] also describes "State sponsored threats" as one of the most persistent threats at NTNU regarding information security.

Insiders
The report address "Insiders" as unfaithful actors or internal opportunists, how might be motivated by revenge or sabotage. These actors are unorganized but can still generate lots of damage. The NTNU report[51] describes "Insiders" as a moderate threat at NTNU regarding information security.

Chaotic Actor
The report address "Chaotic Actor" as activist who might use NTNU resources to push forth their political ideology. This include utilizing methods like denial of service attacks to shut down machines or networks. The NTNU report[51] describes "Chaotic Actor" as a moderate threat at NTNU regarding information security.

Competitors
The report address "Competitors" as national and foreign competitors, who wish to sabotage or conduct defacement operations against NTNU. They may utilize methods through media to achieve this. The NTNU report[51] also describes "Competitors" as a moderate threat at NTNU regarding information security.

The NTNU report[51] depict **organised criminal** and **state sponsored agents** as the most prominent to NTNU in regards to information security. The report also address social engineering methods like phishing/spear phishing as the most persistent threat event at NTNU.

5.2.3 Vulnerabilities at NTNU

Literature regarding information security vulnerabilities in higher education might be limited, as described in section 4.3. This might be due to level of sensitivity that is depicted in such documents. However, two unclassified documents provided insight of the possible vulnerabilities at NTNU.

NTNU, "Mørketallsundersøkelsen ved NTNU 2018"[54]

The 2018, unrecorded statistic study, "Mørketallsundersøkelsen ved NTNU 2018"[54] investigated the information security situation at NTNU to uncover unreported events to achieve better resolutions in regards to cybersecurity. 597 individuals from every faculty at NTNU, participated in the survey. The following two tables presents 9 questions of the original 31 that were featured in the survey, translated into English.

Questions from: Mørketallsundersøkelsen ved NTNU 2018	Results: Yes	No/ Do not know
7. Do you know how you report a information secuirty event?	39.4%	60.6%
9. Do you know if their are installed antivirus programs on your work computer?	77.1%	22.9%
15. Do you know any at your department who has clicked on a link or downloaded files from an e-mail which later proved to be a attempt of deception?	22.1%	77.9%
19. Do you know of any incidents the last 5 years where personal information has been leaked?	11.2%	88.8%
25. Do you know of any incident where a lost device containing files, e-mail, user accounts or information relating to NTNU, has not been reported?	0%	100%
29. Do you know of any sensitive or classified information has been lost due to insufficient storage of the data?	4.7%	95.3%
34. Have you ever been given access to confidential information or systems you shouldn't had access to?	13.5%	86.5%
36. Do you know of any incidents where classified or confidential information relating to research or research results has been lost?	4.5%	95.5%

Table 5.4: Results from the 2018 unrecorded statistic study[54] relating to information security incidents at NTNU

Questions from: Mørketallsundersøkelsen ved NTNU 2018	Results: Strongly agree/ Agree	Slightly agree	Strongly disagree/ Disagree
33. To what extent do you agree with the following statement: "I think it is easy to obtain information outside my area of authority at NTNU"	3.6%	9.2%	77.2%

Table 5.5: Results from the 2018 unrecorded statistic study[54] relating to information security incidents at NTNU

As illustrated in table 5.4 and 5.5, only 39.4% of the 597 participants knew how to report an information security event, 22.1% of the participants knew of incidents where individuals have been tricked by phishing emails, and 11.2% knew of incidents where personal information had been leaked. 12.8% of the participants consider it easy to obtain information outside their area of authority at NTNU. However, nobody knew of incidents were stolen devices hadn't been reported. The 2018 unrecorded statistic study of NTNU uncover many interesting facts about potential vulnerabilities that may be present among employees at NTNU. The study concluded that there is great potential for improving awareness, knowledge and practises among employees regarding information security at NTNU.

Ellestad et al.(2019), "Sikkerhetskultur ved NTNU"[55]

The second document that depicted potential information security vulnerability risk at NTNU, were the 2019 bachelor thesis "Sikkerhetskultur ved NTNU"[55]. It conducted a survey to quantify the information security culture at NTNU. 137 individuals from the IT department at NTNU participated in the survey.
The following two tables presents 9 questions of the original 35 featured in the survey, translated into English.

Questions from: Sikkerhetskultur ved NTNU	Results: Yes	No	Do not know
2. I have read the information security policy	48%	37%	15%
4. I understand the content of information security policy	94%	6%	-
7. I mostly lock my computer when I leave it	92%	8%	-
9. I receive enough information about security	47%	53%	-
10. I know my responsibility when it comes to information security	78%	22%	-

Table 5.6: Results from the 2019 bachelor thesis about security culture at NTNU[55]

Questions from: Sikkerhetskultur ved NTNU	Results: Strongly disagree	Disagree	Slightly disagree	Slightly agree	Agree	Strongly agree
6. I know the risk of opening an e-mail from a unknown source, especially if it contains attachments	4%	0%	0%	1%	28%	66%
11. I receive sufficient training for the tools I use daily	4.4%	6.6%	23.4%	32.1%	26.3%	7.3%
18. My supervisor has information security on the agenda	2.9%	10.9%	16.8%	35.8%	23.4%	10.2%
35. My section implements risk mitigating methods	1.5%	2.9%	14.6%	28.5%	38.7%	13.9%

Table 5.7: Results from the 2019 bachelor thesis about security culture at NTNU[55]

As illustrated in table 5.6 and 5.7, only 47% of the 137 participants believe that they receive enough information about security, and 78% of participant knew their responsibilities regarding information security. Roughly two third of the participant believe they receive enough training for the tools they use daily, and roughly 70% of the participant believe that their supervisor has information security on the agenda. The 2019 bachelor thesis uncover many interesting facts about the information security culture at NTNU[55]. The study concluded that personnel at IT-departments take information security seriously and risk mitigation methods are sufficient in their daily work. However, element of improvement includes training and information management regarding to information security.

5.3 Summary of findings from literature study for NTNU

This section will present a summary of literature findings related to valuable information assets, threats and vulnerabilities at NTNU.

5.3.1 Valuable information assets

As mentioned in section 5.2.1 the literature study has not identify any other sources of literature that added or subtracted to the assumptions presented previously in section 4.4.1. We can therefore assume that the table 4.8 from section 4.4.1 is applicable to NTNU as well.

Top 4 KPIs from Ballard(2013)	Category information assets from QUT
Graduation measures	Student information
	Learning and teaching information
	Financial management information
Stakeholder satisfaction	Research information
	Facilities management information
	Financial management information
	IT support information
Employee & HR	Human resources information
Enrollment	Market and Media

Table 5.8: Proposition of the most valuable information assets based of KPIs from Ballard[28]

As illustrated in table 5.8 information assets regarding “Student information”, “Learning and teaching information”, “Financial management information” and “Research information” might be assumed to be the most valuable information assets.

5.3.2 Threats

The literature study unveiled 3 sources of literature relating to the threat events and threat agent present to NTNU. Wangen[51] address events that caused incidents at NTNU, while Ringdalen et al.[52] and NTNU[51] mainly focus on threat agents. All 3 documents had received data from the section for Digital Security at NTNU. Only the “Threat assessment of cyber security at NTNU”[51] had gathered information from additional external sources. The following table illustrates both threat events and threat agents persistent at NTNU:

Rank	Wangen[51] (Ranked after frequency)	Ringdalen et al.[52] (Ranked after likelihood)	NTNU[51] (Ranked after threat level)
1	Social Engineering	Organised crime	Organised Criminals
2	Compromised Assets	Internal and external opportunist	State sponsored actors(APT)
3	Compromised Users	Chaotic actors/activists	Insiders
4	Vulnerable Assets	Competitors	Chaotic Actor
5	Policy Violation	Unfaithful servant/insiders	Competitors
6	Abuse	Terrorist	
7	Malware	State actors (Unknown)	
8	Other		
9	Denial of Service		
10	Intrusion Attempts		
11	Reconnaissance		

Table 5.9: The rank of the threats present in NTNU according to literature

As illustrated in table 5.9, "Organised criminals", "State sponsored actors(APT)" and "Internal and external opportunist" appears to be the most prominent threat agent for NTNU. "Social Engineering" and phishing appears to be the most prominent threat event that causes several data incidents, according to Wangen[51] and NTNU[51].

Other prominent threat agents prominent to NTNU include: "Chaotic actors/ activists", "Competitors" and "Unfaithful servant/insiders" according to Ringdalen et al.[52] and NTNU[51]. An interesting discovery is that "Malware" is ranked 7^{th} among causes of incidents at NTNU, according to Wangen[51]. This is in great contrast to the results from the literature finding of general threats in higher education, where malware rank among the top threat events, as illustrated in table 4.9. Event caused by human error were also fairly absent among the literature findings. Only Wangen[51] addresses the incident "Policy Violation", which may be attributed to human errors.

We can synthesis based on our literature findings that present threats to NTNU can categorize into the following categories:

Organised cyber criminals with financial motives, which is cited in Ringdalen et al.[52] and NTNU[51].
Espionage from state actors, which is cited in Ringdalen et al.[52] and NTNU[51].
Sabotage from activists which might include threat agents like "Chaotic actors/ activists" which is cited in Ringdalen et al.[52] and NTNU[51].
Insiders, which might include threat agents like "Internal and external opportunist", "Unfaithful servant/insiders" and "Competitors" which is cited in Ringdalen et al.[52] and NTNU[51].
Loss of confidential information, which might include threat events like "Compromised Assets" and "Compromised Users" as cited in Wangen[51].
Human error, which might include threat events like "Policy Violation" as cited in Wangen[51].

5.3.3 Vulnerabilities

The literature study identified two unclassified documents which provided insight of the possible vulnerabilities at NTNU. We can categorize potential vulnerabilities into the following category, based on NTNU's unrecorded statistic study[54] and Ellestad et al.[55].

Lack of information security awareness and knowledge which were cited in both NTNU's unrecorded statistic study[54] and Ellestad et al.[55] as an element for improvement.

"Lack of resources and finance" and "Poor attitude and culture" were cited as two of the three vulnerabilities at higher education in section 4.4.3. However, no literature uncovered such vulnerabilities present at NTNU. A question from NTNU's unrecorded statistic study[54] covered rather the contrary regarding attitude. Question 25 from NTNU's unrecorded statistic study covered that nobody of the 597 participants in the study, knew of any incidents where a lost device hadn't been reported. These literature findings might illustrate that NTNU might be ahead of other higher educational institutions in regarding to information security.

5.4 The three factor information security risk in NTNU

As illustrated in sections above there are several elements that incorporate in assets, threats and vulnerabilities at NTNU. The following figure will illustrate the overall three factor information security risk at NTNU:

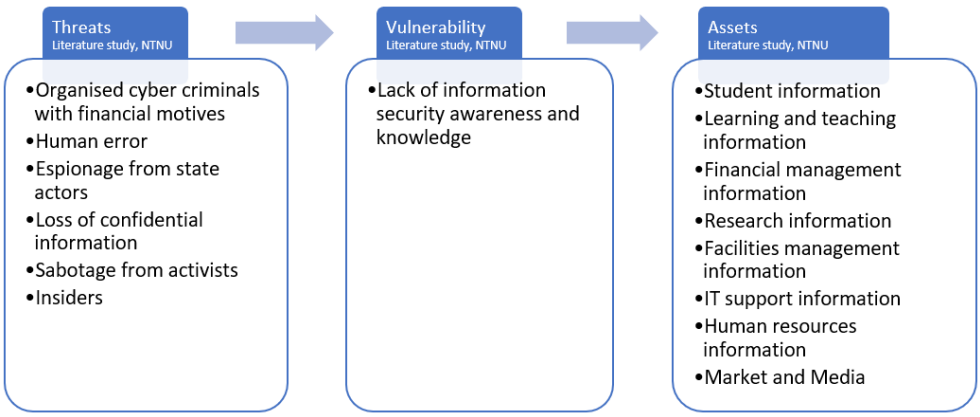


Figure 5.3: Information security risk at NTNU

Figure 5.3 refers to an overview of information security risk at NTNU from literature, where the present threats might exploit vulnerabilities that might gain access to valuable information assets at NTNU. The literature study did not un-

cover any vulnerabilities regarding “Lack Resources and finance” or “Poor attitude and culture” at NTNU. Incidents regarding “Human errors” were to some extent absent from literature, however it might still be present. Asides from these elements the overall information security risk at NTNU and general higher educational institutions are very similar.

Chapter 6

Results and analysis of the survey and interview

This chapter presents the results and analysis of the survey and the interviews of managerial personnel at NTNU.

6.1 Survey demographic and details

All faculties were represented in this survey. The survey was sent to 169 employees at NTNU faculties by email and 107(63.3%) completed the survey. The HF faculties had the biggest response rate of 84.4% and NV had the lowest response rate of 42.9%. 5 of 9 deans participated in the survey. The demographic of the survey is illustrated in table 6.1:

Fac.	n participants	Response	Response rate	Deans	n A.D.	n A.D. represented	Coverage rate A.D.
AD	12	6	50.0%		4	2	50.0
HF	19	16	84.2%	Yes	7	7	100.0
IE	17	12	70.6%	Yes	7	5	71.4
IV	13	8	61.5%	Yes	8	5	62.5
MH	23	18	78.3%	Yes	8	6	75.0
NV	35	15	42.9%		8	7	87.5
SU	22	15	68.2%	Yes	7	5	71.4
OK	16	7	43.8%		4	2	50.0
VM	12	10	83.3%		2	1	50.0
Tot.	169	107	63.3%	5	55	40	72.7%

Table 6.1: Demographic of the survey
(A.D.=Academic Departments)

This project will present and analyse results from 4 of the 14 original questions featured in the survey. This is because they were the only questions that were relevant to the research questions in this project. The following table presents the details regarding of the 4 questions:

Topic	Question	Design	Type	Mandatory
Information assets	How important is to protect the following information assets at your department?	20 information assets ready for ranking	Ranking scale	X
Threats	Do you consider the risk and threats below as relevant to your department?	6 threat descriptions	Yes/No/ Do not know	X
Vulnerability	To what extent do you agree with the following statement?	6 statements	Likert-scale	X
Vulnerability	What do you think is the biggest challenge in regards information security?		Free-text	

Table 6.2: Details of the four survey questions

As illustrated in table 6.2 the questions will try to identify valuable information assets, threats and vulnerabilities that are prominent at faculty level at NTNU. The questions featured in the survey share likeness and similarities with the questions featured in the interview.

6.2 Interview demographic and details

These interviews were conducted on people located in the managerial department at NTNU. All interview subjects had high level managerial positions in either research, education, invasion and art, or the communication sector. There were also other key personnel who had no ties to these sectors. 13 individuals from each of the 5 groups were sampled. This was well within the range of 10-15 interview subject depicted to be the ideal number of interview subjects[24]. The following list presents the departments/titles of the 13 interview subjects that participated in the interviews:

- Pro-Rector for Research
- Education Quality Division
- Student Services Division, Pro-Rector for Education
- Pro-Rector Innovation
- Communication Division
- IT Operations Section
- Rector's staff
- Digital Security Section
- HR and HSE Division

The mayoralty of the participants had acceptable knowledge of the topic. Two participants had minimal knowledge of the topic; however, they manage to respond

sufficiently to the 14 questions and provide valuable insight regarding the subject. The questions featured in the interview share likeness and similarities with the questions featured in the survey. None of the interview subjects participated in the survey.

6.3 Results: Valuable information assets

This section will present the results from the survey and the interview regarding valuable information assets at managerial level at NTNU.

6.3.1 Survey results

The question "How important is to protect the following information assets at your department?" featured 20 preselected information assets. They were based on finding from the literature study, and insight from the Digital Security Section at NTNU. They were selected based on their level of value and involvement in key processes at NTNU. The following two table presents the descriptive statistical analysis and a histogram of the survey results:

	Very Important =5 (Count)	Important =4 (Count)	Slightly Important =3 (Count)	Unimportant =2 (Count)	Not relevant =1 (Count)	Do not know =0 (Count)	N Valid	N Missing	Median	Variance	Range
Username and password	100	5	0	0	1	1	107,00	,00	5,00	,42	5,00
E-mail	48	41	11	4	1	2	107,00	,00	4,00	1,07	5,00
Self-produced research data	61	20	6	0	15	5	107,00	,00	5,00	2,65	5,00
Exams	66	22	0	0	13	6	107,00	,00	5,00	2,63	5,00
Lectures	5	15	39	21	14	13	107,00	,00	3,00	1,81	5,00
Research data received from third parties	65	22	3	0	13	4	107,00	,00	5,00	2,35	5,00
Research contracts (with the EU or others)	41	31	14	2	11	8	107,00	,00	4,00	2,58	5,00
Health research	56	8	1	0	32	10	107,00	,00	5,00	4,19	5,00
Intellectual property and innovational work	47	28	9	2	13	8	107,00	,00	4,00	2,79	5,00
Notes from internal meetings	15	34	43	13	0	2	107,00	,00	3,00	1,00	5,00
Personal information (eg student and staff data)	98	8	0	0	1	0	107,00	,00	5,00	,21	4,00
Publications	9	13	25	31	16	13	107,00	,00	2,00	2,02	5,00
Accounting data	13	30	30	15	4	15	107,00	,00	3,00	2,33	5,00
Sensitive personal information (eg health information and trade union membership)	97	6	1	0	0	3	107,00	,00	5,00	,76	5,00
Strategies, governing documents and guidelines	6	17	30	41	8	5	107,00	,00	2,00	1,34	5,00
Study plan	5	7	12	51	20	12	107,00	,00	2,00	1,44	5,00
Student papers	23	28	21	10	12	13	107,00	,00	3,00	2,78	5,00
Diploma	68	16	4	0	13	6	107,00	,00	5,00	2,69	5,00
Economy reports	9	15	43	24	4	12	107,00	,00	3,00	1,77	5,00
Other communication via digital media	12	33	26	9	2	25	107,00	,00	3,00	2,96	5,00

Figure 6.1: Descriptive analysis of valuable information assets at NTNU

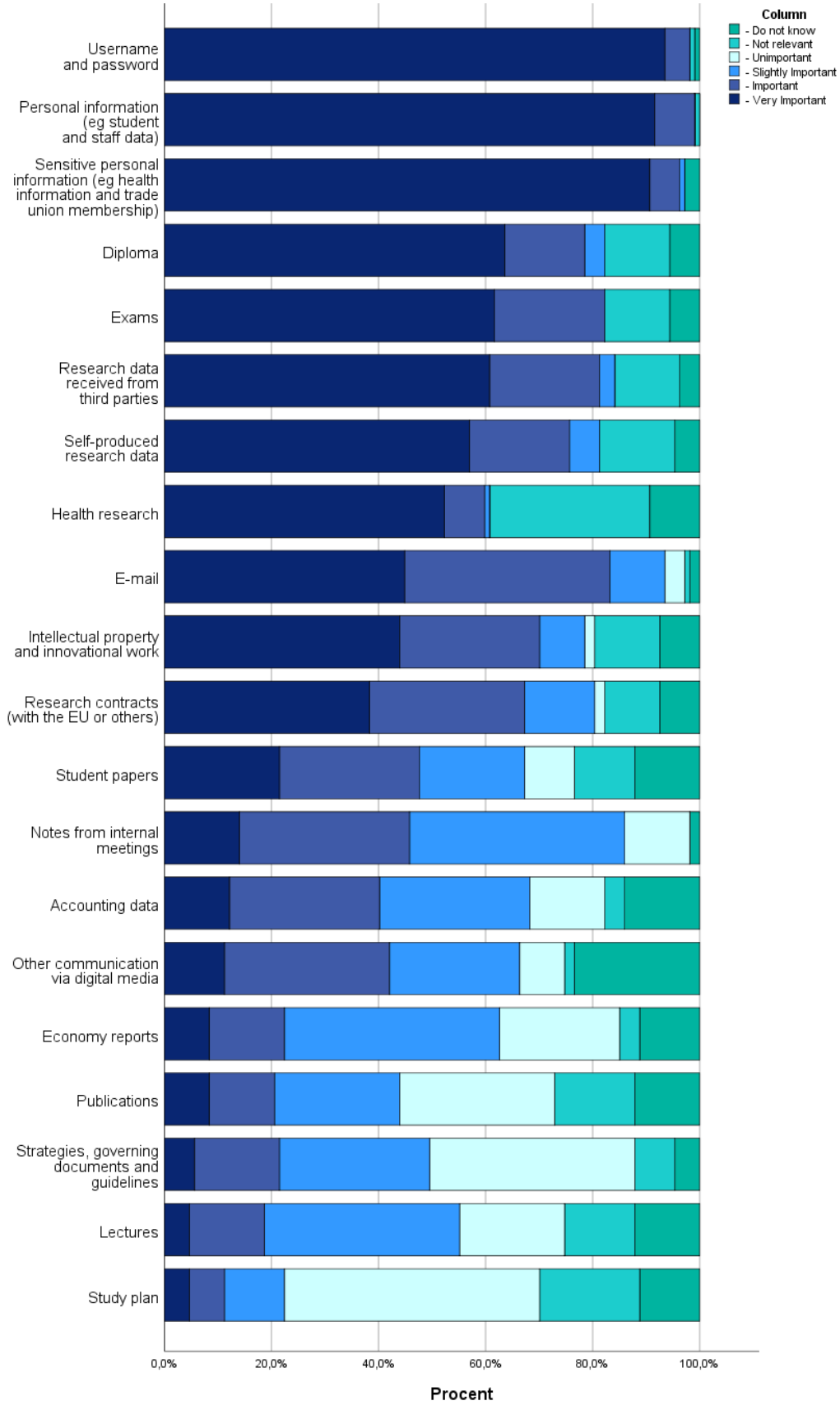


Figure 6.2: Histogram of information asset ranked “Very Important”

Figure 6.1 illustrates the descriptive analysis of the most protection worthy information assets, according to deans and managerial personnel presented from each faculty at NTNU. It features a count of each alternative, along with median, variance and range of the different variables. The median address the central tendency of the distribution. Eight information assets had the median number "5" (Very Important) which indicates that more than 50% of the participants had labelled them as "Very Important". The variance number depicted in figure 6.1 describes how far a set of data is spread out. It illustrates how much participants agree with each other. The largest variance depicted in figure 6.1 are the information assets related to "Health research". However, this is due to the number of participants that does not regard this information assets as relevant to their department.

Figure 6.2 feature a histogram of the distribution. The information assets: "Username and password", "Personal information(eg. student and staff data)" and "Sensitive personal information (eg health information and trade union membership)" where considered the most protection worthy information assets among the 20 information assets. The three least protection worthy information assets were "Strategies, governing documents and guidelines", "Lectures" and "Study plan". The reason for this can be their ability to be duplicated or reproduced.

6.3.2 Interview results

Q1: Is there any data or information that you manage that needs to be protected?

The interview subjects address several information assets during their interview. Their answers were categorized and counted. The following table depict protection worthy information assets according to top administrative personnel at NTNU:

Valuable information assets at NTNU	Quantity	%
Personal data	3	23
Intellectual property	2	15.4
Research management data	2	15.4
Medical information	1	7.7
Research results	1	7.7
Third party information	1	7.7
Personnel management information	1	7.7
Guidelines/policies	1	7.7
Passwords	1	7.7
Tot.	13	100

Table 6.3: Results from the interview question: "Is there any data or information that you manage that needs to be protected?"

As illustrated in table 6.3, "Personal data", "Intellectual property" and "Research management data" were the most frequently addressed information assets by top administrative personnel. "Medical information", "Research results", "Third party information", "Personnel management information", "Guidelines/policies"

and “Passwords” were only mentioned once.

6.4 Analysis: Valuable information assets

The following table illustrates the findings from the survey and the interview.

Survey (Ordered after importance)	**Interview** (Ordered after mentioned frequency)
Username and password	Personal data(3)
Personal information	
Sensitive personal information	Intellectual property(2)
Diploma	Research management data(2)
Exams	
Research data received from third parties	Medical information(1)
Self-produced research data	Research results(1)
Health research	Third party information(1)
E-mail	Personnel management information(1)
Intellectual property and innovational work	Guidelines/policies(1)
Research contracts	Passwords(1)
Student papers	
Notes from internal meetings	
Accounting data	
Other communication via digital media	
Economy report	
Publications	
Strategies, governing documents and guidelines	
Lectures	
Study plan	

Table 6.4: Findings of the most valuable information assets in higher education

As seen in table 6.4, findings from the survey and interviews show that deans and leaders with managerial support at faculties and top administrative personnel share some similarities and differences. “Personal information/data” is ranked on top at both studies. This might illustrate that information assets related to privacy is regarded as the most important information assets according to the managerial level. “Diploma” and “Exams” are also ranked high according to the results from the survey. This corresponds with the literature findings from Ballard[28] illustrated in section 4.4.1, which address “Graduation measures” as the top KPI in higher education.

“Research data” and “Intellectual property” were also ranked fairly high in both the survey and interview study. This does also corresponds with the findings from literature (Ballard[28]) illustrated in section 4.4.1. The “Strategies, governing documents and guidelines” were rank 17^{th} among the 20 preselected information assets in the survey. However, “Guidelines/policies” were also mentioned once by top administrative individual who participated in the interview.

This might indicate that all the information assets depicted in table 6.4 are protection worthy to some extent.

6.5 Results: Threats

This section will present the results from the survey and the interview regarding information security threats at managerial level at NTNU.

6.5.1 Survey results

The question "Do you consider the risk and threats below as relevant to your department?" featured 6 preselected threat descriptions. They were based on finding from the literature study, and insight from the Digital Security Section at NTNU. They were selected based on their level of occurrences and ability to inflict harm on higher education institutions. The following two figures presents the descriptive statistical analysis and a histogram of the distribution:

	Yes =2 (Count)	No =1 (Count)	Do not know =0 (Count)	N Valid	N Missing	Median	Variance	Range
Spying from state actors	38	56	13	107,00	,00	1,00	,43	2,00
Financial losses caused by organized criminal / hacker groups	51	41	15	107,00	,00	1,00	,51	2,00
Insiders	37	53	17	107,00	,00	1,00	,47	2,00
Sabotage from activists	27	58	22	107,00	,00	1,00	,46	2,00
Human error using ICT systems	89	8	10	107,00	,00	2,00	,38	2,00
Loss of confidential information or personal information	83	9	15	107,00	,00	2,00	,52	2,00

Figure 6.3: Descriptive analysis of information security threats at NTNU

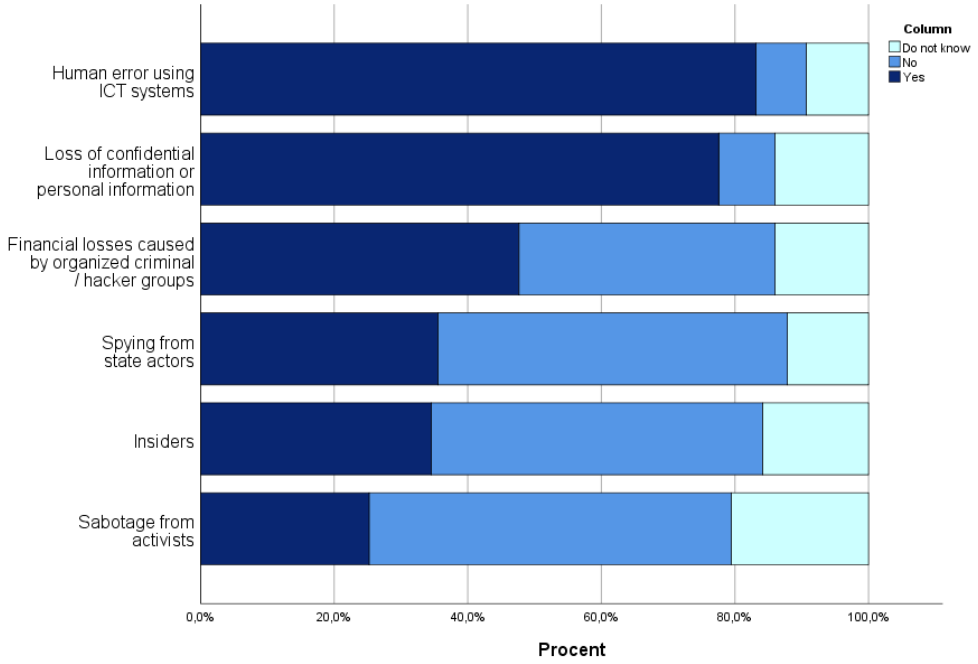


Figure 6.4: Histogram of the most prominent threats according to every NTNU faculty

Figure 6.3 illustrates the descriptive analysis of the most prominent threats, according to deans and managerial personnel presented from each faculty at NTNU. It features a count of each alternatives, along with median, variance and range of the different variables. Only two threats had median-number “2”(Yes) which indicates that more than 50% of the participants had labelled these threats as relevant to their department. The variance number depicted in figure 6.3 were relatively low, which indicates that most of the participant agreed with each other.

Figure 6.4 feature a histogram of the distribution of the threats. The threats “Human error using ICT systems” and “Loss of confidential information or personal information” were considered to be the most prominent threats according to the deans and leaders with managerial support at faculties. “Insiders” and “Sabotage from activists” where considered to be the least prominent threats among the six preselected threats at the NTNU faculties.

6.5.2 Interview results

Q2: To what extent do you perceive espionage by the state actor as a risk to your department?

Key quotes from question 2

"I work a lot internationally and with international cooperation partners, and I have a few strong suspicions of some cases, where someone has been inside and retrieved information from my computer. Some examples over a number of years. I think it's easy to get access to a computer and retrieve information from it. Also, we have employees from all over the world, who we do not know what kind of tasks they are assigned by their home country, either voluntarily or involuntarily."

-Pro-Rector for Research

"For us who work administratively do not see it as the biggest risk, however, departments such as Technology Transfer Office manage a lot of intellectual property rights. [...]They pose a high risk from a commercial perspective. I assume it would be super interesting to get access in there and get patent applications and such."

-Pro-Rector Innovation

"It probably most relevant in areas like innovation. We have research, development and cooperation with industries, and an attacker may use NTNU as a bridge to get access to cooperate information. Since, pretty much everything we do at a university is open, it is accessible. [...]but as a threat, it is primarily research and development conducted with corporations and industry partners."

-Digital Security Section

Approximately half of the interview subjects address the threat of espionage by the state actor as a prominent risk to some degree. This included mostly administrative personnel with ties to research and innovation. The other half addressed it as little to no risk for their department. It appears that this threat is relatively prominent to some key personnel at top administrative level at NTNU. The incident descried in key quote #1 had been reported.

Q3: To what extent do you perceive organized criminal/hacker groups as a risk of causing financial loss to your department?

Key quotes from question 3
"For my department, I see it as a low risk. We do not manage research data, which may have value, but we do manage metadata. Which may have more value for people who are interested in duplicating our business. So, I think it is relatively low."
-Pro-Rector for Research
"I perceive it as a threat, but I do not know if the threat differs from other areas of the university. Crypto locking our data will only hinder our work, in the same way as all other areas of the University. The consequences for our part, will only lead to more work, rather than, loss of sensitive information. Our department do not administer any research results so we do not fear that such things. Even if the probability were high, the consequences would probably not be as great, as for the other areas."
-Pro-Rector Innovation #1
"I think it's low. I don't think there is much to gain. Universities might not be the most willing to pay for example a ransom, so to speak. I would think that private business is more prone to that kind of attacks. However, there is no doubt that attempts from organized hacker targeting NTNU, occurs. [...]I do not think our department are more prone than anyone else, but if you think about NTNU, in general, the threat is present, guaranteed."
-Pro-Rector Innovation #2

The majority of the interview subjects addressed the threat of organized criminal and hacker groups as a prominent risk to some degree. Two individuals didn't have a comment, due to lack of knowledge and insight on the topic. The majority stated that the threat might be more prone to NTNU as an organisation, rather to their individual department. However, majority of the participants addressed that they receive attempts of phishing several times a week. One individual also addressed his concern of financial fraud, due to his involvement with financial management. He told that he approves a lot of invoices and are very cautious when approving and assigning these. However, he had a close relation with the financial and accounting department at NTNU, which gave him confidence in his work.

Q4: To what extent do you perceive insiders to be a risk at your department?

Key quotes from question 4

"It depends, if we are talking exclusively of business or insiders in general. It can be personnel from other universities who have exchange periods with us. Nevertheless, this is characterized by mutual trust and a high degree of openness. There will always be a risk associated with it, but not very high."

-Pro-Rector for Research

"No, I don't perceive it as high risk. Not relation to my department. [...]I'm a little unsure how attractive we would be as a target. I don't think they would find "what" or "whom" we are work with or other business secrets from our partners."

-Pro-Rector Innovation

"No, it's not something I have been thinking of. We have a staff with grown adult, with high average age. Most of them has have worked there for a long time."

-Communication Division

Approximately everybody of the interview subjects addressed the threat as present, but low. One individual had heard a story were a foreign guest had printed out extensive amounts of academic papers from databases and library a few years back. One other individual had heard a story where an individual had entered several offices and used a USB flash drive to upload a script to several computers, a few years back. All incidents had been reported at the time of occurrence.

Q5: To what extent do you perceive that sabotage by activists is a risk to your department?

Key quotes from question 5
"I haven't thought about that. It might be of some risk, but I think the probability is very low. If someone were to attack the university, other places than my department would be a more attractive target, in my opinion"
-Pro-Rector for Research
"Well, that could be quite a big risk, because NTNU generally has a good reputation. We make regular measurements of it. We are the university in Norway that clearly has the best reputation among the Norwegian population. People have confidence in us and we have great credibility when our researchers, for example, go public, participate in debates or discovery something new. It is perceived as a good thing. If something comes from NTNU then it has quality. We try to protect that reputation in the communications department."
-Communication Division #1
"No, there are no current chaotic actors that are a currently a risk to our work. The biggest risk these players can pose is to compromise or hack NTNU's website. This can have consequences for recruitment, accesses of internal communication or external web solutions. [...]Long-term consequences may be reduced research collaboration and projects."
-Communication Division #2

The majority of the interview subjects addressed the threat of sabotage by activists as low or non-existent risk. Only personnel with ties to the communication department regarded the risk as relevant, to their department, but regarded the risk as fairly low. One individual from the communications department addressed the risk of using NTNU to promote "fake-news" as a more prominent threat.

Q6:To what extent do you perceive that human error and lack of expertise in ICT systems is a risk at your department?

Key quotes from question 6

"I do not feel that I have the confidence to say, "I'm now working safely with things and I know what happens if I store some personal data somewhere", when I work from my home office. I'm a little uncertain about it and feel that I need more expertise on that topic."

-Pro-Rector for Research #1

"Yes, there is a certain risk to it. Consequences, would been linked to work, not going as fast as it could have. It would affect work efficiency, like digital tools we manage in our everyday work. However, the biggest consequences would be located elsewhere."

-Pro-Rector for Research #2

"Lack of expertise is a major risk. I have not seen any form of IT security training or how to protect data in general, and I do not think our departments differ from the rest of NTNU, in any way. We have a number of employees with a relatively high age, which might indicate that competence is somewhat limited."

-Pro-Rector Innovation

All participants in the interview addressed the threat of human error and lack of expertise in ICT systems as a prominent risk to some degree. One individual tied to the communication department addressed this threat as the most prominent threat to the communications department. This was due to the he large turnover rate of summer substitute and personnel with 5% position with varying HTML expertise.

Q7: To what extent do you perceive insufficient storage and distribution of personal data as a risk at your department?

Key quotes from question 7

"Sending email with personnel information is a relevant risk. Some students submit their social security number and sensitive information by mail. And I might mistakenly forward it to someone who shouldn't have it, or it gets leaked. So it's a great risk in my opinion, probably the most prevalent."

- Student Services Division, Pro-Rector for Education

"No, I'd say it's really low. We do not manage personal information; it is mainly based on names and e-mail addresses. Everybody can go to publicly available website and find the same information we have."

-Pro-Rector Innovation

"Yes, it certainly is an everyday risk. We need to be vigilant and be careful with it. Both because we manage personal data and because we manage GDPR legislation in the department."

-HR and HSE Division

The majority of the interview subjects addressed the threat of insufficient storage and distribution of personal data as a low risk. Only one individual addressed it as a prominent risk in his department. All interview subjects recognize the importance of legislation's relating to privacy, and that violations could cause serious consequences. Five individuals who participated in the interview did not manage personal or sensitive data in their daily work.

6.6 Analysis: Threats

The following table illustrates the findings from the survey and the interview.

Survey (Ranked after results)	**Interview** (Ranked after survey results)
Human error using ICT systems	Q6: Human error using ICT systems
Loss of confidential information or personal information	Q7: Loss of confidential information or personal information
Financial losses caused by organized criminals/ hacker groups	Q3: Financial losses caused by organized criminals/ hacker groups
Spying from state actors	Q2: Spying from state actors
Insiders	Q4: Insiders
Sabotage from activists	Q5: Sabotage by activists

Table 6.11: Finding of the most prominent information security threat at NTNU according to the managerial level

Red	The majority (100%-60%) label the threat as prominent
Yellow	Half(60%-40%) label the threat as prominent or the majority (100%-60%) label the threat as prominent to some/low degree
Green	The majority (100%-60%) label the threat as low

As seen in table 6.11, findings from the survey and interviews show that deans and leaders with managerial support at faculties and top administrative personnel share some similarities and differences regarding information security threats. “Human error using ICT systems” were addressed as the most prominent threat, both in the survey and the interview. The top administrative personnel at NTNU, labelled the threat “Loss of confidential information or personal information” as low to some degree. This might be due to the lack of personnel managing personal data at top administrative personnel. The results from the survey unveiled that only half of deans and leaders with managerial support at faculties perceive “Financial losses caused by organized criminals/hacker group” as a prominent threat. However, top administrative personnel at NTNU perceive this as a more prominent threat. This might be due to the level data and resources these individuals are managing. This might also imply why “Spying from state actors” were labelled as a more prominent threat by the top administrative personnel, as well.

6.7 Results: Vulnerabilities

This section will present the result from the survey and the interview regarding information security vulnerabilities at managerial level at NTNU.

6.7.1 Survey results

The survey result regarding vulnerabilities will assess two questions. The first question regarding vulnerability were the "To what extent do you agree with the following statement?". This question featured 6 statements and were a mandatory question. The statements featured in this question were based on the findings during the literature study, and insight from the Digital Security Section at NTNU. These six statements cover topics like: *Proper knowledge*, *proper awareness* and *sufficient resources* regarding information security. They were selected based on their level of relevance regarding possible vulnerabilities at managerial level at higher education. The following two figures presents the descriptive statistical analysis and a histogram of the distribution:

	Totally Agree =4 (Count)	Slightly Agree =3 (Count)	Slightly Disagree =2 (Count)	Totally Disagree =1 (Count)	Not relevant / Do not know =0 (Count)	N Valid	N Missing	Median	Variance	Range
There are enough resources in my unit to work with information security	3	18	40	35	11	107	0	2,00	,932	4,00
My unit has sufficient expertise in the field of privacy	6	49	39	9	4	107	0	3,00	,754	4,00
My unit has sufficient expertise in information security	2	29	53	16	7	107	0	2,00	,763	4,00
Employees at my unit are familiar with NTNU's information security management system	4	35	40	12	16	107	0	2,00	1,198	4,00
My unit has discrepancies in information security and privacy as a regular theme in our internal meetings.	4	13	18	64	8	107	0	1,00	,872	4,00
We receive adequate information security assistance when we request it	10	26	32	9	30	107	0	2,00	1,793	4,00

Figure 6.5: Descriptive analysis of information security vulnerabilities at NTNU

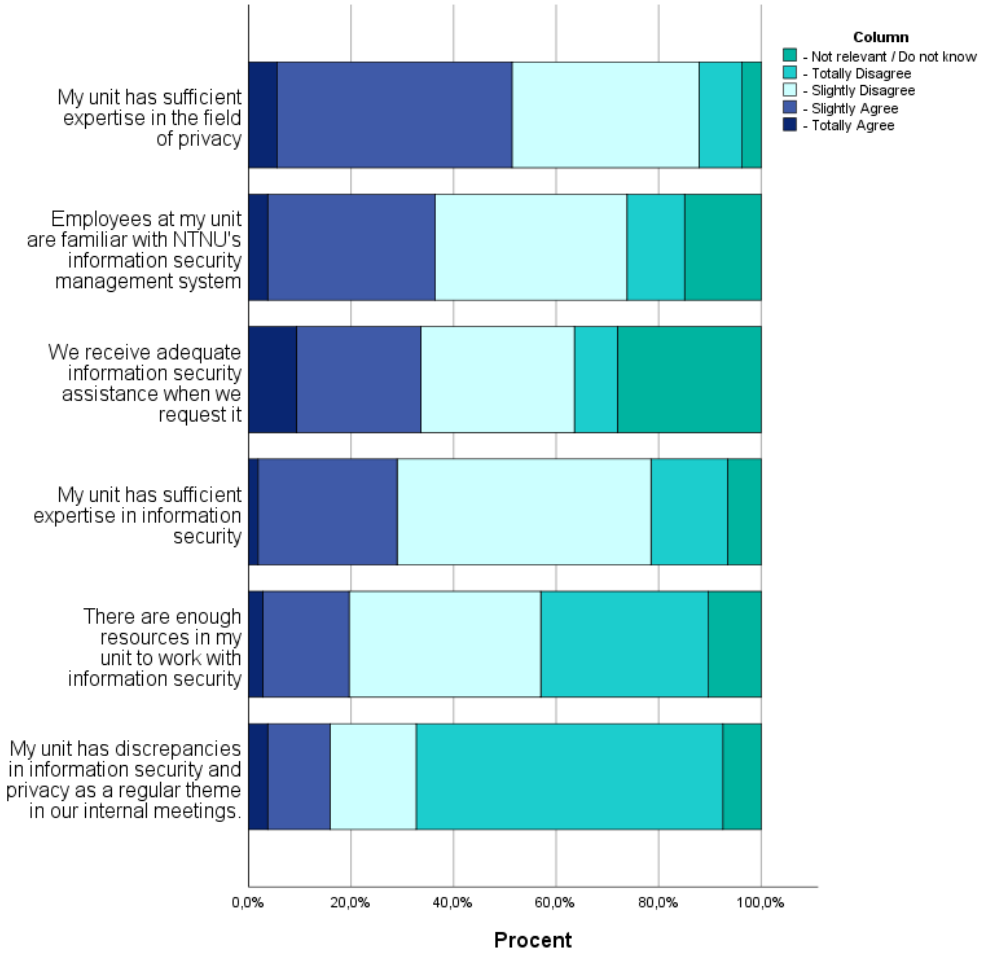


Figure 6.6: Subject matter regarding vulnerabilities ranked after most prominent

Figure 6.5 illustrates the descriptive analysis of the most prominent vulnerabilities according to deans and managerial personnel from each faculty at NTNU. It features a count of each alternative, along with median, variance and range of the different variables. The median address the central tendency of the distribution. The statement "My unit has sufficient expertise in the field of privacy" had the highest median of "3"(Slightly Agree). Four of the six statements had a median of "2"(Slightly Disagree) which indicates that these statements did not correspond with the current situation at NTNU faculties. The variance number depicted in figure 6.5 describes how far the set of data is spread out. The largest variance depicted in figure 6.5, were related to the statement 'We receive adequate information security assistance when we request it". However, this might be due to the number of participants choosing the option "Not relevant/Do not know".

Figure 6.6 feature a histogram of the distribution. The statement "My unit has sufficient expertise in the field of privacy" scored the highest count, in regard to the options "Totally agree" and "Slightly agree", with total of 51%. The statement "My unit has discrepancies in information security and privacy as a regular theme in our internal meetings" and "There are enough resources in my unit to work with information security" had the lowest count in regard to "Totally agree" and "Slightly agree". As illustrates in figure 6.6 almost none of the statements featured in the survey did correspond with the situation current at NTNU faculties.

The second question regarding vulnerabilities were "What do you think is the biggest challenge in regard to information security?" and were a non- mandatory free-text option. This gave us the opportunity to uncover unforeseen vulnerabilities that might be present at the managerial level at NTNU. 58 individuals responded this question, 22 of which addressed more than one challenge. These responses have been categorized into topics and counts 80 challenges in total. The following table illustrated results of the free-text question:

Information security challenges at NTNU	Quantity	%
Knowledge, awareness, culture and attitude	25	31.3
Information storage	8	10
Correct use of ICT-tools	4	5
Procedure and work procedure	4	5
Security in e-mail	4	5
Lack of risk assessment	3	3.8
Export control	2	2.5
GDPR/privacy	2	2.5
General computer security at NTNU	2	2.5
Hacking	2	2.5
Lack of follow-ups/Lack of help	2	2.5
Lack of time and resources for information security	2	2.5
Weak information regrading information security	2	2.5
Employees from abroad	1	1.3
Contract regarding information storage	1	1.3
Data breach, destroyed data	1	1.3
Sharing of of sensitive information with externals	1	1.3
Too much centralization	1	1.3
Loss of indirectly identifiable research data	1	1.3
Lack of interest ("IT should work")	1	1.3
Knowledge of threats and security requirements	1	1.3
Little knowledge of security in ICT solutions	1	1.3
Lack of information security requirements from leaders	1	1.3
Lack of overview of old information	1	1.3
Human error	1	1.3
Training	1	1.3
Security vs openness and accessibility	1	1.3
System complexity and structure	1	1.3
Cumbersome implementation of own applications	1	1.3
Awkward central ICT systems	1	1.3
Keeping up to date	1	1.3
Tot.	80	100

Table 6.12: Results from question: "What do you think is the biggest challenge in regards to information security?"

As illustrated in table 6.12 more than 30% address "Knowledge, awareness, culture and attitude" as an information security challenge at NTNU. These results do also correspond with the results addressed in table 6.6, and the literature findings addressed in section 4.4.3 and 5.3.3.

6.7.2 Interview results

Q8: To what extent do you find that you have sufficient resources in your department to work on information security?

Key quotes from question 8

"We get a lot of assistants from the IT department, however within our department there is none. I'm the GDPR contact in our department, however I have no time to following it up. [...]I don't have time to work with it until it's crucial, but I have instructed others on how to undertake information security in the department. [...]We have so many subjects we are work on, so we leave IT security to the IT security people, and we'll try to do your best on the small details."

-Student Services Division, Pro-Rector for Education

"No, there is no one working with or has that focus, so it is not sufficient, because nobody is assigned the task. Something should be done about it."

-Pro-Rector Innovation

"We discuss it loosely for time to time, however the biggest challenge is time. Time to sit down and go through routines and stuff. But the fact that we have become a digital university has forced us to focus more on general awareness, by putting information security on the agenda."

-Communication Division

The majority of the interview subject addressed the subject matter regarded sufficient resources in their department to work with information security as not sufficient. The majority claimed that general information security resources were non-existent or that lack of time limited the information security work. Only one of the interview subjects claimed that they were satisfied with the available resources in their department.

Q9: To what extent do you feel that your department has sufficient expertise in privacy?

Key quotes from question 9

"We have focused very much on privacy. It has even gotten better after the implementation of GDPR. Additionally, have we had some colleagues who have worked in the health care system in the past, which are extreme on privacy and sensitivity. So, there are much expertise in my group and more will come. However, the practical execution are far more challenging."

-Student Services Division, Pro-Rector for Education

"There may be some lack of awareness, however our absence from working with sensitive information may, cause our lack of focus on the topic. Unlike some others who work in the organization who manage it."

-Pro-Rector Innovation

"I believe we have very good attitude and very high awareness about it, but I don't believe everybody has sufficient knowledge about it or the knowledge of what to do on a PC or who to safeguard general privacy."

-HR and HSE Division

The majority of the interview subjects addressed the subject matter regarding sufficient privacy competence at their department as sufficient or sufficient to some degree. Five individuals who participated in the interview did not manage personal or sensitive data in their daily work. Some of these individuals addressed that the lack management related to personal data, might reduce general attitude for privacy. However, they were well aware of the consequences with consequences linked to violations of privacy.

Q10: To what extent do you feel that your department has sufficient information security expertise?

Key quotes from question 10
"It is low to medium, I would say."
-Pro-Rector for Research
"It's low"
-Pro-Rector Innovation
"It could certainly have been better. We have three employees who are quite interested with those kinds of topics, and it helps that we have this kind of people in our department, who are nit-picky and tell us to "remember this and remember that". But the general awareness should have been better, yes."
-Communication Division

Approximately everybody of the interview subjects addressed the competence regarding information security at their department as insufficient. Only one individual addressed that the competence at his department were very well sufficient. All participants stated that the general information security competence has room for improvements.

Q11: To what extent do you perceive that personnel in your department are familiar with NTNU's information security management system?

Key quotes from question 11

"I think it varies, someone might know some about it and others might know it by heart. Others may have read the document; some may have heard of the document. I'm a little unsure if I know the document myself, I don't remember if I do."

-Student Services Division, Pro-Rector for Education

"If I evaluate people based on myself, I would think that people know it exists, but not necessarily the content of it. People may look it up if you are asked about it. However, if you were to have a quiz about it, I think, nobody would have passed it."

-Pro-Rector Innovation #1

"I see it as satisfying, really. There has been an online campaign on the topic and at intranet on how to behave, with tests. Information is also posted, in relation when attacks occur and such. So, I believe people have sufficient attitude to it."

-Pro-Rector Innovation #2

"We in IT operations have a good understanding of the management system, but we are still jet to operationalize them."

-IT Operations Section

Approximately half of the interview subjects addressed that their department were familiarity with NTNU's information security management system to some degree. These individuals had either, review NTNU's ISMS several times or claimed to be familiar with the content. The other half of the interview subjects address it as low or non-existing. These individuals had either, not heard of it or knew where to find it. The majority of the interview subjects addressed that general competence are varying, but had room for improvement.

Q12: To what extent do you feel your department has information security and privacy as a regular theme in their internal meetings?

Key quotes from question 12
"It is not much. When that topic is relevant it is probably mentioned, but we do not have it on our agenda."
-Pro-Rector for Research
"Information security low, privacy high"
-Education Quality Division
"It is not been a topic, in our department. It has been on the agenda, in my group, due to issues we have had in the group. We manage sensitive information, after all. So we've had a lot of conversations in the group and talked about it. However since we only have one meeting in the department once a semester, it's used to talked about other things, rather than information security."
-Student Services Division, Pro-Rector for Education
"No, it is not often. It is very rare."
-Pro-Rector Innovation

Approximately everybody of the interview subjects addressed that information security were rarely on their internal meeting agendas. However, some of the interview subjects stated that privacy was occasionally on the agenda, and far more frequent than information security. Only one participant stated that information security was a frequent theme on the internal meeting agenda.

Q13: To what extent do you receive sufficient information security information when they request it?

Key quotes from question 13

"I have never asked on behalf of my department regarding it. However, I have, asked on my own behalf and have received sufficient help, when I have requested it."

-Education Quality Division

"[...]it can sometimes be difficult to know where to situate a particular question. I don't always know where to go, so I sometimes makes myself stupid and just asks the question some place."

-Student Services Division, Pro-Rector for Education

"I have the impression that I receive help when needed. However, we have not requested much information security assistance. But in general, I think we have an IT department that follows up if there are any problem. If we request something, we'll get an answer. If we submit something, we'll receive quick feedback."

-Pro-Rector Innovation

Approximately everybody of the interview subjects addressed that they would have or have receive adequate help when they request information regarding information security. However, some participants didn't necessarily know exactly where to ask specific questions relating to information security.

Q14: What would you perceive as the biggest vulnerability or information security challenge at your department?

Key quotes from question 14

"I think of two things, the first one is the human factor, more specifically, the competence to each individual. I think competence regarding IT-security at our department is to poor and does not has proper focus. The second thing is our systems. They are probably too open, and too simple. I wish that some of the systems had two-factor authentication.[...]I was a little surprised when I started here, because I have previously worked at companies, where you are forced to change your passwords either after three or six months. And when I started here at NTNU, where you could have the same password for eternity, until recently. Something so basis, indicates for me that NTNU might not focus so much on security, as I was used to from other companies."

-Pro-Rector Innovation

"It is lack of overview. Our structure of our information assets is too open and there are too many information systems. It is almost impossible to have sufficient overview of where information is located and which classification these data have."

-Digital Security Section

The majority of the interview subjects addressed that the biggest vulnerability at their department were insufficient competence and knowledge regarding information security among individuals, lack of information security attitude, and general lack of awareness and overview of information assets. Four of interview subject had no comment to this question.

6.8 Analysis: Vulnerabilities

The following table illustrates the findings the survey and the interview.

Survey (Ranked after results)	**Interview** (Ranked after survey results)
My unit has sufficient expertise in the field of privacy	Q9: My unit has sufficient expertise in the field of privacy
Employees at my unit are familiar with NTNU's information security management systems	Q11: Employees at my unit are familiar with NTNU's information security management systems
We receive adequate information security assistance when we request it	Q13: We receive adequate information security assistance when we request it
My unit has sufficient expertise in the field of information security	Q10: My unit has sufficient expertise in the field of information security
There are enough resources in my unit to work with information security	Q8: There are enough resources in my unit to work with information security
My unit has discrepancies in information security and privacy as a regular theme in our internal meetings	Q12: My unit has discrepancies in information security and privacy as a regular theme in our internal meetings
(Free-text): What do you think is the biggest challenge in regards to information security?	*Q14: What would you perceive as the biggest vulnerability or information security challenge at your department?*
-Knowledge, awareness, culture and attitude	-Knowledge, awareness and attitude

Table 6.20: Finding of the most prominent information security vulnerabilities at NTNU according to the managerial level

Red	The majority (100%-60%) label the subject matter as inadequate
Yellow -	Half(60%-40%) label the subject matter as inadequate or the majority (100%-60%) label the subject matter as adequate to some/low degree
Green	The majority (100%-60%) label the subject matter as adequate

As seen in table 6.20 findings from the survey and interviews show that deans and leaders with managerial support at faculties and top administrative personnel share some similarities and differences regarding subject matter describing information security vulnerabilities. Approximately half of the participants in both the survey and the interview addressed that their department had sufficient expertise in the field of privacy. However, this did not reflect the level of expertise in the field of information security. Both the survey and interviews unveiled that most of the preselected subject matter regarding vulnerabilities were inadequate or insufficient. However the top administrative personnel in the interviews unveiled in "Q11: Employee at my unit are familiar with NTNU's information security management systems" were adequate to some degree, and "Q13: We receive adequate information security assistance when we request it" were label as adequate by all participants. These two questions were labelled as inadequate by the majority of participant in the survey.

The question "What do you think is the biggest challenge in regard to information security?" accumulated statements and factors regarding: Knowledge, awareness, culture and attitude in both the survey and the interview. This correspond with the result of the six previous preselected questions regarding information security vulnerabilities.

6.9 The three factor information security risk according to the managerial level at NTNU

As illustrated in the section above there are several elements that incorporates in the assets, threats and vulnerabilities related to higher educational institutions. The following figure illustrate the top assets, threats and vulnerabilities according to the managerial level at NTNU, illustrated by the three factor information security risk addressed in section 2.2 by Whitman and Mattord[2].

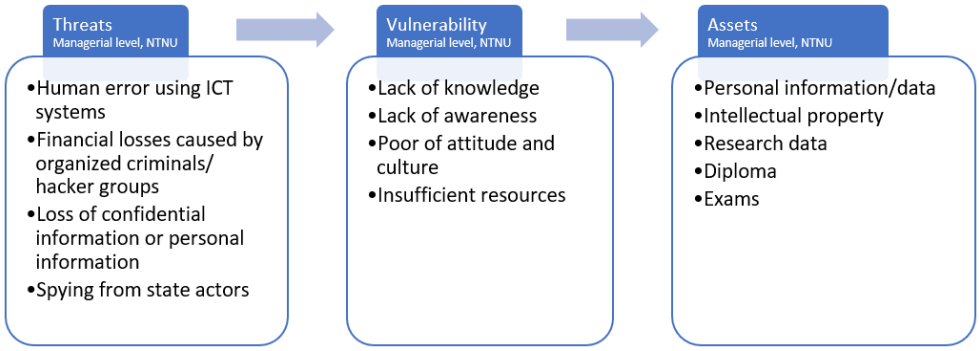


Figure 6.7: Information security risk present at managerial level at NTNU

Figure 6.7 refers to an overview of information security risk at the managerial level in NTNU where threats might exploit vulnerabilities that might gain access to valuable information assets at NTNU. The managerial level at NTNU perceive "Human error using ICT systems" as the most prominent threat. Other threat included "Financial losses caused by organized criminals/ hacker groups", "Loss of confidential information or personal information" and "Spying from state actors". These threats can exploit some prominent subject matter related to vulnerabilities which include: "Lack of knowledge", "Lack of awareness", "Poor attitude and culture" or "Insufficient resources". These threats and vulnerabilities can contribute to the abuse of the most protection worthy information assets accorded to the managerial level. These information assets included "Personal information/data", "Intellectual property", "Research data", "Diploma" and "Exams". These information assets were related to their level of *protection worthiness*. The combination of all these three factors will gives an overview of the information security risks prominent to the managerial level at NTNU.

Consequences of these risk may vary. However, the following papers[30, 32] address that potential consequences as disruption of learning, identity theft, loss of intellectual property and financial cost like legal representation, fines and the expense of notifying affected individuals all can occur. Other long-term effects might include consumer confidence, defacement and loss of reputation, which in turn might affect donations and recruitment.

Chapter 7

Discussion

This chapter will address the research questions in this project and potential future work.

7.1 Discussion of the research questions

RQ1: Which information security risks threatens academia according to literature?
As presented in literature the overall information security risk in general higher education and NTNU shares a high degree of likeness and similarities. Persistent threats like “Organised Criminals” and “Espionage from state actors” might exploit vulnerabilities like “Lack of information security awareness and knowledge”, “Lack of resources and finance” and “Poor attitude and culture” to gain access to valuable information assets like “Student information”, “Learning and teaching information”, “Financial management information”, “Research information”, “Facilities management information”, “IT support information”, “Human resources information”, “Market and Media” in higher educational institutions.

The extensive literature study has given us a sufficient overview of the many information security risk that are prominent to higher educational institutions. However, overall lack of adequate literature regarding threats and vulnerabilities were quite alarming. Few academic papers consisted of adequate or holistic data, regarding information security threat in higher education from a proper source. No academic paper uncovered during the literature study had conducted a holistic study of possible information security vulnerabilities that are present at higher educational institutions.

None of the literature findings had data sets elaborated on the managerial perception regarding information security threats towards their higher educational institution. It is evident that it still exists a shortage of information security risk and general awareness in literature regarding information security risk in higher education.

RQ2: Which information security risks threatens academia according to the managerial level at NTNU?
This project conducted both, a survey in collaboration with the Digital Security Section at NTNU were deans, institution leaders and other managerial support personnel from NTNU faculties participated. Along with interviews of top administrative personnel managing core processes at NTNU. Both the survey and the interview assessed the perception of valuable information assets, threats and vulnerabilities in higher education based on findings from literature. The combination of these three elements gives an overview of the information security risk at NTNU.

The managerial level at NTNU perceive "Human error using ICT systems" as prominent threat, along with "Financial losses caused by organized criminals/ hacker groups" and "Loss of confidential information or personal information" (illustrated in table 6.11). These finding depict that internal in the institutions may be equal, or even more prominent than external threats.

These threats can exploit some prominent subject matter related to vulnerabilities addressed by the managerial level at NTNU. These subject matters were lack of knowledge, awareness, attitude and culture, or insufficient resources. These finding depict that social vulnerabilities and factors might be more prominent than technical vulnerabilities.

Threats and vulnerabilities can contribute to the abuse of the most protection worthy information assets accorded to the managerial level at NTNU. These information assets included "Personal information/data", "Intellectual property", "Research data", "Diploma" and "Exams". These information assets were related to their level of *protection worthiness*. Their level of protection worthiness is a subjective variable based on the participants opinion. Combining all these three factors will gives an overview of the information security risks prominent to the managerial level at NTNU.

Consequences related to these risks might include disruption of learning, identity theft, loss of intellectual property and financial cost. Long term effects can be loss of reputation, loss of donation and decline in student application. These finding depict the information security risk according to the managerial level at NTNU.

RQ3: How do the information security risk identified in literature overlap with risk identified at the managerial level in NTNU?
As depicted in section4.5, section 5.4 and section 6.9 the overall information security risk identified in both the literature study and at the managerial level in NTNU shares a high degree of likeness and similarities.

Literature from both NTNU and general higher educational institution addressed "Organised cyber criminals" and "Human error" as the most prominent threat to information security at higher education among others. Vulnerabilities identified in literature does also correspond with the vulnerabilities depicted by the managerial level at NTNU. Valuable information assets identified in literature related to "Graduation measures", "Stakeholder satisfaction", "Employee & HR" and "Enrollment" were identified as the most valuable. These does also correspond with the information assets identified by the managerial level at NTNU. These included "Personal information/data", "Intellectual property", "Research data", "Diploma" and "Exams". These findings illustrate that information security risk depicted in literature overlap and correspond with the risk identified at the managerial level in NTNU.

7.2 Suggestions for future research

This thesis has given an overview of information security risk based on valuable information assets, threats and vulnerabilities present in higher education institutions. However, a quantitative study of the top administrative level of NTNU were absent in this study. It can therefore be beneficial to conduct further studies of the top administrative level of NTNU regarding information security.

Other future research topics can relate to an in-depth study of vulnerabilities related to information security risk at higher education institutions. A qualitative or quantitative study, investigating the level of resources and finance related to information security and the level attitude and culture regarding information security at higher education can be beneficial.

Chapter 8

Conclusion

One can never achieve completely accurate perception of the information security risk at any organisation. Several factors might intervene and obfuscate the results. It is therefore pivotal to collect data from several sources to achieve accurate and valid results. This project has utilized qualitative and quantitative research methods to determine the information security risk by identifying valuable information assets, threats and vulnerabilities at higher educational institutions.

The finding from this project show that the overall information security risk identified in the literature study and at the managerial level at NTNU shares a high degree of likeness and similarities. Threats based on "Organized criminals" and "Human error" were among the topmost prominent threats in higher education. These threats can exploit vulnerabilities prominent in higher education which includes lack of information security knowledge, awareness, attitude, culture and insufficient resources. Valuable information assets in higher education relating to "Graduation measures", "Stakeholder satisfaction", "Employee & HR" and "Enrollment" were identified as the most valuable information assets and abused of these would be critical to higher education institutions. The combination of these three factors illustrate an overview of the information security risk relevant for higher educational institutions.

Bibliography

[1] PST, 'Nasjonal trusselvurdering 2020', Norwegian, White Paper, Feb. 2020, Library Catalog: www.pst.no, p. 32. [Online]. Available: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/ (visited on 16/06/2020).

[2] M. Whitman, *Management of information security*, eng, 2018.

[3] J. Chapman, 'How safe is your data? cyber-security in higher education', 2019.

[4] 'ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls', International Organization for Standardization, Geneva, CH, Standard, Sep. 2014.

[5] R. Von Solms and J. Van Niekerk, 'From information security to cyber security', *computers & security*, vol. 38, pp. 97–102, 2013.

[6] D. Landoll, 'The security risk assessment handbook: A complete guide for performing security risk assessments', 2011.

[7] 'ISO/IEC 27002:2013 Information technology – Security techniques – Information security risk management', International Organization for Standardization, Geneva, CH, Standard, Jul. 2018.

[8] E. Turban, L. Volonino and G. Wood, *Information Technology for Management: Advancing Sustainable, Profitable Business Growth*. Wiley, 2013, ISBN: 978-1-118-35704-0. [Online]. Available: https://books.google.no/books?id=vJO7nE7EI64C.

[9] P. Bocij, A. Greasley and S. Hickie, *Business Information Systems, 5th edn: Technology, Development and Management for the E-Business*, English, 5 edition. Harlow, England ; New York: Pearson, Dec. 2014, ISBN: 978-0-273-73645-5.

[10] C. J. Vidal and M. Goetschalckx, 'Strategic production-distribution models: A critical review with emphasis on global supply chain models', *European journal of operational research*, vol. 98, no. 1, pp. 1–18, 1997.

[11] H. Gupta, *Management Information System*. International Book House, 2011, ISBN: 978-93-81335-05-5. [Online]. Available: https://books.google.no/books?id=PWRYwOJ8FmgC.

[12] F. Burstein, P. Brézillon and A. Zaslavsky, *Supporting Real Time Decision-Making: The Role of Context in Decision Support on the Move*, ser. Annals of Information Systems. Springer US, 2010, ISBN: 978-1-4419-7406-8. [Online]. Available: https://books.google.no/books?id=8wiP2js4kvEC.

[13] D. M. Brandon, *Project management for modern information systems*. IGI Global, 2005.

[14] R. Arababadi, S. Moslehi, M. [Asmar, T. Haavaldsen and K. Parrish, 'Energy policy assessment at strategic, tactical, and operational levels: Case studies of EU 20-20-20 and U.S. Executive Order 13514', *Energy Policy*, vol. 109, pp. 530–538, 2017, ISSN: 0301-4215. DOI: https://doi.org/10.1016/j.enpol.2017.07.042. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0301421517304731.

[15] W. Darmalaksana, M. Ramdhani, R. Cahyana and A. Amin, 'Strategic design of information system implementation at university', *International Journal of Engineering and Technology(UAE)*, vol. 7, pp. 787–791, May 2018. DOI: 10.14419/ijet.v7i2.29.14257.

[16] S. Posthumus and R. Von Solms, 'A framework for the governance of information security', *Computers & security*, vol. 23, no. 8, pp. 638–646, 2004.

[17] E. McFadzean, J.-N. Ezingeard and D. Birchall, 'Perception of risk and the strategic impact of existing it on information security strategy at board level', *Online Information Review*, 2007.

[18] S. Rajasekar, P. n. Pitchai and C. Veerapadran, 'Research methodology', Jan. 2006.

[19] S. Gürbüz, 'Survey as a quantitative research method', in. Jan. 2017.

[20] J. W. Creswell and C. N. Poth, *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications, 2016.

[21] J. Ritchie and J. Lewis, *Qualitative research practice : A guide for social science students and researchers*, eng, London, 2003.

[22] A. J. Onwuegbuzie and R. Frels, *Seven Steps to a Comprehensive Literature Review: A Multimodal and Cultural Approach*, en. SAGE, Feb. 2016, pp. 48–64, ISBN: 978-1-4739-4412-1.

[23] OECD, *"Good Practices in Survey Design Step-by-Step" in Measuring Regulatory Performance: A Practitioner's Guide to Perception Surveys*. 2012, Type: doi:https://doi.org/10.1787/9789264167179-6-en. [Online]. Available: https://www.oecd-ilibrary.org/content/component/9789264167179-6-en.

[24] S. Brinkmann, *Doing interviews*, eng, Thousand Oaks, California, 2018.

[25] J. Pinheiro, 'Review of cyber threats on educational institutions', in *Digital Privacy and Security Conference 2020*, p. 43.

[26] D. A. P. James J. Giszczak, 'Pass or fail? Data privacy and cybersecurity risks in higher education', English, McDonald Hopkins, White Paper, Aug. 2016. [Online]. Available: https://www.mcdonaldhopkins.com/Insights/August-2016/Pass-or-fail-Data-privacy-and-cybersecurity-risks.

[27] M. Asif and C. Searcy, 'A composite index for measuring performance in higher education institutions', *International Journal of Quality & Reliability Management*, 2014.

[28] P. J. Ballard, 'Measuring performance excellence: Key performance indicators for institutions accepted into the academic quality improvement program (aqip)', 2013.

[29] A. E.-A. Ahmed, M. Badawy and H. Hefny, 'Exploring and measuring the key performance indicators in higher education institutions', vol. 18, pp. 37–47, Jan. 2018.

[30] A. V. Singar and K. Akhilesh, 'Role of cyber-security in higher education', in *Smart Technologies*, Springer, 2020, pp. 249–264.

[31] C. Ncube and C. Garrison, 'Lessons learned from university data breaches', *Palmetto Business & Economic Review*, vol. 13, pp. 27–37, 2010.

[32] J. Grama, 'Just in time research: Data breaches in higher education.', *EDUCAUSE*, 2014.

[33] Verizon Inc., '2017 Data Breach Investigations Report', English, White Paper, Apr. 2017, Library Catalog: enterprise.verizon.com. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/ (visited on 20/06/2020).

[34] V. Inc., '2018 Data Breach Investigations Report', English, White Paper, Apr. 2018, Library Catalog: enterprise.verizon.com. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/ (visited on 20/06/2020).

[35] V. Inc., '2019 Data Breach Investigations Report', English, White Paper, May 2019, Library Catalog: enterprise.verizon.com. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2019/introduction/ (visited on 20/06/2020).

[36] P. Passeri, *2018: A Year of Cyber Attacks*, en-US, Library Catalog: www.hackmageddon.com, Jan. 2019. [Online]. Available: https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/ (visited on 06/07/2020).

[37] P. Passeri, *2019 Cyber Attacks Statistics*, en-US, Library Catalog: www.hackmageddon.com, Jan. 2020. [Online]. Available: https://www.hackmageddon.com/2020/01/23/2019-cyber-attacks-statistics/ (visited on 06/07/2020).

[38] D. B.-M. ITU, 'Measuring digital development: Facts & figures 2019', *ITU Publication*, Nov. 2019, Library Catalog: news.itu.int Section: Broadband/Network, ISSN: 978-92-61-29511-0. [Online]. Available: https://news.itu.int/measuring-digital-development-facts-figures-2019/ (visited on 28/05/2020).

[39] FireEye, Inc., 'CYBER THREATS TO THE EDUCATION INDUSTRY', en, White Paper, 2016, Library Catalog: www.fireeye.com. [Online]. Available: https://www.fireeye.com/current-threats/reports-by-industry/education-threat-intelligence.html (visited on 15/06/2020).

[40] S. Al-Janabi and I. AlShourbaji, 'A study of cyber security awareness in educational environment in the middle east', *Journal of Information Knowledge Management*, vol. 15, p. 1 650 007, Feb. 2016. DOI: 10.1142/S0219649216500076.

[41] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, G. Giannakopoulos and C. Skourlas, 'Human factor and information security in higher education', *Journal of Systems and Information Technology*, vol. 16, no. 3, pp. 210–221, 2014.

[42] P. Nyblom, G. B. Wangen, M. Kianpour and G. Østby, 'The root causes of compromised accounts at the university', Jan. 2020, pp. 540–551. DOI: 10.5220/0008972305400551.

[43] R. Yilmaz and Y. YALMAN, 'A comparative analysis of university information systems within the scope of the information security risks.', *TEM Journal*, vol. 5, no. 2, pp. 180–191, 2016, ISSN: 22178309. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=115717068&site=ehost-live.

[44] Y. Rezgui and A. Marks, 'Information security awareness in higher education: An exploratory study', en, *Computers & Security*, vol. 27, no. 7, pp. 241–253, Dec. 2008, ISSN: 0167-4048. DOI: 10.1016/j.cose.2008.07.008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404808000485 (visited on 16/03/2020).

[45] W. Ismail and S. Widyarto, 'A formulation and development process of information security policy in higher education', in *1st International Conference on Engineering Technology and Applied Sciences, Afyonkarahisar*, 2016.

[46] FireEye, Inc., 'Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do About It', en, White Paper, 2015, Library Catalog: www.fireeye.com. [Online]. Available: https://www.fireeye.com/current-threats/threat-intelligence-reports/wp-storming-the-ivory-tower.html (visited on 15/06/2020).

[47] C. Group, '2019 Cyberthreat Defense Report', en-US, White Paper, Mar. 2019, Library Catalog: cyber-edge.com. [Online]. Available: https://cyber-edge.com/portfolio/2019-cyberthreat-defense-report/ (visited on 22/06/2020).

[48] C. Group, '2018 Cyberthreat Defense Report', en-US, White Paper, Mar. 2018, Library Catalog: cyber-edge.com. [Online]. Available: https://cyber-edge.com/portfolio/2018-cyberthreat-defense-report/ (visited on 22/06/2020).

[49] Unit - Department for ICT and joint services in higher education and research, 'Tilstandsvurdering-av-informasjonssikkerhet-personvern-blant-de-statlig-eide-universitetene-og-hogskolene.pdf', Norwegian, Tech. Rep., Jul. 2019. [Online]. Available: https://www.unit.no/sites/default/files/media/filer/2019/06/Tilstandsvurdering-av-informasjonssikkerhet-personvern-blant-de-statlig-eide-universitetene-og-hogskolene.pdf (visited on 29/01/2020).

[50] B. T. Inc, 'The Rising Face of Cyber Crime: Ransomware Report', en, White Paper, 2016, Library Catalog: info.bitsight.com. [Online]. Available: https://info.bitsight.com/bitsight-insights-ransomware (visited on 15/06/2020).

[51] G. Wangen, 'Quantifying and Analyzing Information Security Risk from Incident Data', in *Graphical Models for Security*, M. Albanese, R. Horne and C. W. Probst, Eds., Cham: Springer International Publishing, 2019, pp. 129–154, ISBN: 978-3-030-36537-0.

[52] Ola Flølo Ringdalen, Lasse Sørli, Sebastian Bråthen Warhuus and Arne Martin Laxå, 'Trusselprofilering og etterretning i åpne kilder', Norwegian, NTNU, Bachelor Thesis, May 2018, p. 111.

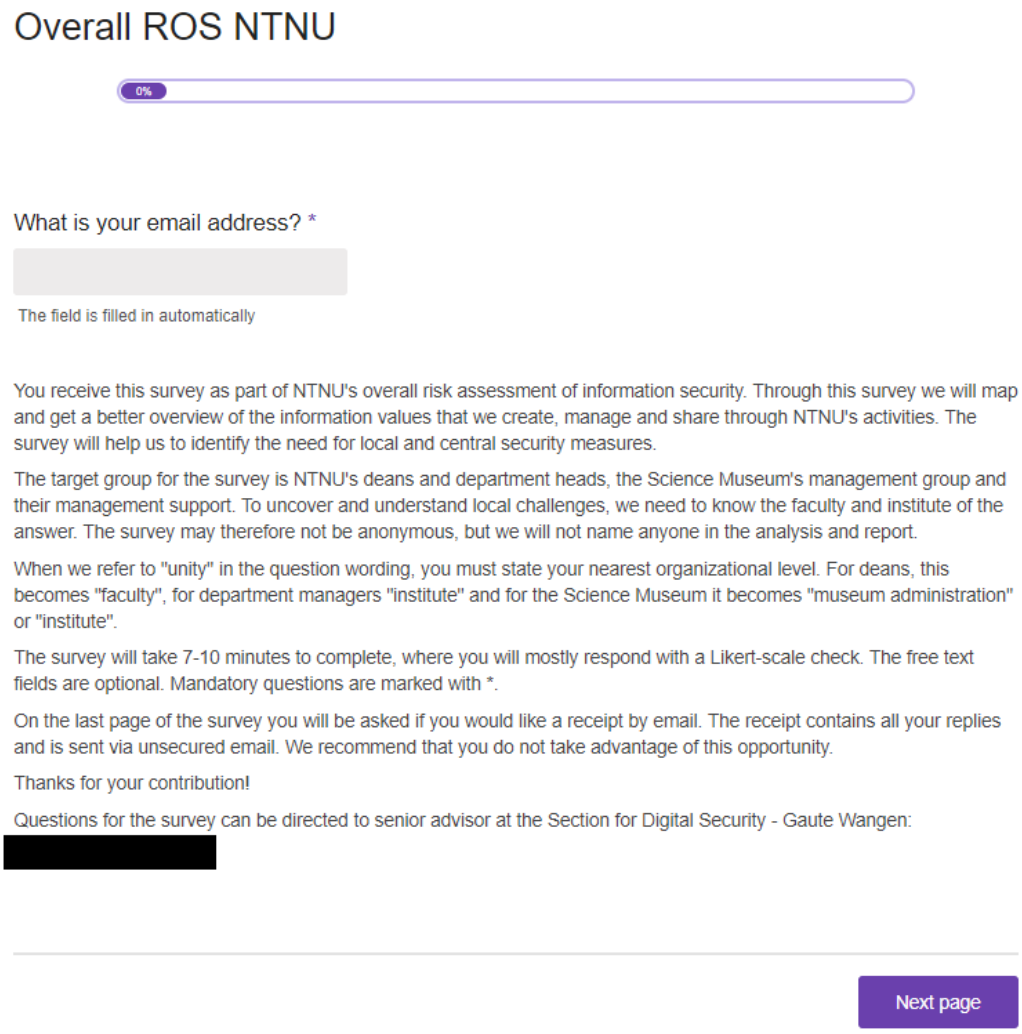
[53] Gaute Wangen, 'Threat assessment of cyber security at NTNU', Tech. Rep., 2019.

[54] G. Wangen, E. Ø. Brodin, B. H. Skari and C. Berglind, 'Mørketallsundersøkelsen ved NTNU 2018', nob, *54*, 2019. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2592949 (visited on 30/01/2020).

[55] J. N. Ellestad, M. L. Lilja, A. G. Gustad and E. S. Skuggerud, 'Sikkerhetskultur ved NTNU', nob, 2019. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2617762 (visited on 29/01/2020).

Appendix A

Survey (English- and Norwegian version)



Overall ROS NTNU

0%

What is your email address? *

The field is filled in automatically

You receive this survey as part of NTNU's overall risk assessment of information security. Through this survey we will map and get a better overview of the information values that we create, manage and share through NTNU's activities. The survey will help us to identify the need for local and central security measures.

The target group for the survey is NTNU's deans and department heads, the Science Museum's management group and their management support. To uncover and understand local challenges, we need to know the faculty and institute of the answer. The survey may therefore not be anonymous, but we will not name anyone in the analysis and report.

When we refer to "unity" in the question wording, you must state your nearest organizational level. For deans, this becomes "faculty", for department managers "institute" and for the Science Museum it becomes "museum administration" or "institute".

The survey will take 7-10 minutes to complete, where you will mostly respond with a Likert-scale check. The free text fields are optional. Mandatory questions are marked with *.

On the last page of the survey you will be asked if you would like a receipt by email. The receipt contains all your replies and is sent via unsecured email. We recommend that you do not take advantage of this opportunity.

Thanks for your contribution!

Questions for the survey can be directed to senior advisor at the Section for Digital Security - Gaute Wangen: [redacted]

Next page

Overall ROS NTNU

0%

Information assets and processing of personal data

How important is it to protect the following information assets at your department?

Information value in information security is a collective term that includes both information and associated support assets such as the ICT system.

By unit is meant: Dean / management support faculty responds to faculty level, department managers with management support responds to department level

	Do not know	0 - Not relevant	1 - Important	2 - A little important	3 - Important	4 - Very important
Username and password *	○	○	○	○	○	○
E-mails *	○	○	○	○	○	○
Self-produced research data *	○	○	○	○	○	○
Exams *	○	○	○	○	○	○
Lectures *	○	○	○	○	○	○
Research data received from third parties *	○	○	○	○	○	○
Research contracts (with the EU or others) *	○	○	○	○	○	○
health Research *	○	○	○	○	○	○
Intellectual and intellectual work *	○	○	○	○	○	○
Internal meetings *	○	○	○	○	○	○
Personal information (eg student and staff data) *	○	○	○	○	○	○
publications *	○	○	○	○	○	○
Accounting Data *	○	○	○	○	○	○
Sensitive personal information (eg health information and trade union membership) *	○	○	○	○	○	○
Strategies, governing documents and guides *	○	○	○	○	○	○
syllabus *	○	○	○	○	○	○
student papers *	○	○	○	○	○	○
Diploma *	○	○	○	○	○	○
Economy Report *	○	○	○	○	○	○
Other communication via digital media *	○	○	○	○	○	○

Overall ROS NTNU

0%

Digital security risk and areas of concern

Do you consider the risks and threats below as relevant to your department?

	Yes	no	Do not know
Spying from state actors *	○	○	○
Financial losses caused by organized criminal / hacker groups *	○	○	○
Inside problems / unfaithful servant *	○	○	○
Sabotage from activists *	○	○	○
Human error using ICT systems *	○	○	○
Loss of confidential information or personal information *	○	○	○

Organizational areas

To what extent do you agree with the following statement?

	0 - Not relevant / Don't know	1 - Totally disagree	2 - A little disagree	3 - A little agree	4 - Totally agree
There are enough resources on my unit to work on information security *	○	○	○	○	○
My unit has sufficient expertise in the field of privacy *	○	○	○	○	○
My unit has sufficient expertise in information security *	○	○	○	○	○
Employees at my unit are familiar with NTNU's information security management system *	○	○	○	○	○
My unit has discrepancies in information security and privacy as a regular theme in our internal meetings. *	○	○	○	○	○
We receive adequate information security assistance when we request it *	○	○	○	○	○

What do you think is the biggest challenge in regards to information security?

Last page

Next page

Overordnet ROS NTNU

0 %

Hva er din e-postadresse? *

Feltet er automatisk utfylt

Du mottar denne spørreundersøkelsen som en del av NTNUs overordnede risikovurdering av informasjonssikkerheten. Gjennom denne undersøkelsen skal vi kartlegge og få bedre oversikt over informasjonsverdiene som vi skaper, forvalter og deler gjennom NTNUs virksomhet. Kartleggingen vil hjelpe oss med å avdekke behov for lokale og sentrale sikringstiltak.

Målgruppen for undersøkelsen er NTNUs dekaner og instituttledere, Vitenskapsmuseets ledergruppe og deres lederstøtte. For å avdekke og forstå lokale utfordringer er vi avhengige av å vite fakultet og institutt på besvarelsen. Spørreundersøkelsen kan derfor ikke være anonym, men vi vil ikke navgi noen i analyse og rapport.

Når vi referer til "enhet" i spørsmålsformuleringene, skal du oppgi ditt nærmeste organisasjonsnivå. For dekaner blir dette "fakultet", for instituttledere "institutt" og for Vitenskapsmuseet blir det "Museumsadministrasjonen" eller "institutt".

Undersøkelsen vil ta 7-10 minutter å gjennomføre hvor du for det meste skal svare med avkrysning på Likert-skala. Fritekstfeltene er valgfrie. Obligatoriske spørsmål er merket med *.

På siste siden av undersøkelsen blir du spurt om du ønsker kvittering på epost. Kvitteringen inneholder alle svarene dine og sendes via usikret epost. Vi anbefaler at du ikke benytter deg av denne muligheten.

Takk for ditt bidrag!

Spørsmål til undersøkelsen kan rettes til seniorrådgiver ved Seksjon for Digital sikkerhet – Gaute Wangen: [redacted]

Neste side

Overordnet ROS NTNU

33 %

Informasjonsverdier og behandling av personopplysninger

Hvor viktig er det å beskytte følgende informasjonsverdier ved din enhet?

Informasjonsverdi i informasjonssikkerhet er et samlebegrep som inkluderer både informasjon og tilhørende støtteverdier som IKT-system.

Med enhet menes: Dekaner/lederstøtte fakultet svarer for fakultetsnivå, instituttledere med lederstøtte svarer for instituttnivå

	Vet ikke	0 - Ikke relevant	1 - Uviktig	2 - Litt viktig	3 - Viktig	4 - Svært viktig
Brukernavn og passord *	○	○	○	○	○	○
E-poster *	○	○	○	○	○	○
Egenproduserte forskningsdata *	○	○	○	○	○	○
Eksamensoppgaver *	○	○	○	○	○	○
Forelesninger *	○	○	○	○	○	○
Forskningsdata mottatt fra tredjeparter *	○	○	○	○	○	○
Forskningskontrakter (med EU eller andre) *	○	○	○	○	○	○
Helseforskning *	○	○	○	○	○	○
Intellektuelt arbeid og åndsverk *	○	○	○	○	○	○
Interne møtereferater *	○	○	○	○	○	○
Personopplysninger (f.eks. student- og personaldata) *	○	○	○	○	○	○
Publikasjoner *	○	○	○	○	○	○
Regnskapsdata *	○	○	○	○	○	○
Sensitive personopplysninger (f.eks. helseopplysninger og fagforeningsmedlemskap) *	○	○	○	○	○	○
Strategier, styrende dokumenter og føringer *	○	○	○	○	○	○
Studieplan *	○	○	○	○	○	○
Studentoppgaver *	○	○	○	○	○	○
Vitnemål *	○	○	○	○	○	○
Økonomirapporter *	○	○	○	○	○	○
Annen kommunikasjon via digitale medier *	○	○	○	○	○	○

Overordnet ROS NTNU

67 %

Digital sikkerhetsrisiko og bekymringsområder

Vurderer du risikoene og truslene under som aktuelle for din enhet?

	Ja	Nei	Vet ikke
Spionasje fra statlige aktører *	○	○	○
Økonomiske tap forårsaket av organiserte kriminelle / hackergrupper *	○	○	○
Innsideproblematikk / utro tjener *	○	○	○
Sabotasje fra aktivister *	○	○	○
Menneskelig feil ved bruk av IKT systemer *	○	○	○
Fortrolig informasjon eller personopplysninger på avveie *	○	○	○

Organisatoriske områder

Hvor enig er du i følgende utsagn?

	0 - Ikke relevant / Vet ikke	1 - Helt uenig	2 - Litt uenig	3 - Litt enig	4 - Helt enig
Det er tilstrekkelig med ressurser på min enhet til å arbeide med informasjonssikkerhet *	○	○	○	○	○
Min enhet har tilstrekkelig kompetanse innen innen personvern *	○	○	○	○	○
Min enhet har tilstrekkelig kompetanse innen informasjonsjonssikkerhet *	○	○	○	○	○
Ansatte ved min enhet er kjent med NTNU sitt styringssystem for informasjonssikkerhet *	○	○	○	○	○
Min enhet har avvik informasjonssikkerhet og personvern som et fast tema i våre interne møter. *	○	○	○	○	○
Vi får tilstrekkelig hjelp med informasjonssikkerhet når vi etterspør det *	○	○	○	○	○

Hva tenker du er de største utfordringene innen informasjonssikkerhet?

Forrige side

Neste side

Appendix B

Interview guide (English- and Norwegian version)

Spring 2020 – Joachim Ulven – NTNU, MIS

Interview of NTNU employee
Who: _____

Intro:

Hi, thank you very much for the opportunity to participate in this interview.

The interview will take the form as structured conversation, with a duration of 45 minutes. The interview intends to collect data for my master's thesis, titled:

"High level information security risk in higher education"

NTNU has fire core assignments that are written in the strategy. These core tasks include research, education, innovation, and dissemination and communication.

The goal of my master's thesis is to gain insight into various information security risks that threatens the strategic levels at NTNU. You have been invited basis of your unique insight (into one or more of the 4 core tasks) in NTNU.

We will mainly seek to identify priority activities and information assets that are linked to your work at NTNU and identify the extent to which current digital threats these. The maste thesis will also be a supplement to extensive risk assessment of NTNU conducted by the Digital Security section later this year. This conversation will also provide an opportunity to provide feedback on general information security done at NTNU.

There is desirable to conduct audio recordings of this interview to ensure quality of transcription, which will be sent to you for approval with notes. The audio recording will be deleted after your approval.

Do you approve of audio recording in this interview?

Do you have any questions?

Spring 2020 – Joachim Ulven – NTNU, MIS

Identifying information assets:

1. Is there any data or information that you manage that needs to be protected?

Information security threats:

I have identified several threat agents and risk present to academic institutions and higher education from cyber space. We are going to talk which extent perceive these threats and scenarios as a risk to your department.

2. Spying and obtaining information by foreign states is a real threat. They have great capabilities and have ambitions to stealing research data, intellectual property or use NTNU's resources.
To what extent do you perceive espionage by the state actor as a risk to your department??

3. We see an increase in organized criminal hacker groups using methods such as blackmail and theft to acquire large sums of money from universities and colleges. Popular methods are, for example, stealing valuable and confidential information or installing malware such as ransomware.
To what extent do you perceive organized criminal/hacker groups as a risk of causing financial loss to your department?

4. NTNU works hard to be a competitive university, with many attractive projects from the business community. This can also open the risk of inside problems, unfaithful servants and industrial espionage.
To what extent do you perceive insiders to be a risk at your department?

5. We also have chaotic actors who usually consist of activists who want to exploit or sabotage NTNU's resources for their own benefit.
To what extent do you perceive that sabotage by activists is a risk to your department?

Internal risk:

6. Human error and lack of competence when using IT systems can have major consequences. This can lead to changes or loss of valuable and confidential information.
To what extent do you perceive that human error and lack of expertise in ICT systems is a risk at your department?

7. Storage and distribution of personal data must be done correctly. Legislation such as the GDPR may impose fines for processing personal data done incorrectly. As well, trust and reputation failure can be a consequence.
To what extent do you perceive insufficient storage and distribution of personal data as a risk at your department?

Vulnerabilities (security challenges)

8. To what extent do you find that you have sufficient resources in your department to work on information security?

9. To what extent do you feel that your department has sufficient expertise in privacy?

10. To what extent do you feel that your department has sufficient information security expertise?

11. To what extent do you perceive that personnel in your department are familiar with NTNU's information security management system?

12. To what extent do you feel your department has information security and privacy as a regular theme in their internal meetings?

13. To what extent do you receive sufficient information security information when they request it?

14. What would you perceive as the biggest vulnerability or information security challenge at your department?

The interview is now over. Thank you for your participation.

Vår 2020 – Joachim Ulven – NTNU, MIS

Intervju av NTNU ansatte
Hvem: _____

Intro:

Hei, mange takk for muligheten du har til å delta på dette intervjuet.

Intervjuet vil ha form som en strukturert samtale, med en varighet på ca 45 minutter. Intervjuet har til hensikt å samle inn data til en master oppgave, som har tittelen:
«Higher level information security risk in higher education"

NTNU har fire kjerneoppgaver som blir beskrevet i strategiene. Disse kjerneoppgavene er forskning, utdanning, innovasjon og nyskapning, samt formidling og kommunikasjon.
Målet med min master oppgave er å få innsikt i ulike informasjonssikkerhets risikoer som truer det strategiske nivået på NTNU. Du har dermed blitt inviterte på bakgrunn av din unike innsikt (innfor én eller flere av de 4 kjerneoppgavene) i NTNU.

Gjennom samtalen vil vi i hovedsak søke å identifisere prioriterte aktiviteter og informasjonsverdier som er knyttet til ditt arbeid på NTNU og identifisere i hvilken grad dagens digitale trusler er en risiko for disse. Master oppgaver vil også være et supplement til den overordnede ROS analysen som seksjonen for digital sikkerhet vil gjennomføre senere i år. Denne samtalen vil også gi mulighet til å gi tilbakemelding om det generelle informasjonssikkerhets arbeidet som gjøres på NTNU.

Det er et ønske å gjennomføre lydopptak av dette intervjuet for å kvalitetssikre en transkripsjon, som vil videre bli sendt til deg for godkjenning med intervjutakers notater. Etter å ha sendt og fått godkjent transkripsjonen av deg vil lydopptaket bli slettet.
Godkjenner du gjennomføring av lydopptak i dette intervjuet?

Har du noen spørsmål?

Vår 2020 – Joachim Ulven – NTNU, MIS

Identifisere informasjons verdier:

1. Er det data eller informasjon som du administrerer som må beskyttes? Har du noen eksempler?

Informasjonssikkerhets trusler:

Jeg har identifisert ulike trussel-aktører og risikoer mot akademiske institutter og høyre utdanning fra det digitale rom. Vi skal snakke i hvilken grad disse aktørene og ulike scenarioer er en risiko mot din avdeling.

2. Spionasje og informasjonsinnhenting fra fremmede stater er en reell trussel. De har stor kapabilitet og har mål om å stjele forsknings data, åndsverk og bruke NTNU sine ressurser.
I hvilken grad oppfatter du at spionasje fra statelig aktør er en risiko mot din avdeling?

3. Vi ser en økning av organiserte kriminelle hackergrupper som bruker metoder som utpresning og tyveri for å tilegne seg store pengesummer fra universiteter og høgskoler. Populær metoder er f.eks stjeler verdifull- og fortrolig informasjon eller installere såkalte «løsepengevirus».
I hvilken grad oppfatter du at organiserte kriminelle hackergrupper er en risiko for å forårsake økonomisk tap i din avdeling?

4. NTNU jobb hardt for å være en konkurranse dyktig universitet, med mange attraktive prosjektet fra næringslivet. Dette kan også åpne risikoen for innsideproblematikk, utro tjenere og industrispionasje.
I hvilken grad oppfatter du at innsidere er en risiko mot din avdeling?

5. Vi har også kaotiske aktører som gjerne består av aktivister som ønsker å utnytte eller sabotere NTNU sine ressurser til egen vinning.
I hvilken grad oppfatter du at sabotasje fra aktivister er en risiko mot din avdeling?

Risikoer internt i avdelingen:

6. Menneskelig feil og manglende kompetanse ved bruk av IT-systemer kan få store konsekvenser. Det kan føre til endring eller tap av verdifull- og fortrolig informasjon.
I hvilken grad oppfatter du at menneskelig feil og manglende kompetanse på IKT-systemer er en risiko mot din avdeling?

7. Lagring og distribuering av personopplysninger må gjøres på korrekt vis. Lovverk som GDPR kan utgi bøtter om behandling av personopplysninger gjøres på ukorrekt vis. Samt, kan tillit og omdømmesvikt være en konsekvens.
I hvilken grad oppfatter du at ufullstendig lagring og distribuering av personopplysninger er en risiko mot din avdeling?

Sårbarheter(sikkerhetsutfordringer)

8. I hvilken grad opplever du at du har tilstrekkelig ressurser i din avdeling til å jobbe med informasjonssikkerhet.

9. I hvilken grad opplever du at din avdeling har tilstrekkelig kompetanse innen personvern.

10. I hvilken grad opplever du at din avdeling har tilstrekkelig kompetanse innen informasjonssikkerhet.

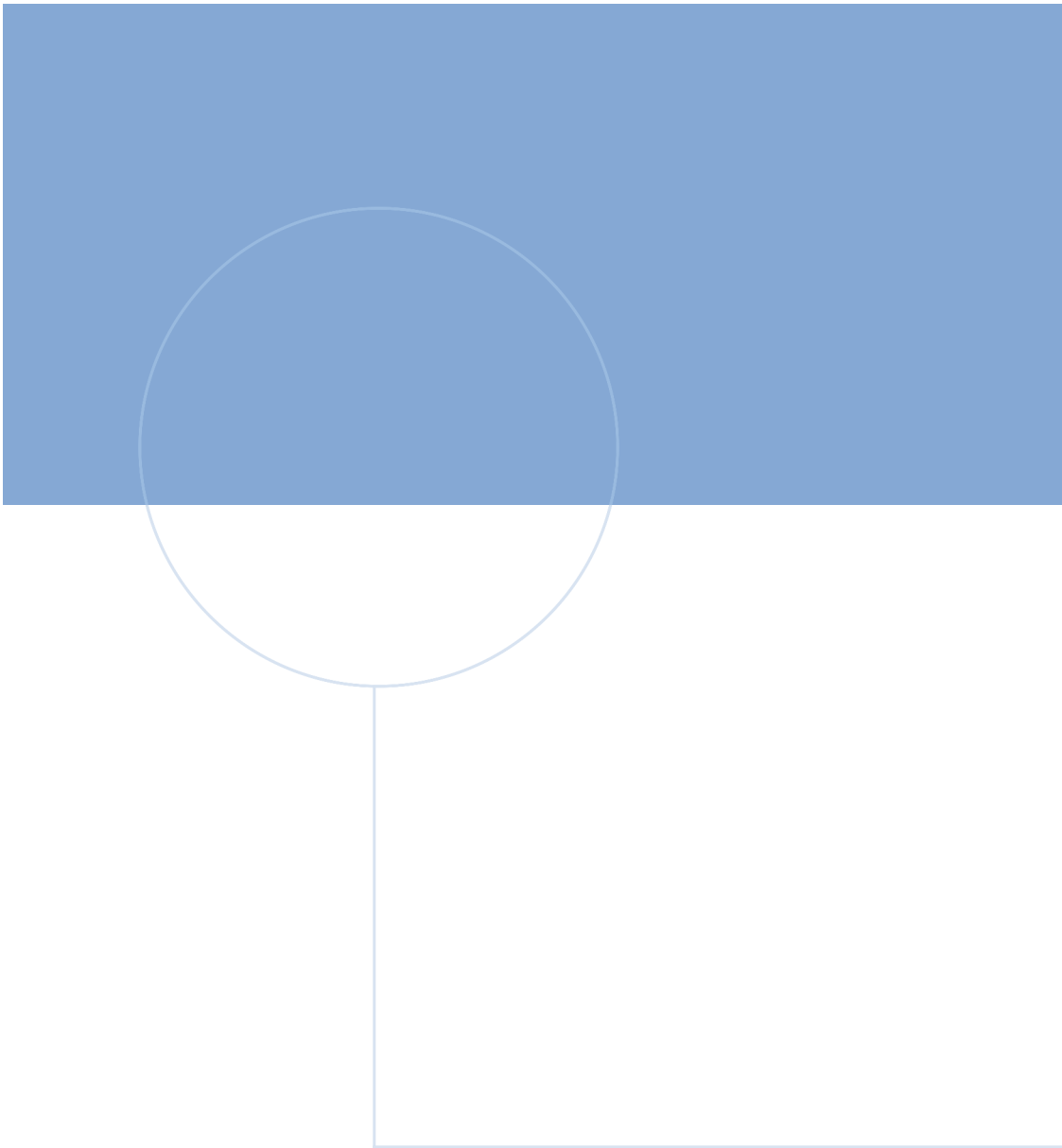
11. I hvilken grad oppfatter du at personell i din avdeling har kjennskap til NTNU sitt styringssystem for informasjonssikkerhet.

12. I hvilken grad opplever du din avdeling har informasjonssikkerhet og personvern som fast tema i deres interne møter.

13. I hvilken grad mener du NTNU får tilstrekkelig hjelp om informasjonssikkerhets når de etterspør det.

14. Hva vil du anse som de største sårbarhetene eller informasjonssikkerhetsutfordringene i din avdeling?

Da er intervjuet over. Takk for din deltakelse.



NTNU

Norwegian University of
Science and Technology