Universitetet
i Stavanger

FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study programme/specialisation:

Offshore Technology:
Industrial Asset Management

Spring / ~~Autumn~~ semester, 20.17..

Open/~~Confidential~~

Author:
Fritzvold, Einar

…………………………………………
(signature of author)

Programme coordinator: Professor Jayantha Prasanna Liyanage, PhD

Supervisor(s): Faculty Supervisor: Professor Jayantha Prasanna Liyanage, PhD
External: Martin Guy Williams, EY

Title of master's thesis:

Cyber Security in Organizations

Credits: 30 credits

Keywords:
Cyber Security, risk, digital risk, digitalization, digital systems, cyber threat, cyber actors, risk management, asset management, critical functions, sensitive information, supervisory authorities, connectivity, dependency.

Number of pages: ……164……

+ supplemental material/other: …4……

Stavanger,…10.06.2017………
date/year

Cyber Security in Organizations

By

Einar Fritzvold

A Thesis

Presented to the Faculty of Science and Technology

University of Stavanger

In fulfillment of the Requirements for the degree of

Master of Science

(MSc)

University of Stavanger
Faculty of Science and Technology
-2017-

Abstract

The cyber threat towards digital systems and organizations are increasing. WannaCry is one of the latest large-scale cyberattacks which has had a global impact. The digitalization is transforming organizations to innovate and utilize new digital technology and infrastructure. This is raising the connectivity and dependency on digital systems. Organizations, authorities, individuals, and operations are susceptible to cyber risk. Threat actors are becoming more organized, sophisticated, and cyber-crime has been commercialized. Easy access to malicious tools is one of the drivers for the increased threat. Organizations must know how to face this new cyber threat and understand how it affects their systems and operations.

The purpose of this thesis is to compare cyber security solutions and capabilities of three different organizations in the Norway. The main objective is to find industry similarities, key issues and challenges related to cyber security, and find areas of improvement. The method for this thesis is a qualitative analysis. The data is acquired through an interview process. The interview is based on a semi-structured interview guide. Three organizations from different Norwegian industries have been interviewed – Railway, Health Care, and Power Distribution.

The thesis discovers that there are many similarities in the industry solutions, and that there are challenges related to innovation vs security, security assurance and control of ICT service providers, location of ICT service providers, how change in technology also means organizational change, and that there are ambiguities in the legislations which does not ensure quality in cyber security activities. The organizations' strengths are emergency response. The general improvement areas of the three organizations are ensuring that the organization has an updated threat picture and understands how internal factors affects the cyber risk exposure, and the development of measurable security requirements and targets. Additionally, individual improvement areas have been described for each organization.

There is a need for ICT and cyber security in education to raise the cyber security competence, as well as, bridge between traditional engineering and ICT professions to ensure a common risk language and understanding of cyber risk. There are many benefits in collaborative efforts between organizations and CERTs. Information- and experience-sharing helps create a front against the threat actors and increases the general industry security culture. Management decisions has a large impact on cyber risk exposure. Cyber risk understanding is critical for minimizing the effect of managerial decisions. The supervisory authorities must increase their industry engagement and communication efforts to ensure that a high level of cyber security capabilities are implemented in their given industrial sector. Organizations must evolve with the growing threat and the new innovative solutions. Security measures should not be implemented out of compliance, but out of self-interest. Security is a premise for a successful and sustainable future.

Acknowledgements

This thesis has been completed during period from January to June 2017. It has been a challenge and a great learning experience. Learning is not always pretty, as this thesis has proven with its ups and downs. Yet, the thesis has provided me with experiences and knowledge that I could not obtained elsewhere or in a different matter. It is truly a great feeling completing this thesis.

I would like to thank my faculty supervisor Professor Jayantha Prasanna Liyanage for helping me with the structure of the thesis and given me motivation. I would like to thank the interview participants for taking the time and effort to participate in this thesis; Lars Erik Baugstø-Hartvigsen, Helse Vest IKT, Arild Nybrodahl, Bane Nor, Lars Strømmen, Bane Nor, and Jon Andreas Pretorius, Hafslund Nett.

I would also like to thank my peers, Mats Tronstad Gulliksen and Helge Nordal, for support and great teamwork during this study program.

Einar Fritzvold, 09.06.2017, Stavanger.

Contents

Table of Figures

List of Tables

Abbreviations

ICT – Information and Communication Technology

IT – Information technology

SCADA - Supervisory Control and Data Acquisition

ICS – Industrial control systems

NSM – Nasjonal Sikkerhetsmyndighet - National Security Authority

PST – Politiets Sikkerhetstjeneste - Police Security Service

E-tjenesten – Etterretningstjenesten - Norwegian Intelligence Service

RAMS – Reliabilty, availliability, maintainability, and security

NVE – Norges vannkraft og Energidirektorat - Norway's Hydro Power and Energy Directorate

IDS- Intrusion detection system

OT – Operational Technology

Chapter 1 - Introduction

1.1 Background

Wanna Decryptor, or WannaCry, is the name of the ransomware that roamed during May 2017. NSM states that it is the largest cyberattack they have seen at a global level (Omland and Wernersen, 2017). It utilizes an exploit in Windows, a commonly used operating system, and has attacked approximately 57 000 users in 99 countries (Omland and Wernersen, 2017). Among the victims were Norwegian hotels, British health care services, Russian government, and a French car manufacturer. The virus originates from the increasing threat from cybercrime. Along with other digital threats, these are one of the concerns of modern organization.

The digitalization has led to social change and changed the way organizations control processes, complex operations and infrastructure. It allows us to make use of a wide range of new services, such as cashless trade and financial services on mobile, real-time monitoring and data streams. It has led to effective automated and data-driven industries, and new ways of connecting suppliers, products and customers through ICT. This change has caused a growing interconnectivity and dependency on digital systems and networks. In the wake of the digital transformation, the threats have been growing and malicious actors have found new ways of causing harm to organizations and individuals. Large actors, such as nations, have developed a new type of warfare that has great potential for causing major consequences by attacking critical infrastructures. Criminals, hackers, and activist have new platforms for conducting criminal acts to individuals and organizations.

Sensitive information, high risk operations, critical infrastructure and government functions are values that are important to protect to maintain privacy, democracy, and safety. This means that organizations and governments must be aware of the vulnerabilities of their own operations and find a way to protect their values and assets. Cyber security considerations should be made in relation to risk and vulnerability analyses, human resource management, technological development, and installation, operation, and maintenance. Technical systems become complex, and the use of production networks, communication networks and the internet of things causes many systems to be interconnected. This may cause unidentified exposures and weak points. Increased interdependence and expectation to availability increases with the need for continuity and reliability in operations.

Lysneutvalget (DNV GL, 2015) created a basis for cyber security awareness, and pointed out a few weaknesses in the Oil & Gas industry in Norway. There has also been a focus on cyber related incident/emergency response from authorities, such as NSM. Incident response plans, routines, exercises should create an indication on how prepared organizations are for critical incidents and situations. Leadership and management roles must change to include cyber security at an organizational level. A new mindset related to vulnerabilities and exposure in digitalization and development, including value chains and business models, must be acquired. An organization should strive for having an overview of increasingly complex and interwoven systems.

1.2 Problem Definition

Cyber security is a perspective on information security risk that focuses on addressing the types of attack that have the potential to cause large-scale harm. Such attacks can have serious consequences, not just economically and reputationally, but also on an organization's reliability and the safety and wellbeing of its people, as well as the environment. Cyberattacks are highly sophisticated in nature and multi-faceted in that they typically exploit weaknesses in organizational, technical and physical aspects of an organization at the same time.

Public and private organizations rely on smart digital technology and interconnected systems is more vulnerable than analogue solutions. Modern organizations should be able to develop cyber security capabilities to respond to the new cyber threat. Organizations must know how their role (critical function, assets, sensitive information) affects their cyber risk exposure, how to incorporate cyber security into their strategy, how to actively manage cyber risk, and how use innovative technology without compromising cyber security, or vice versa.

1.3 Aim of Thesis

The purpose of this thesis is to present an insight to cyber security solutions of Norwegian organizations. The thesis will compare the three organizations' cyber security solutions from three different industries, and highlight the similarities, key issues and challenges. Additionally, the organizations' cyber security capabilities will be compared to cyber security practices and recommendations, and the thesis will highlight the organizations' areas of improvement. The analysis will include three Norwegian organizations from three different industrial sectors – Health Care, Railway, and Power distribution.

Two models will be provided for the analysis – a vulnerability model, the foundation for the interview questions and the comparison of industry cyber security solutions – and a cyber security capability model for the evaluation of the organizations' cyber security capabilities.

1.4 Scope of Work and Objectives

To understand the risks and vulnerabilities in digital systems, the thesis starts at the drivers and impact of digitalization. Further, it connects the challenges of digitalization to the risks of digital systems and connectivity. Then, the thesis presents the importance of cyber security in digital systems and how to reduce the risks by implementing cyber security. The thesis provides practical examples to the relevant topics to make the issues and principles more understandable. Moreover, the thesis performs an analysis. The objectives can be divided into:

- Describe the drivers, impact and challenges of digitalization and provide suitable practical examples.
- Describe what role risk plays in digital systems and connectivity, provide examples of incidents, and describe the different aspects of vulnerability in organizations.

- Explain the relevance and importance of cyber security, and identify best practices and emergency response procedures.
- Combine the vulnerabilities and make a vulnerability model based on the human, organizational and technological (HOT) perspective.
- Combine the cyber security practices and recommendations and make a Cyber Security Capability model based on the HOT perspective.
- Develop an interview guide and choose three organizations for the interview.
- Perform the interview process.
- Perform analysis. Part one - compare the three organizations to each other and find similarities in industry solutions, key issues and challenges. Part Two - compare the organizations' cyber security capabilities and find areas of improvement.

1.5 Methodology

The thesis is based on academic literature, industry whitepapers, surveys, various publications, and the information provided through the interview process. This thesis follows the qualitative method with the use of a semi-structured interview guide. This method was chosen because it facilitates a conversation on the topic. It enables the interviewees to share opinions, information and explanations in a better way than via a questionnaire. This is beneficial to make the interviews a free-flowing conversation, where the interviewer can focus on asking follow-up questions and not be hindered by the structure of a questionnaire. The interview guide is based on the HOT Vulnerability Model, found in chapter 5.2.2, and additional questions about cyberattacks and the future of digitalization. The interviews were conducted via skype in Norwegian. All the interviews were audio recorded and the participants agreed to the recording. The recording makes the data available for later use and analysis for the researcher. The interviewees were sent the questions beforehand to prepare answers and gather information. They were also given the opportunity to evaluate if there were some questions that they did not want to answer due to privacy or other concerns.

Delimitations

The interview approach means that the answers are edited by the researcher in order to be presented in a systematic way and that the answers were interpreted. The qualitative method may cause results that are difficult to compare and need interpretation. The interviewed organizations share similarities in that they all use digital systems, networks, databases, and are exposed to cyber threats, but their operations and organization are different. The analysis is limited by the current level of understanding of the area. Some of the topics are difficult to gather sufficient data to present a representative answer. The study is limited by the secret nature of the topic. Organization will not admit weaknesses in security measure and do not want to share information that can be used to expose vulnerabilities in their organizations. In most cases, the organization are willing to share procedures and information regarding the topic, but the actual evaluation of the state of the technical system and vulnerabilities are secret. The study takes a broad approach to the topic. The topic could be limited to increase accuracy and technological depth. There can be a mismatch between the interview answers, the comparison models, because of the semi-structured interview and the secrecy involved in security measures. The HOT Cyber Security Capability Model is not an ISO certification, but a guide to incorporate the HOT perspective.

1.6 Thesis Structure

The thesis is divided in to eight chapters with a literature study and an interview part. The structure of this thesis is as follows:

1. **Introduction**
   - Presents the background for the study
   - Aim of thesis
   - Scope of work
   - Description of methodology.
2. **Digitalization**
   - Drivers for digitalization
   - Impact of digitalization
   - Practical examples
   - Challenges of digitalization
3. **Digital Risk**
   - How risk connects to digitalization
   - Description of digital risk and threat agents
   - Example of incidents and exposure
   - Description of vulnerabilities in organizations
4. **Cyber security**
   - How cyber security links to risk and digitalization, and why it is important
   - A presentation of cyber security best practices
   - A presentation of incident response management
5. **Analysis**
   - Analysis background, structure and approach
   - Description of the two models – HOT Vulnerability Model and HOT Cyber Security Model
   - Short introduction to the three organizations
   - Analysis part 1: compare the three organizations to each other and find similarities in industry solutions, key issues and challenges.
   - Analysis part 2: compare the organizations' cyber security capabilities and find areas of improvement.
6. **Discussions**
   - Discussion of the Analysis
   - Discussion of the Results
7. **Reflections**
   - Reflections of Scope of work and Objectives
   - Challenges encountered
   - Areas for further studies
8. **Conclusion**

Chapter 2 - Digitalization

2.1 Drivers for Digitalization

Digitalization is to utilize digital technology and tools to replace or streamline manual/physical tasks, and use it to produce products or services (Bratbergsengen, 2016). This means that organizations apply digital technology to produce products, perform services or operations. This chapter will try to identify why digitalization happens. There are many factors contributing to the transformation. The drivers for digitalization can be identified as technological, political, financial, environmental and social. These are factors that enables and drives the digitalization process and will be described in this chapter.

- Technological drivers

This is technology that provides new opportunities in cost-efficiency, task optimization, quality, or can in some way change the operation, service or manufacturing for the better.

- Political drivers

These are political incentives that allows or encourages the use of new technology, or in some way influences the industry to change. These are regulations, legislations, governmental focus areas and visions.

- Financial drivers

Increased competition from globalization causes organizations to thrive to find new ways to gain competitive advantage. The industries drive towards more effective solutions, better quality, customer satisfaction, and better performances. Any technology, method, or tool that can provide this will used.

- Environmental drivers

Environmental requirements for producing less waste and use less resources such as power and water. These are elements that contributes to the organization's self-interest in using less resources and thus creating better solutions for the environment.

- Social drivers

These are user behavior and demands for availability and reliability of services, products or information. Additionally, efforts made towards a better society and human life.

2.1.1 Technological Drivers

Internet of things

The Internet of Things (IoT) is a system of interconnected computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction (Rouse, 2016).

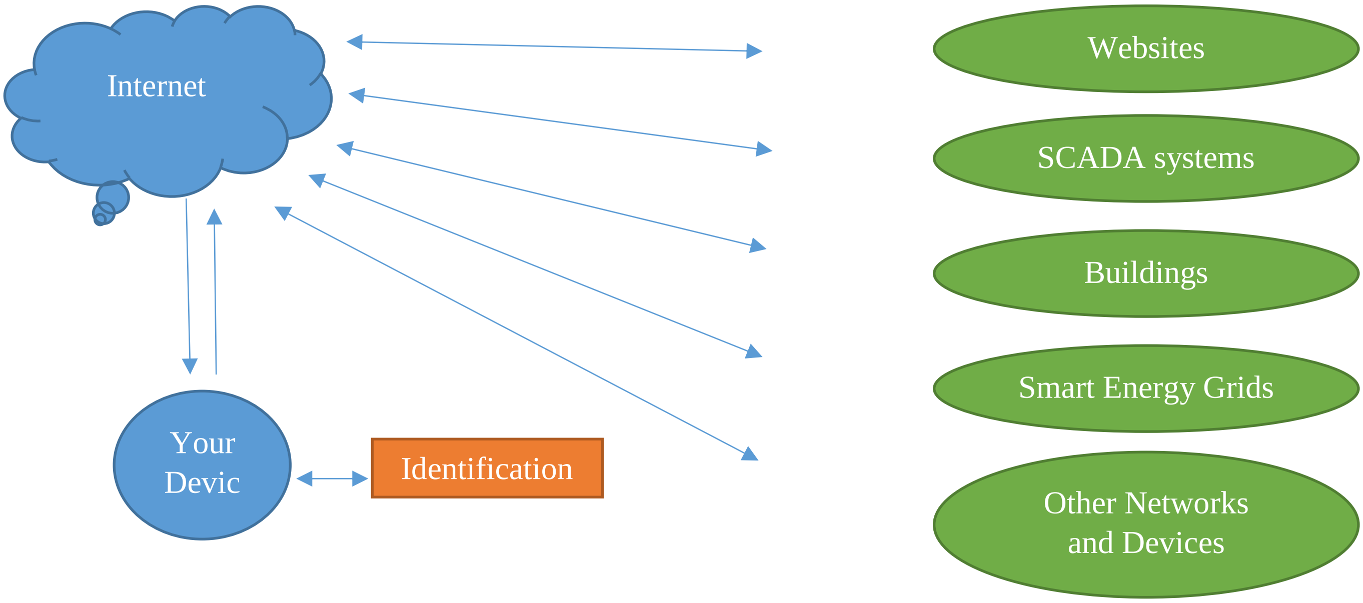


Figure 2.1.1 – Internet of Things

The internet of things is the interconnectivity of physical devices, sensors, electronics, software, actuators, and networks (shown in figure 2.1.1). The easiest "thing" to imagine is the smart phone. It is a combination of sensors, software and electronics, such as camera and gyroscope, and is connected to the internet. It has the theoretical ability to connect to any other device also connected to the internet. This causes a security issue as more and more devices are connected to the internet, such as industrial databases, systems, machines, as well as personal information.

An example of the possibilities of IoT is found in farming. A farmer with a drone and a self-driving tractor has removed the necessity of traditional human intervention (Brown, 2016). The tractor is driven by remote control or an autonomous guidance system. The farmer can control the equipment by using a computer or a table, and monitor the process by viewing the cameras that are attached to the system.

Cloud services and cloud computing

The Norwegian Data Protection Authority (Datatilsynet, 2017) defines cloud computing as "*a collective term of everything from data processing and data storage to software on servers available from remote server parks associated with the internet.*" These are methods to store, process, and manage large amounts of data. There technology provides organizations with potential for increased efficiency and cost savings. The market for cloud services is growing. The challenge with cloud services is that data and information is transferred between nation boarders and it is difficult to guarantee as data is processed and stored outside the business premises (NSM, 2015).

Big data

Big data is the development of data power that enables data collection that allows to assemble and analyze a large information volume quickly or in real time (NSM, 2015). This process is resource-demanding and acquires an infrastructure that enables data availability and integrity (Dvergsdal, 2015). The development of such resources can be both costly and technologically challenging. Artificial intelligence and visualization techniques are a necessity to be able to analyze such large data volumes. Big Data has its uses when looking for trends and patterns. It is very usable in public statistics and tourism, public transportation, and health and infection protection. Telenor (2017) is using mobile phone data to map and visualize the traffic behavior in Oslo. This data can be used to modify and improve the future road network in the area.

Robotic process automation

IBM (2016, page 1) defines robotic process automation (RPA) as "*the automation of a wide range of administrative tasks through specific software algorithms that interact with multiple applications and computer-centric processes, to execute transactional processes at User Interface (UI) level.*" The RPA is perfect for predictable, rule-based, and repetitive processes that requires managing large volumes of data (IBM, 2016). It can be used as a privacy insurance when managing sensitive information, such as patient information, because it removes the human element from the task. The process can operate 24/7 and is not affected by other human factors, such as inaccuracy, errors, the need for breaks and sleep, these are engineered out of the process. The human efforts to be used more purposefully elsewhere. It is a cost-reducing improvement that increases efficiency in organizations. It can outperform employee costs and the outsourced man power from low-cost countries (Gaarder, 2016). The RPA is suited for managing administrative processes, work flow processes, and customer and IT support processes. It can be integrated in any industry where there is a large volume of repetitive and rule-based processes.

A software can be programed to do a simple task such as remembering specific key strokes for a process, reducing the time of executing the process. The second use is in cognitive operations and combines the automation with intelligence. This is explored through IBM's Watson. Watson is a program that manages RPA and analyses input from customer, supplier and employee behavior. It can do this because of its ability to (IBM, 2016):

- Understand natural language, structured and unstructured data.
- Generate and evaluate hypothesis' for better outcomes.
- Adapt and learn from user sensations and responses.

Voice recognition software means that the machine can collect information and structure a response through a RPA answer process (IRPA, 2014). This can be used in call centers, or similar, where there is a predictable and structured way of managing customer issues.

Industry 4.0

Baur and Wee (2017) defines Industry 4.0 "*as the next phase in the digitization of the manufacturing sector, driven by four disruptions:*

- *the astonishing rise in data volumes, computational power, and connectivity, especially new low-power wide-area networks;*
- *the emergence of analytics and business-intelligence capabilities;*
- *new forms of human-machine interaction such as touch interfaces and augmented-reality systems;*
- *and improvements in transferring digital instructions to the physical world, such as advanced robotics and 3-D printing."*

Improve productivity by using data from processes and operation systems. The data analysis can highlight weaknesses in a manufacturing process and enables optimal operations. Collecting data from operations, maintenance and organizational performance has a great potential for cost-efficiency. However, it may be difficult to utilize the large streams of information. The traditional manufacturing business model is changing, and new models are emerging. This means that the organizations must identify, acknowledge, and adapt to these new competitive challenges (Baur and Wee, 2017). Digitalization is a process that acquire planning and investments made to the future the organization. The two major challenges of Industry 4.0 is Data management and cyber security ((Baur and Wee, 2017).

2.1.2 Political Drivers

The political or governmental focus to be more effective drives the digital transformation. Removing costs and free resources in public services makes it possible to devote more resources to schools, police force, and health care (Chaffey, 2017). There are arguments for digitalization saying that it will lower public costs, increase profitability, motivate innovation and new ideas (Chaffey, 2017). Additionally, a low-cost and efficient Norwegian industry can outperform international low labor-cost countries, providing an increase in GDP (Sunde, 2017). The Norwegian Police reform is a political incentive to decrease the bureaucracy, use less resources, and become more efficient (Justis- og beredskapsdepartementet, 2013). ICT solutions are a large part of this reform, as there has been deviating practices and ICT-use throughout the police districts. Digitalization of the Norwegian police is believed to improve the overall efficiency and asset utilization.

2.1.3 Financial Drivers

Economic Growth

The digitalization is an opportunity for innovation and economic growth. New technology evokes new business models, business networking, and the transfer of knowledge and access to international markets. Digital trends such as cloud computing, mobile web services, smart grids, and social media, are radically changing the business landscape, reshaping the nature of work, the boundaries of enterprises and the responsibilities of business leaders (European Commission, 2017). It is the prediction of the EU Commission (2017) that businesses will get excluded from the global market if they do not connect digitally. The digital economy has a great potential for creating jobs. Nearly 500 000 new jobs have been created in the USA over the last five years (European Commission, 2017). This means that there is an untapped potential in the EU and the rest of the world to create jobs in the digital economy.

Reducing Cost

A large financial driver is the businesses' ability to reduce cost. New maintenance methods, such as predictive maintenance can greatly reduce the maintenance costs of production systems. Automation and robotics removes the disadvantages of human factors in manufacturing and can introduce 24/7 production. Customer data gathering and analysis are tools that can improve product and service accuracy and customer satisfaction. Businesses are always looking for cost-efficient solutions to gain a competitive advantage.

2.1.4 Environmental Drivers

Government Focus and International Agreements

Protecting the environment is a part of the corporate social responsibility. In the pursuit of lowering costs and increasing resource efficiency, there are also indirect benefits to the environment, such as using less power, water, and produce less waste. The Norwegian government are focusing on reducing the environmental impact of industry, housing and estates, transportation, and other factors. At the same time wanting to make the public sector more efficient. This is visible through the digitization of building and planning processes, and the Municipal reform (Sanner, 2015). International climate agreements play an important part in motivating change and improvement (Klima- og miljødepartementet, 2014).

2.1.5 Social Drivers

Customer Demands

People’s behavior towards technology is changing. Advanced technology is available to individuals and many devices contains personal information and is an integrated part of their lives. Technology makes it possible to have one device with multiple functions, such as portable cassette and cd-players, cameras, and phones. Additionally, people wants to communicate with other people regardless of distance and location. This is a core driver for connectivity in personal devices. Globalization leads to international companies and interaction across borders. As businesses needs to communicate with other businesses in other location, the need for fast and reliable communication and connectivity is created.

People demands available information and reliable devices. This creates new requirements for products and services. Businesses, in their pursuit of market shares and profit, will have to develop their products and services to meet the needs of their customers, both private and professional. New requirements for customer support, health care, transportation, and power & water supply creates a need for smart thinking and development of engineering solutions.

Engineering Out Human Factors

Automation excludes human intervention. This removes the concerns of active human errors and the drawbacks of human factors and increases safety and security. Machines can operate 24/7 and tough manual labor can be automated. The same goes for information processes, where the monotonic process can be automated with the use of software. This is beneficial when managing sensitive information without human intervention. It increases the confidentiality of the information. As human safety and wellbeing is a part of corporate social responsibility, there is always a need for improving work processes and work environment. As stated previously, automation removes the drawbacks of human factors and contributes to increased safety and security of the organization.

2.2.1 Changes to work life

Repetitive and physical demanding jobs disappears along with highly hierarchal structures. Procedures are becoming more flexible and knowledge-based. Communication between levels and across departments causes the organization to achieve a more network-resembling structure. ICT allows for direct communication between employees, levels and geographical spaces.

Introducing computers

Introducing computers and ICT into an organization will affect the work life of the employees. Major structural change will affect the routines, procedures, and interactions of the employees. Some tasks will be integrated into the ICT and the functions of some levels would become unnecessary. Data processing and information technology will make it easier to control and manage the organization, and may cause some of parts of the organization to be decentralized. ICT can be used to develop information systems that will enhance cooperation within a level, making it easier to share information between projects and employees. The use of ICT creates new challenges, for example, the need for education and an environment with new stress factors. At the same time, it enables tools such as CAD, word-processing, video-communication, personal computers, phones, etc.

Replacement of old jobs

Since the development of the microprocessor, the computerization has become personal. Smart-phones and personal computers exists on the work stations of many individuals when they arrive to work. ICT is a part of the personal life and work life for most individuals. The development of the computer and ICT have replaced and changed some of the jobs in the organizations. Automation has become a large part of manufacturing and software is doing a lot of the designing, calculation, and analysis. The work life environment has changed in line with the implementation and development of ICT. The development of the computer has created new jobs and replaced unnecessary jobs. Some workers, during the years of exploring what computers could do, faced the reality that the machines "took over" their jobs. Their expertise was no longer needed and they were given new tasks to do. In the process of implementing new technology which replaces human jobs, the need for "retraining" or "reeducation" of the workless employees emerges. At the same time, the technology creates a need for higher educated employees who can handle the new jobs.

New interactions and routines

As the work place and structure change, the interaction between human-to-human and human-machine changes. The routines of the human individual and teams is affected by the technology. New stress factors are introduced with new technology and they are not easily understood at first. Human factors and ergonomics is a helpful multidisciplinary scientific tool to help understand and deal with stress factors and human-machine interaction. ICT and organization is also subjected to “humanizing”. The following points are based on Bradley’s (2002) list of effects related to the integration of ICT in work life:

1) Transfer and growth of knowledge, power, and influence

The access to knowledge is changing. More knowledge and information is available to more people, different communities, countries, etc. The connection globally is increasing, for example, long distance services, learning, and work is possible. The availability of knowledge has increased and can be accessed by anyone. Because of this, there will be an increased necessity for data security and control in the future, both personal security and organizational security.

2) Work organization and work content

Repetitive and physical demanding jobs disappears along with highly hierarchal structures. Procedures are becoming more flexible and knowledge-based. Communication between levels and across departments causes the organization to achieve a more network-resembling structure. ICT allows for direct communication between employees, levels and geographical spaces.

3) Human communication

The number of available connections increases with ICT. The demand for collaboration increases the quantity of connections with other humans. However, the connection is not necessarily in physical space. Technology is enabling being social without the presence of another human in the room. Typed words may be more frequent than actual conversations. Bradley (2002) states that “electronic solitude”, that is structural loneliness forced on a person, and which exist today, should be prevented in the ICT society or at least combated and counteracted. The social intelligence of the human is important in these ICT communities. The ability to interact in complex social structures, relationships, and environments becomes just as important as education or technical skills.

4) Stress

The ICT causes a fast pace environment for humans. New expectations and demand for availability, speed and accuracy in the work life. Workers can be reached anywhere at any time. Stress will occur when a lot of information is being processed by the human mind which is constantly filtering out “noise” from usable information. Even tough, ICT makes tasks and communication faster, the person may feel that there is not enough time available and “overconnected”. The organizations strive for better and faster technology, which means that the workers can do more at a shorter period of time. A future consideration in relation to ICT, would be to implement “offline-time” where people are not connected and can relax.

5) ICT, education, and learning

The ICT has made it possible for an organization to continuously learn about itself and change things that does not work. People within all levels of an organization have access to knowledge and communication. The availability of knowledge makes it easier for an employee to gather information and learn skills at a fast pace. It also enables continuous learning about work processes, equipment, software, internal organizational change, local and global events, etc. The employee and the organization is always up to date. ICT may change the focus of education. Capabilities like teamwork, coping with demand, problem-solving, computer skills, social communication, multicultural understanding, leadership, creativity, and language skills are needed in a ICT environment (and in the future).

2.2.2 Access to knowledge, information, and technology

Bang and Markeset (2011a) states that the spread of technology and ICT are two of the drivers for globalization. As the world become connected because of trade, lower transportation costs and technology, it becomes more interconnected because of ICT. Forums, groups, websites, and chats makes it possible for people to share information and culture across nationalities and languages. ICT makes it possible to gain access to knowledge, information, and technology across the world via networks. Long distance communication and shared networks makes it possible for a business, organizations, nations, and people to share their knowledge, news, technology, and culture. The access to information can impact the way cultures see other cultures. The access to technology makes it difficult to maintain a competitive advantage in discovering or creating new technology. The time it takes before someone else creates a similar product is shorter than before. Businesses experiences increased competition from international actors because of globalization and outsourcing (Bang and Markeset, 2011a). This changes how corporations think about rivalry, substitutes, suppliers, customers, and new entrants as markets become international. The access to knowledge, information, and technology has changed. More knowledge and information is available to more people, different communities, countries, etc. The connection globally is increasing, for example by long distance- services, learning, and work. The availability of information has increased and can be accessed by anyone. This requires data security, control and reliable systems.

2.2.3 Business models

Collecting User Data

New technology gives businesses the opportunity to get more personal than before with the use of applications for the smart phone. These application makes it possible to distribute information directly to the customer, as well as gather information about the customer's behavior, interests, and location. The number of users is vital for the success of these application. Social platforms such as Facebook, Instagram, and Snapchat utilizes a free-to-use model, which makes is easy to gain users and distribute their product. The business model is dependent on income from advertising (Ovide, 2017). Websites gather information from users. This kind of information can be used to tailor advertising and increase the accuracy of the advertising (WebWise team, 2012). This new way of collecting data requires regulations for secure data management and needs to be managed privacy in mind.

Peer-to-Peer Services

Uber, Air BnB, BitTorrent, and Ebay are so called peer-to-peer service (Inverstorpedia, n.d.). Uber has created a taxi-service based on user participation. Anyone can become a driver and the driver is connected to the customers through the application. This is a part of the new share economy which is possible through the development of ICT and smart phones. People can share cars, houses, tools, equipment they do not use and make money on it (PWC, 2015). This is a creative way of doing business in a way that seem beneficial for all the participants. And it allows for people to gain some extra income by the accessibility of ICT. These new business models can cause problems in policies and regulations. The evolution in share economy have created a need for new policies and regulation to make them more trustworthy and make them operate in a legitimate zone.

Fragmentation and complex supply chains

Globalization has given opportunities for offshoring and outsourcing, and it is successfully achieved though technological development in ICT among other drivers (Bang and Markeset, 2011a ;2011b). Bang and Markeset (2011b) states that fragmented value chains, or vertical disintegration, leads to more specialization on individual tasks. Fragmented value chains make the organizations able to focus on the core operation, while outsourcing parts of the value chain to other companies. This means that there are service businesses which specializes on a task or function. In a competitive market, outsourcing may prove to be more cost-efficient. This concept leads to complex supply chains where many companies are involved in one large operation. This is where new technology contributes to minimize the location difference with tools such as cloud computing and video communication. The competition speeds up, as more companies enter the market as suppliers, buyers, substitutes, new entrants, or industry competitors, creating a need for a competitive edge and low-cost productions (Bang and Markeset 2011b).

Changing Organizations

Google says that digitalization can become so comprehensive that is can sink some of the largest companies in Norway (Sivertsen and Sommer, 2017). Digitalization provides new business solutions and work methods in medicine, retail, advertising, transport, etc. The companies need to change and adapt to the increased competition from other companies with digital solutions, or they may not exist in ten years. Machine learning, artificial intelligence, advanced analysis technologies, and 3D printing changes industry production and operation (Sivertsen and Sommer, 2017). This impacts the competitive advantage of the businesses and competition at a global level.

2.2.4 Productivity, efficiency, and SMART systems

The internet of things and connectivity gives an opportunity for greater efficiency and productivity. The digitalization of the industry integrates cyber-physical production systems. A smart system uses a feedback loop of data, which provides evidence for informed decision-making (The Royal Academy of Engineering, 2012). This means that decisions can be based on system data and input, monitoring of operations can happen in real-time, infrastructure and systems can adjust to changes in the environment. ICT and smart automation connect and enable the integration of embedded production systems and processes, creating intelligent, object-oriented networking, moving from centralized to decentralized models, and evolving into cyber-physical design and simulation by using models and intelligent software (Hoske, 2014). This can be used to improve safety, efficiency, cost, and control while monitoring and controlling production- and operation systems. The Royal Academy of Engineering (2012) presents three different types of smart systems:

- collect usage and performance data to help design or improve efficiency in the system
- collect data, process them and present information to help a human operator to take decisions
- use collected data to act without human intervention

Smart Engineering: Operational Technology and Integrated Operations

According to Gartner IT glossary (2017): *Operational technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise*. This includes systems such as manufacturing execution systems (MES) and SCADA. Operational technology enables companies to have control over complex operations, gather data from production, and monitor production and transport over long distances. Integrated operation is a multi-disciplined operation which is enabled by ICT. Industrial control systems (ICS) and ICT is connected via fiber optic cables and networks to enable real-time monitoring and control. It is used in the petroleum industry to ensure safe production and lower cost. The combination of IT and ICS enables this great opportunity to have greater control of operations and processes. In figure 2.2.3 explains the difference in IT and OT.

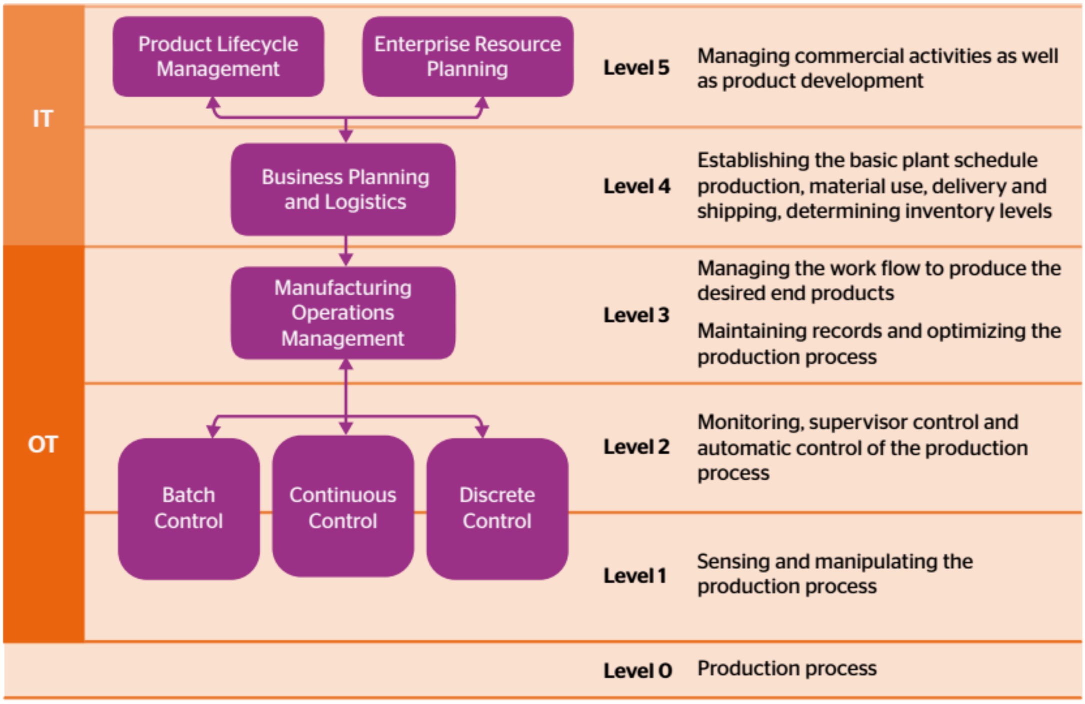

IT
OT
Product Lifecycle Management
Enterprise Resource Planning
Level 5
Managing commercial activities as well as product development
Business Planning and Logistics
Level 4
Establishing the basic plant schedule production, material use, delivery and shipping, determining inventory levels
Manufacturing Operations Management
Level 3
Managing the work flow to produce the desired end products
Maintaining records and optimizing the production process
Batch Control
Continuous Control
Discrete Control
Level 2
Monitoring, supervisor control and automatic control of the production process
Level 1
Sensing and manipulating the production process
Level 0
Production process

Figure 2.2.4 - The Difference Between IT and OT (ATOS, 2012)

The vulnerability of these systems has changed over time. They were previously not dependent on protocols such as the Ethernet and were simple, isolated point-to-point networks (ISACA, 2016). Nevertheless, these systems have become reliant on networks protocols such as Ethernet and Internet (IP). The merger of IT and ICS/OT combines two cultural opposites. IT personnel are concerned with confidentiality, integrity and availability, with a strong focus on confidentiality. ICS/OT personnel typically prioritize availability, data integrity and then confidentiality (ISACA, 2016). The system lifecycle of the two systems are also different. IT systems have a lifespan of 3-5 years before they are replaced or updated, ICS and OT have a lifespan of 15-25 years. The consequences of failure in a IT system is loss of data, while in a ICS/OT environment it can lead to loss of lives, injuries, equipment, material, and environmental damage. The connectivity and availability of these systems is an advantage, but also a vulnerability. In the context of cyber security, these systems are exposed to great risk if not proper security measures and practices are introduced. As suggested by ISACA (2016): Establishing cross-functional teams to handle security of both IT and OT will enable the enterprise to generate a holistic approach to cyber security in the ICS environment and reduce enterprise risk.

Smart Manufacturing and Maintenance

Automation, operations information, and advanced analytics are combined to create smart manufacturing and maintenance. These factors link machines and equipment through open platforms and enable them to interact with each other, analyze data to predict failure (predictive maintenance), and adapt to changes within the manufacturing process (Rockwell Automation, 2016a). This method is using IoT device intelligence, cloud connectivity and data analytics to process large data sets required for balancing production activities based on inventory and demand. Manufacturing decisions can be based off of consumer data and input and used to determine how and when production starts. The more data sets are analyzed, the more the system learns about itself. Data can be gathered throughout individual plants and across corporations. Once the data has been analyzed and the manufacturing intelligence grows, it can be used to improve cost, safety, and environmental impact.

Rockwell Automation (2016b) presents examples of the benefits generated from using smart manufacturing and maintenance:

- Automotive companies are using automated data systems and increasing overall efficiency and productivity by 50%. The use of real-time flow between enterprise resource planning software, production and supply chain makes delivery system close to errorless.
- Oil and Gas companies are using predictive maintenance and decreases unscheduled downtime and increases safety.
- Mining companies are utilizing technology to gain visibility from pit to port, enabling remote information access and increasing safety by keeping workers out of dangerous environments.

Smart manufacturing encompasses the merger of IT and Operations Technology (OT) systems into a single, unified network infrastructure and identify opportunities for using IoT technologies that enable seamless connectivity and information sharing across people, processes and things (Rockwell Automation, 2016a). This use of interconnectivity can benefit the efficiency, visibility, and productivity of manufacturing, but it also creates a necessity for security.

Smart infrastructure

Smart systems can be used in energy production, water and wastewater distribution, land and maritime transport, communications, buildings. Utilities, such as water and power, apply smart grids to make them more efficient. Smart grids are adaptive, predictive, integrated, reactive, and optimized (The Royal Academy of Engineering, 2012). The system can adapt to the changes in supply and demand based on data from the water or power source and customer usage. It can also “learn” based on models and used data to predict how much of the system capacity is needed. This can be useful when planning and operating the system. The use of sensors, networks, etc., makes the system integrated, which means it can distribute supply, collect consumption data and control according to information at any location of the grid. The system is reaction in the sense that the system can respond to the actual usage of the customers, rather than distributing a fix amount. The smart control system makes the grids themselves capable of maximizing efficiency while operating.

2.2.5 Connectivity, Risk and Security

Threats evolves with the development in technology and to the extent that it is used. The digital transformation drives new developing business trends, applications and uses. As described in a previous chapter, digitalization brings change into technology, business, society, and culture. All the factors impact decision making related to future investments, operation and overall objectives. There are additional factors that needs to be considered in the decision-making process, such as interconnectedness, the impact of long and complex supply chains, and ownership, governance, assurance, and control of outsourcing and third parties. Lloyd's (2010) describes four trends that impacts the modern business:

- **The Explosive Growth in Digital Information**

The digital transformation brings new ways of gathering information related to production, manufacturing, customer and marked. Terms like Big Data, Machine Learning, and Cloud Computing, utilizes large amounts of data, analysis and access to information. Business intelligence can bring surprising benefits to an organization. However, it requires sophisticated data management procedures and investment in IT infrastructure. Additionally, there is a challenge in maintaining data integrity availability and confidentiality when managing large volumes of data and users.

- **Advancements in Connected Technology**

Advancements in mobile devices, connectivity and visualization of information has had a great impact on businesses. Personal devices and interconnected networks and infrastructures makes for great availability, but it makes it easier for malware to spread other networks and devices (Lloyd's, 2010). The risk is affected by user behavior and the business' digital architecture. Further, international supply chains make it difficult to have assurance of services and products (Lloyd's, 2010). Additionally, better security needs to be built in devices and standard computer systems. This has potential to significantly impact the risk management. Generally, the connectivity leads to more exposure from interconnected devices, networks, and infrastructures.

- **Changes in How People Connect**

People are connected and share information in a different way than before. Whether it be work related or personal, information can be shared on the internet via social networking (Lloyd's, 2010). Social networking is used to create and maintain relationships, as well as distribute information (picture, metadata, text, etc.) about themselves and others. This can affect the work environment in positive and negative ways (Lloyd's, 2010). The negative part is that information can be leaked intentionally or unintentionally. It is also a source for social engineering attacks (manipulation based on available personal information), spread of malware, and reputational damage (Lloyd's, 2010). People share more information online than before. The technology allows a seamless distribution of pictures and similar. The social culture encourages the distribution of personal information and users are unaware, or not mindful of, the possibility that it can be misused. This information presents a risk and can be used to establish the initial stage of a targeted cyberattack.

- **The Trend Towards Virtual Online Business**

There is a growing trend to investments in cloud services (Lloyd's, 2010). This can lead to the development of true virtual businesses as the almost every aspect of the business can be outsourced. The growing market for IT services is great for business agility and cost reduction, as it is costly to operate IT infrastructures (Lloyd's, 2010). The services make businesses have less capital commitment and does not need to have the specialized expertise. However, there are risks linked to this way of doing business. Lloyd's (2014, page

28) states “*It is not that cloud is necessarily less secure. In fact, when run by specialist IT providers, it may offer better security. However, for cloud to become a trusted platform for critical business services, it will need to provide much better assurance offerings, giving improved visibility on security levels that integrate into the overall digital risk management process.”* There are clear visibility and control issues related to outsourcing of services – location, audit, governance and financial resilience (Lloyd’s, 2010). There are legal and regulatory issues associated with location of the cloud operation. Businesses must be aware of what country the service is operated from and what the legal jurisdiction are. Audits of the IT systems and services must be performed. Generic audits may not be sufficient, and managing a variety of audits may be costly and contradictory to the initial intent. Governance is vital for ensuring that the service provider complies with the requirements of the customer. Customers and suppliers may have different security and identity management approaches. This could undermine the overall control and compliance (Lloyd’s, 2010). The last factor is financial resilience. This has a large impact because of its relevancy in rapidly changing economy and may create unexpected events. If a service provider fails to profit from its service, it can go bankrupt or withdraw its service. This contributes to the operational risk, where data availability may get lost and unrecoverable along with the service. A worst-case scenario would be that service provider’s assets are sold and the ownership of the data would disappear and the data would be in outsider’s possession.

Large scale service providers can be an attractive target for threat agents, due to the large data content from various companies. The cloud service providers can also use third parties in parts of their operation. This leads to long and complex supply chains. The customer must then manage the risks beyond the cloud service provider. This can be difficult to assess the quality of other service provider’s infrastructure and platforms. All stakeholders should perform due diligence and share appropriate assurance information (Lloyd’s, 2010).

2.3 Practical Examples of Connectivity

2.3.1 Medical and Health Care

Digital Patient Journal – shared between medical health care services

The digitalization of the patient journals is a new way of making information accessible for health care services across the country (Zachariassen, 2012; Direktoratet for e-helse, 2016a). It is a new information platform where all the health care services and sectors, including the patients, have *access to and shares the same patient journal*. Hospitals and other health care services are currently using different systems that are not compliable with each other. A system like this can improve the communication and collaboration between different health care services and sectors, and increase connectivity between systems. Thus, the patient and health care personnel benefits from spending less time on patient documentation and it does not matter where in the country the patient is treated.

Personal sensors and remote data gathering

The digital infrastructure allows for further digital development, as seen with *personal sensors, data gathering, and data processing*. With personal sensors, patients can be monitored and the data can be harvested in a database for analysis. This method can find indications of diseases earlier than previous methods. Mobile sensors can be used to monitor groups at risk at home, for example persons with heart failure, heart rhythm disorder, or diabetes (Sykehusbygg, 2016). These sensors include mobile units, application-based programs, and simple support services to motivate the patients in treatment (Direktoratet for e-helse, 2016b). These solutions are portable, wearable, and can be placed inside bodies. This allows for the health care services to access information about the specific patient and process the data.

2.3.2 Aviation

Remote Controlled Air Traffic Control Towers

Avinor is developing remote controlled air traffic control towers (ATC) (Avinor, 2017). The purpose it to allow one person to control multiple airports at the same time. This decreased the investment costs for each air traffic control tower. The maintenance costs for each ATC is expected to decrease, which will in turn decrease the total costs of operation. The challenge is to implement the system and maintaining the same level of security as before. Avinor's area of operation include several small airports which experiences small amounts of, or large deviations in, traffic volume. This presents the opportunity to merge the control of several towers. The aviation industry is regulated by strict rules for safety and security. The technologies in remote controlled ATC allows the staff to have access to more information than traditional towers, by the help of military technology, *cameras and visualizations techniques* (Solberg, Bjerkeseth and Brønseth, 2015). The increased information flow can give the staff a better overview of the situation. The remote-controlled solution will be implemented if it is documented that it as safe as todays solutions. This solution of remote monitoring and control increases connectivity of the ATC and presents a cyber risk.

2.3.3 Public Sector

Public Service Management - Altinn Portal

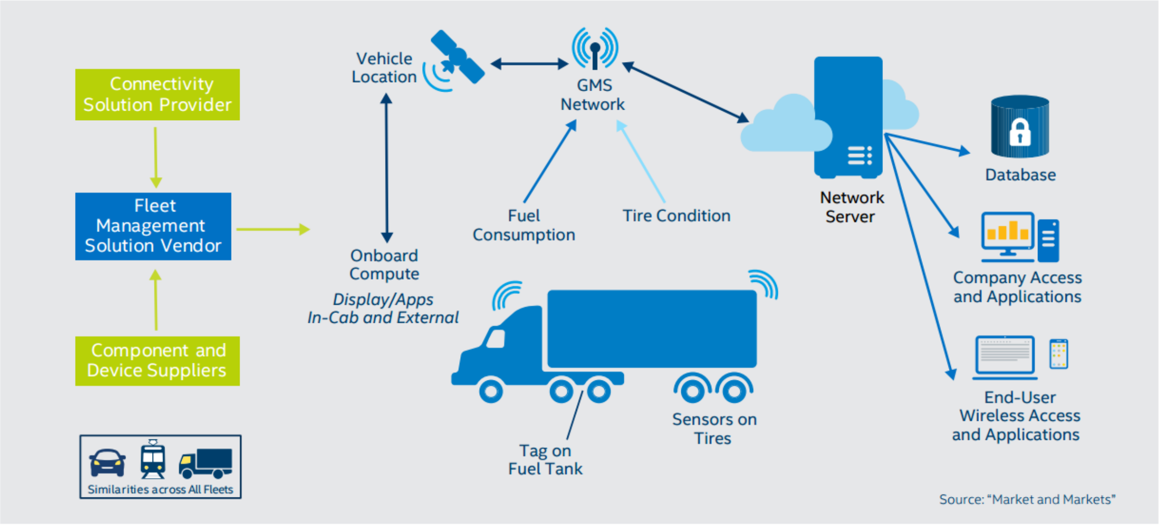
Altinn is an internet portal for communications between business, individuals and government agencies, as well as a platform in which public organizations can utilize for digital services (Altinn, 2016). Its purpose it to manage public forms and applications. The portal offers an infrastructure for the development, management and operation of forms and services from the public sector. The aim of Altinn is to facilitate simplified and more efficient interaction between the users and the public sector (Altinn, 2016). It is a joint operation between Skatteetaten (Tax Administration), Statistisk Sentralbyrå (Central Bureau of Statistics), and Brønnøysundregistrene. It is operated by Brønnøysundregistrene's Department for Digitalization.

It is utilized by over 4 million private individuals and over 1 million organizations. The digital platform is a very cost-efficient and has saved billions of NOK since its start in 2003. The platform *connects businesses with the public sector and the Norwegian citizens*. This means that the digital platform contains a lot of information and access point, which introduces cyber risk due to the connectivity.

2.3.4 Transport

Connected and Autonomous Vehicles

The next generation transport vehicles will be autonomous with increased connectivity to other devices, vehicles, and infrastructures. Vehicle-to-vehicle and vehicle-to-infrastructure communication creates a need for automotive manufacturer to ensure data protection and include cyber security in their products (SMMT, 2017). Intel Corporation (2016) is creating a platform that allows cars to be connected to a cloud. This leads to many new services such as immediate driver feedback. The ongoing developments in telematics, a multidiscipline of ICT and engineering in vehicles, makes vehicles safer and increases productivity and profitability (Intel Corporation, 2016). A scalable cloud makes it possible for fleets of transport vehicles to communicate with each other. The technology allows owners to check its location, condition, speed, etc.


Connectivity Solution Provider
Fleet Management Solution Vendor
Component and Device Suppliers
Similarities across All Fleets
Vehicle Location
GMS Network
Fuel Consumption
Tire Condition
Onboard Compute
Display/Apps In-Cab and External
Tag on Fuel Tank
Sensors on Tires
Network Server
Database
Company Access and Applications
End-User Wireless Access and Applications

Source: "Market and Markets"

Figure 2.3.4 – Fleet Management Solution (Intel Corporation, 2016)

Figure 2.3.4 shows how the vehicles are connected to other devices and the cloud. There are many uses for connectivity, but it produces major data streams that can be misused. This creates new requirements for security.

2.4 Challenges of Digitalization

The digital transformation can benefit society and industry in many ways. However, there has never been a transformation or a change without any challenges and obstacles to overcome. The growing dependency, interconnectivity and complexity of digital systems may cause problems. There are many organizational, technical and human challenges in transforming into the modern times. Issues such as privacy, security, availability, dependency, complexity, change, risk and competence are important and must be addressed at some point or another. Some of the challenges are considered in this chapter.

2.4.1 Successful Implementation of a New ICT system

The first level that must be completed is the successful implementation of the new ICT system. This is not a new thought, but it is the first step in an essential and important process. Organizations tend to focus more on the technical side of the change process, rather than the social system and the organizational structure. Eason (1992) has given several propositions regarding the exploitation of new technology, here are three of the main objectives:

1) The successful exploitation of information technology depends upon the ability and willingness of the employees of an organization to use the appropriate technology to engage in worthwhile tasks;
2) The design target must be to create a socio-technical system capable of serving organizational goals, not to create a technical system capable of delivering a technical service;
3) The effective exploitation of socio-technical system depends upon the adaptation of a planned process of change that meets the needs of people who are coping with major changes in their working lives.

The success of the implementation process depends on the employees' motivation to use the technology. Many employees fear that new technologies may steal their job and make themselves useless for the organization. Also, many employees may feel that it is an unnecessary change to their work flow, or that they feel distant to the technology because of lack of knowledge, competence or skills. The first objective is to ensure that the employees feel that the technology is a worth the time to learn and the effort to use the technology. If a IT system is difficult to use, the workers may reject the system and will make the integration unsuccessful. The second objective is to see beyond the technical aspect of the technology and see how the technology will help the organization reach their goals. It is not purposeful to implement a technical system if it does not contribute to value creation, such as increased work flow efficiency and employee engagement, or to the overall organizational goal. The relationship between technology and the socio-technical system must be matched. The socio-technical system cannot succumb for technological capabilities. For example, if a new technology (automation, software, hardware, etc.) is implemented to do a task more efficiently, but in the process, causes substantial change to the organization and socio-technical structure, the implementation may be inefficient and unwelcomed. The productivity is not better until the social structure is compatible with the technical system. Eason (1992) states that implementing an optimal technical system and forcing a social system to become sub-optimal must create sub-optimal results overall because the two systems (social and technological) are closely interconnected. The technical system should be harmonized with the organizational system to create a functioning socio-technical system. This will help achieve the goals of the individuals and the organization. The third objective is to be aware of needs and the impact the change has on the “stakeholders”. A properly planned process of change will involve workers or end-users and identify their needs. The social system needs time to get used to and adjust to the changes. If the workers (or “stakeholders”) are involved in the planning and design phase, they are more likely to reach a successful implementation and a higher performance more quickly.

The transition and implementation of new complex technology

The primary motivation for using new technology is the potential for reducing operational cost, increase performance, higher yield from resources, and increased safety and control. In general, utilizing new technology is a risk taken for the potential of gaining a competitive advantage, or simply in fear of becoming outdated and lose market shares. An example from the oil and gas industry shows that the swift implementation of integrated operations may become more cumbersome than expected (Jaatun et al., 2007, page 5). The complexity of the system becomes of a higher degree than expected and the projects become delayed due to the underestimation of the implementation process. Not only does new ways of working take time to implement and get used to, the security issues related to new technology is often not considered in depth. The oil and gas industry have invested in expensive platforms and equipment. Are they willing to upgrade these old, but still profitable solutions? The cost of an upgrade may prove to be very expensive. However, the organizations must consider the possible consequences of using old and unsecure equipment.

Changing the Organization

Rick (2016) states that the challenge is to educated and train the employees of the organization. The change is not about hardware of software, but the function of the organization and how it behaves. Successful digital transformation needs management commitment and an interest in technology. The change needs to start at the top and move down throughout the organization (Rick, 2016). There are new requirements to leadership skills, expertise, processes, and data, and most importantly how they interact.

2.4.2 Creating a Common Culture

Common Language and Understanding of Risk

The use of digital systems means that groups and leaders of different professional backgrounds engage in conversations about risk, decisions, etc. The technical knowledge and language will be different between the individuals in the discussion. If directions are misinterpreted the organization will suffer from low efficiency and possible unwanted events. As well as, poor communication and misunderstandings are common causes to high temperature discussions and unfriendly encounters. It is important to establish a common understanding of the system's function, application and vulnerabilities to engage in smart conversations. In addition, the understanding that individuals have different backgrounds and levels of knowledge. This means that leaders and technical personnel can discuss best practices and routines related to operation, maintenance, safety, and security. This also apply to the relationship between suppliers and customers. Upstream Intelligence (2017) makes a statement that operations management is not interested in the latest and high-tech components for digital solutions, but to understand risk and return of investment (ROI) very well. The communication should be built around terms such as increases in production, lower operating expense, lower capital expense, lower maintenance and improved and equipment integrity. ICT and ICS language can be difficult to understand. This means that in a conversation between a surgeon, a mechanical engineer and an IT-service operator to develop a new aid in surgery, they must recognize that all the participants have different professional backgrounds and language. This also applies to the difference in culture and language between international organizations.

Creating a Common Security and Safety Culture

In the same way that language can be a barrier in achieving efficiency, a common understanding of risk is most important in an organization. There are many different departments and modern organization may have a virtual structure and value chains based on the collaboration between many international organizations. This may result in divergent and different practices related to risk, safety and security across the organization. New technology, business models and virtual organizations creates a need for a common understanding of digital risk and a common security and safety culture. Incident reporting and learning from incidents (for example a cyberattack) among all the involved actors are key issues to reduce the risks (Jaatun et at, 2007). Developing common policies, awareness and distributing information and knowledge to the involved actors are key elements in creating a common culture. How can an organization collaborate with other organizations with different understanding of digital risk? If organizations shared security related information, such as threat picture and best practices, it may help create a common understanding of risk and in turn create more secure trade.

2.4.3 Cyber security and constantly changing treat picture

The cyber threat picture is always changing. Organizations and governments must deal with threats from cyber criminals and nations. Organizations must protect their assets and values in a different way than before. Espionage, sabotage and insider threats have possibilities through digital vulnerabilities. In addition, the value chains are becoming more intertwined, vulnerabilities in one organization may influence others. The aspects of cyber security and vulnerabilities in cyber security will be assessed in chapter 4.

2.4.4 User and Data Management

Industries can make great use of data related to production and operation. With the use of strategically placed sensors and instruments, the manufacturing process can become more efficient, but only if the data is managed. Organizations may have access to substantial amounts of data, but lack the ability to analyze and find a use it. Data collection, processing and analysis may have a more important role in the future and it may become a profitable industry. Key principles in information security can be challenged in the digitalization process (NSM, 2015):

- Confidentiality – the principle in which information is only available for authorized users
- Integrity - the principle in which information is complete, accurate and valid, and has not been altered or changed unintentionally or in a malicious way.
- Availability - the principle in which authorized user has access to the information when they need it.

As systems become more complex, interdependent, and interconnected, the challenge is to ensure:

- Authentication - that the user of an ICT system has the right identity.
- Authorization - that user of ICT system is provided with the right access.
- Non-repudiation - that the actions in a ICT system is logged and cannot be refuted.

This is a relevant issue in managing sensitive information and ensuring a secure operation, for example in the medical sector, finance, or in oil and gas. Privacy issues and security in data management are issues that the regulations and laws need to take in consideration.

2.4.5 Dependency

As more organizations develop a digital infrastructure, the organizations become dependent on the digital systems. The systems have vulnerabilities that can be exploited. This presents a need for redundancy and emergency procedures for critical societal functions. What does the organization do if the digital systems fail? It has been a concern of authorities and key issues presented in Lysneutvalget (DNV GL, 2015).

Chapter 3 – Digital Risk

The digitalization is changing the world, society, and culture. The work flow and infrastructure of governments and organizations are changing to a more efficient and controllable process. Decisions are assisted by information, data analysis, and computer assistance. Complex operations can be controlled and monitored from long distances, employees have access to networks and databases, and automation is making manufacturing more efficient. These benefits come with a downside. The increased connectivity creates exposure to digital vulnerabilities and cyberattacks is the current threat in the digital age. Society relies upon the undisturbed functions of infrastructures and their services. A failure in one of these infrastructures or services may lead to serious consequences, such as loss of life, financial damage, environmental damage, or compromised functions of authorities. Digital systems are exposed to risk from organizational decisions, and technical and human failure. Unwanted events can also be caused by actors with harmful intents through cyberattacks. Cyberattacks have the purpose of stealing or manipulating data and information, or causing accidents and sabotage by taking control over production systems. The increased connectivity comes with a risk, a cyber risk.

3.1 What is Risk?

Aven (2015) defines risk as an activity, for a specified period of time, that leads to some future consequences. These consequences are unknown, uncertain and include both positive and negative outcomes. However, it is a requirement that one of the consequences would be undesirable or negative. A risk description is defined from the event, assumed consequences, a description of uncertainty, and background knowledge or information (Aven, 2015). Table 3.1.1 and 3.1.2 shows an example, adapted from Aven (2015, page 15) to describe digital risk:

Table 3.1.1 – Digital Risk

Digital Risk
Consequence: The occurrence of a cyberattack of a specific type (known or unknown types) and its time occurrence, and its consequences for an organization (loss of data, production interruption, etc.).
Uncertainty: Today we do not know if the organization will be exposed to one or more of these cyberattacks, and we do not know what the consequences will be.

Table 3.1.2 – Digital Risk Description

Digital Risk description
Event: The organization is exposed to a specific type of cyberattack next year.
Consequence: The organization's consequences are simplified in four categories: 1) the organization suffers production stoppage, 2) reduced production speed, 3) loss of important data, 4) no consequences.
Uncertainty: Based on the knowledge we have obtained through our process, we can express the likelihood of such an event and the consequences. This can be a quantitative or a qualitative expression of the uncertainty.
Knowledge: the knowledge we have based the assessments on are data, information, models, justified beliefs and assumptions.

3.1.1 Uncertainty

It is important to notice that information carries uncertainty, meaning that information can be biased, wrong, or partly true. Like most decisions and assessments, they are done without a 100% certainty and complete access to information. In situations where there is high risk and large uncertainties, it is difficult to predict the consequences or outcome of the decision. This affects the quality of the risk assessment. Sometimes, the risk assessment process contributes more value than the actual probability that an event occurs. The risk assessment is a tool in which the participants get acquainted with the possible events and its consequences. The assessment guides the management or risk assessors through a process which proves an outcome (or probability) given a set of information, models, or data which carries uncertainty. The process can strengthen risk awareness and at the same time, demonstrate to the management what the results are based on. If not properly used, a risk assessment can give a false understanding of risk by narrowing it down to a specific number without explaining the reasoning of the conclusion.

In the matter of digital risk, there is the emerging threat of sabotage, espionage, and cybercrime from criminals, hackers, and nations. This risk picture is evolving and the probability of any form of cyberattack changes with the increasing number of malicious actors and their access to sophisticated tools and methods. As organizations depends more on digital systems to function, the organizations are more vulnerable and can suffer large consequences if not properly secured. This implies that a risk assessment should be done regularly with updated background knowledge, as the risk picture is constantly evolving. Digital risk is developing and black swans can emerge due to a low risk awareness or a smart cyberattack which utilizes an unknown exploit. A black swan is a surprising, extreme event relative present perception and knowledge (Taleb, 2007). These events may have catastrophically consequences for the organization, environment, and humans. There are three types of black swans (Aven and Krohn, 2014, page 9):

- Unknown unknowns – events that are completely unknown to the scientific environment

Unknown viruses and methods can occur as the criminal actors become more cunning and sophisticated in their methods. In some incidents, the attackers use a zero-day attack, such as Stuxnet, which means that there has been no record of a similar event from the time the threat becomes active. These events rely on high competent personnel and resources to be able to respond and reduce the consequences of such an unknown threat.

- Unknown knowns – events that are not on the list of known events from the perspective of those who carries out risk analysis, but known to others. Unknown to some, known to others.

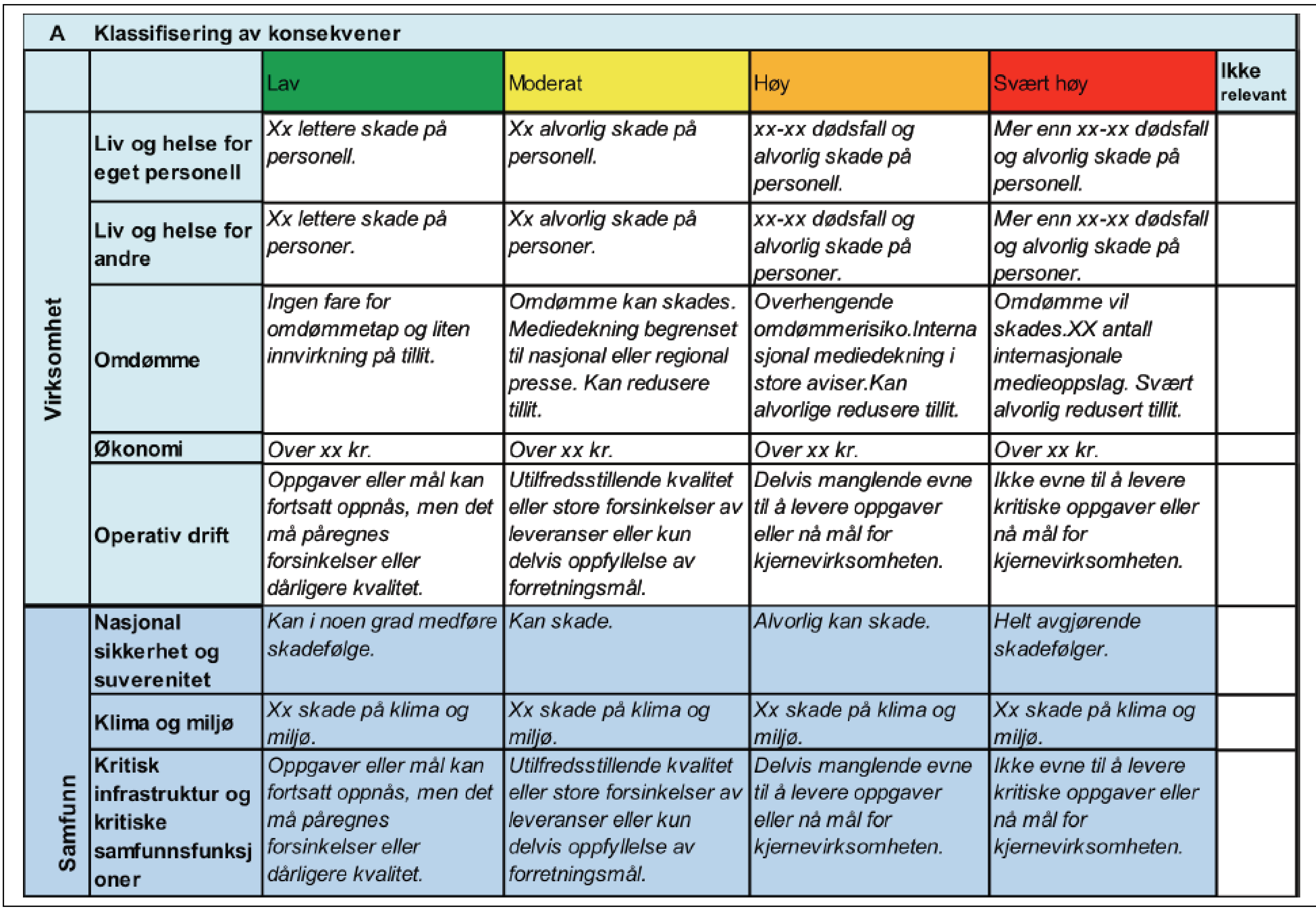
The competence level and resources within the organization depicts how the information of digital risk is utilized, which makes some organizations more aware of risks than others. The prioritizing of digital risk and risk assessment in general, makes a difference to how well the organization knows about black swans.

- Knowns, but not believed to occur because of low judged probability

Each organization have access to and can allocate resources differently. Some organizations the benefit of preventing some unlikely scenarios is best not to be bothered with. This prioritizing may have something to do with the size and the values created by the organization, and how much of digital technology they use.

Risk acceptance criteria (risk tolerability limits) is the organization’s predetermined limit to how much risk is acceptable at a given time. If the calculated risk is within range of this value, then it is acceptable. Otherwise, the risk is unacceptable (intolerable), and risk-reducing measures are required (Aven, 2015). It should be calculated to fit the organization’s ability to carry risk. All risks should be reduced by following the ALARP principle (As Low As Reasonably Practicable). This principle means that the benefits of a risk-reducing measure should be assessed in relation to the disadvantages or costs of the measure (Aven, 2015). This implies that a measure should be implemented if it does not create a significant disadvantage for the organization, such as high costs. This suggests that there will be differences in risk acceptance criteria and ALARP principle of industry companies. For example, a large organization, such as a highly profitable international oil and gas company with 30 000 employees, and a smaller organization, such as a steel structure production company with 15 employees. These two organization will have different risk carrying capabilities.

Risk can be accepted, reduced, avoided or transferred to a different party. A structured risk assessment is an analysis that includes identification and categorization of risk for humans, environment, and financial value (DNV GL, 2015). Risk reducing measures can be made and identified as barriers. The function of a barrier is to prevent an unwanted event and partly reduce the consequences of an occurred unwanted event. There are tools that help the risk assessors define critical systems, consequences and threats. NSM (2016b) has developed a handbook for risk assessment which serves as a good framework for a structured risk assessment. It is based on a set of ISO standards, NSMs own guidelines for security management, and other public authorities' guidelines for security management. The process includes identification of values and assets in the organization, assessment of security targets, threat assessment, scenario planning, vulnerability assessment, and an overall risk presentation with risk reducing measures. First the organization should do a categorization of consequences by using figure 3.2.1. This figure is produced as a reference point for the future assessments. The process continues with a value assessment.



A	Klassifisering av konsekvener					
		Lav	Moderat	Høy	Svært høy	Ikke relevant
Virksomhet	Liv og helse for eget personell	Xx lettere skade på personell.	Xx alvorlig skade på personell.	xx-xx dødsfall og alvorlig skade på personell.	Mer enn xx-xx dødsfall og alvorlig skade på personell.	
	Liv og helse for andre	Xx lettere skade på personer.	Xx alvorlig skade på personer.	xx-xx dødsfall og alvorlig skade på personer.	Mer enn xx-xx dødsfall og alvorlig skade på personer.	
	Omdømme	Ingen fare for omdømmetap og liten innvirkning på tillit.	Omdømme kan skades. Mediedekning begrenset til nasjonal eller regional presse. Kan redusere tillit.	Overhengende omdømmerisiko.Internasjonal mediedekning i store aviser.Kan alvorlige redusere tillit.	Omdømme vil skades.XX antall internasjonale medieoppslag. Svært alvorlig redusert tillit.	
	Økonomi	Over xx kr.	Over xx kr.	Over xx kr.	Over xx kr.	
	Operativ drift	Oppgaver eller mål kan fortsatt oppnås, men det må påregnes forsinkelser eller dårligere kvalitet.	Utilfredsstillende kvalitet eller store forsinkelser av leveranser eller kun delvis oppfyllelse av forretningsmål.	Delvis manglende evne til å levere oppgaver eller nå mål for kjernevirksomheten.	Ikke evne til å levere kritiske oppgaver eller nå mål for kjernevirksomheten.	
Samfunn	Nasjonal sikkerhet og suverenitet	Kan i noen grad medføre skadefølge.	Kan skade.	Alvorlig kan skade.	Helt avgjørende skadefølger.	
	Klima og miljø	Xx skade på klima og miljø.	Xx skade på klima og miljø.	Xx skade på klima og miljø.	Xx skade på klima og miljø.	
	Kritisk infrastruktur og kritiske samfunnsfunksjoner	Oppgaver eller mål kan fortsatt oppnås, men det må påregnes forsinkelser eller dårligere kvalitet.	Utilfredsstillende kvalitet eller store forsinkelser av leveranser eller kun delvis oppfyllelse av forretningsmål.	Delvis manglende evne til å levere oppgaver eller nå mål for kjernevirksomheten.	Ikke evne til å levere kritiske oppgaver eller nå mål for kjernevirksomheten.	

Figure 3.2.1 – Categorization of consequences NSM (2016b)

Value Assessment

The purpose of the value assessment is to identify intangible and tangible values and assets that are most important for the organization and its operation. The approach will identify the consequences if one of the assets or values are targeted. It is an awareness process which helps build the foundation for the risk assessment. Regulations and legislations can demand that certain assets shall be secured, such as according to the Security Act (in Norwegian: *Sikkerhetsloven*) or sector regulations. The organizations are obligated to secure these assets. In addition to the mandatory obligations to secure certain assets, there are those assets that the organizations regard as valuable or critical. The main steps of the value assessment include (NSM, 2016b):

1) A limitation of scope to include certain processes, or parts of the value chain.
2) Identify processes that are critical for operation and an evaluation of the consequences if it fails.
3) Identify the resources, assets or systems that are connected to the critical process. These resources, assets or systems include equipment, networks, power & water supply, third party services, etc.
4) Combine the resources, assets and systems into a list.
5) Categorize the values according criticality based on the reference in figure 3.2.1.

The organizations operation must be divided into departments or processes to be able to assess the different parts of the organization, such as equipment, information, networks, etc.

Determine an Acceptable Risk Target

This is where the organization determine the acceptable risk or security target. This means that the organization must choose what is acceptable damage or loss of assets, values, system, or resources. The security target is the basis for how much resources is applied to reduce the risk. This step is reevaluated at the end of the risk assessment when the organization have an overview of the full risk picture. A cost-benefit analysis in combination with the acceptable risk target forms the basis for development of the risk management strategy. Steps in this process (NSM, 2016b):

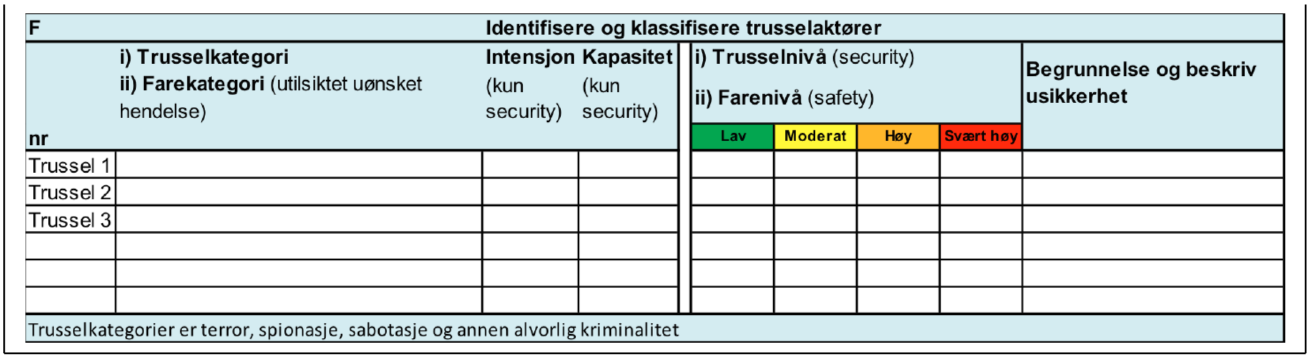
1) Create a security target for each of the values. For example, downtime of a system cannot exceed more than 20 minutes, or incident response must be active less than 30 minutes after incident detection.
2) Evaluate all values and security targets, and accept.

Threat assessment

The threat assessment looks at the current threat picture for the relevant values and assets. It assesses the motivation and capabilities of real and potential threat agents. The relevant threat agents related to cyber security is presented in chapter 3.4. The cyber threat is continuously evolving, which means that it is difficult to obtain an updated threat picture. Organizations such as NSM, PST, Norsis, and other publicly available documents and reports can be great sources for an updated threat picture.

Figure 3.2.2 show the template of the threat assessment. The steps in this process are (NSM, 2016b):

1) Acquire information about the threat picture using relevant sources. Evaluate the information and source credibility.
2) Identify relevant threat.
3) Evaluate and categorize the threat agents according to motivation and capabilities.
4) Determined the threat level of each threat agent.
5) Explain the choice of threat agents and threat level.
6) Comment the uncertainty of the evaluation.



F	Identifisere og klassifisere trusselaktører							
nr	**i) Trusselkategori** **ii) Farekategori** (utilsiktet uønsket hendelse)	**Intensjon** (kun security)	**Kapasitet** (kun security)	**i) Trusselnivå** (security) **ii) Farenivå** (safety)				**Begrunnelse og beskriv usikkerhet**
				Lav	Moderat	Høy	Svært høy	
Trussel 1								
Trussel 2								
Trussel 3								
Trusselkategorier er terror, spionasje, sabotasje og annen alvorlig kriminalitet								

Figure 3.2.2 – Example of Threat Assessment (NSM, 2016b)

Scenario Planning

The purpose of utilizing scenarios is to highlight vulnerabilities in the organization. The value and threat assessment forms the basis for each scenario. Each scenario is simplified so that decision makers can understand how the threat agent will proceed to cause harm to the assets and values. The scenario includes chain of events, motivation and capabilities of the threat agent, a description of how values and assets can be harmed, the consequence on connected or coupled values, if there is a warning from authorities prior to the event, and the time and duration of the event. The steps in this process are (NSM, 2016b):

1) Choose the most relevant threat agents. Explain why.
2) Approach the case from the threat agent's point of view and consider what values and assets are of interest and how they can be attacked. Develop a scenario from this evaluation.
3) Document each scenario.
4) Compile the scenarios in an overview.

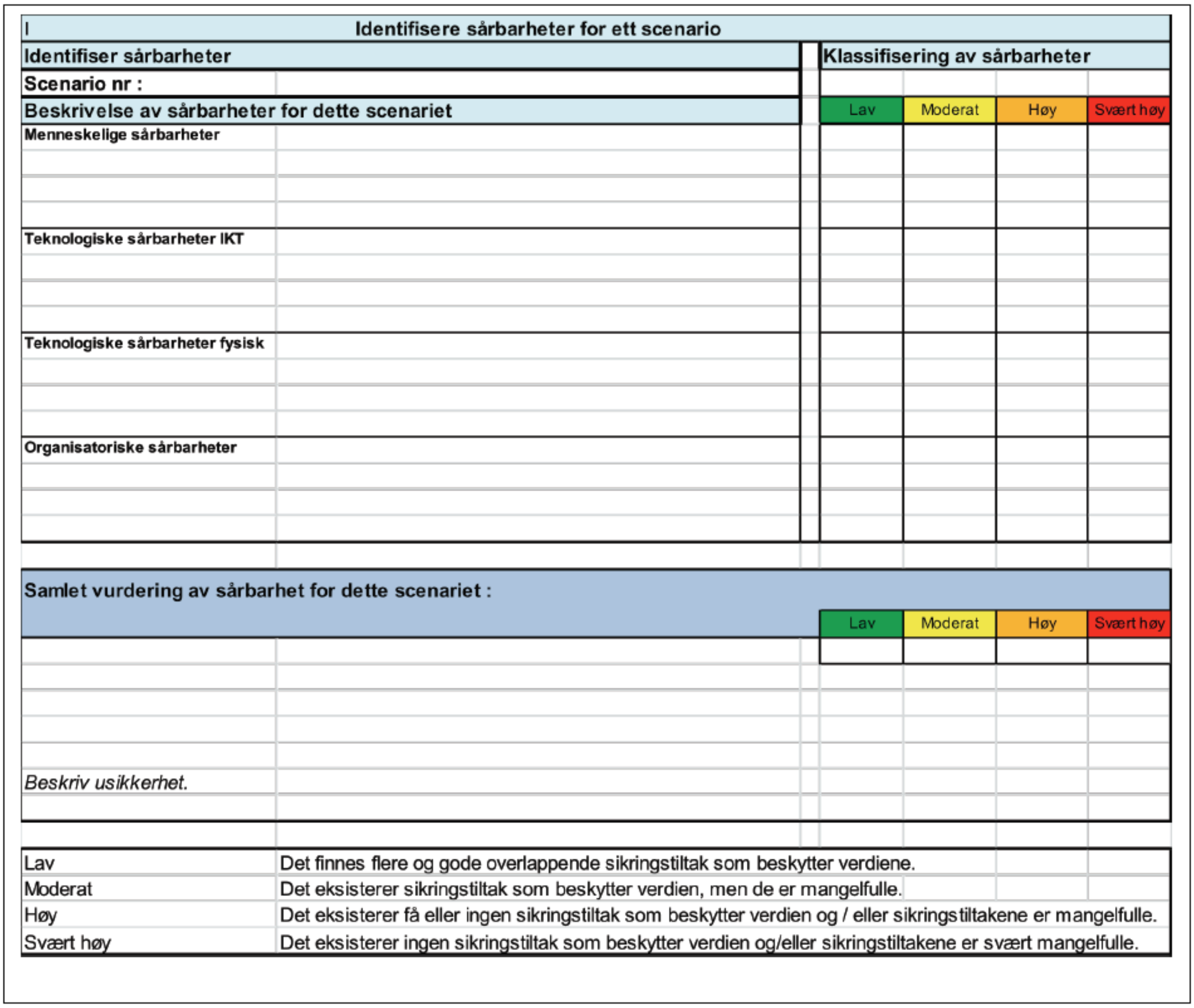
Vulnerability Assessment

The vulnerability assessment highlights the gap between security measures and the threat agent's intention and capabilities. A vulnerability is the inability to resist an unwanted event or to establish a steady state once a value or asset has been affected (NSM, 2016b). To evaluate the vulnerability one must look at the existing security measure and how they perform. If no security measures have been implemented, then a desired performance criteria is established. Vulnerabilities and their security measures can be divided into three main categories: Organizational (security management), human (personal security), and technological (ICT security and physical security). The steps in this process are (NSM, 2016b):

1) Describe the vulnerabilities for each scenario. Evaluate the performance of each security measure.
2) Categorize each vulnerability into low, moderate, high, or very high.

3) Assess the vulnerabilities for each scenario.
4) Explain the uncertainty of the assessment.
5) Make a list of the most critical vulnerabilities and its scenario reference

Figure 3.2.3 shows an example of a setup for the vulnerabilities per scenario.



I	Identifisere sårbarheter for ett scenario				
Identifiser sårbarheter		Klassifisering av sårbarheter			
Scenario nr :					
Beskrivelse av sårbarheter for dette scenariet		Lav	Moderat	Høy	Svært høy
Menneskelige sårbarheter					
Teknologiske sårbarheter IKT					
Teknologiske sårbarheter fysisk					
Organisatoriske sårbarheter					
Samlet vurdering av sårbarhet for dette scenariet :					
		Lav	Moderat	Høy	Svært høy
Beskriv usikkerhet.					
Lav	Det finnes flere og gode overlappende sikringstiltak som beskytter verdiene.				
Moderat	Det eksisterer sikringstiltak som beskytter verdien, men de er mangelfulle.				
Høy	Det eksisterer få eller ingen sikringstiltak som beskytter verdien og / eller sikringstiltakene er mangelfulle.				
Svært høy	Det eksisterer ingen sikringstiltak som beskytter verdien og/eller sikringstiltakene er svært mangelfulle.				

Figure 3.2.3 – Example of Vulnerability Description (NSM, 2016b)

Compilation of the Risk Factors

This step in the process is the completion of the risk assessment. This is where the value, threat, and vulnerability assessment is combined to describe risk. For example, risk R2 is when value V2 is harmed by threat agent T3 which exploits the vulnerabilities V1, V2, and V6. The steps are NSM, 2016b):

1) Compile the results from the assessments.
2) Formulate each risk.
3) Decide the risk level based on the categorization of value, threat and vulnerability of each risk.
4) Explain the choice of risk level for each risk, including uncertainty.

Risk Picture and Risk Management

When the risk description is done, a visual presentation can provide an overview of the risk picture. The presentation of the risk picture can include qualitative opinions, diagrams, etc. The main point is to communicate the risk to the decision maker. The risk assessment should be evaluated, updated, and form the basis for future assessments. The risk assessment result in a risk management strategy - avoid, transfer, accept or reduce risk. If the risk is to be reduced, risk recuing measures or security measures are implemented. Risk analysis tools that are presented in the next chapter.

3.2.1 Risk Analysis Tools

In the occurrence of an unwanted event or incident, it is critical to identify the root cause or causes were. From a root cause analysis, it is possible to learn and gain experience from the event. It highlights the weaknesses and strengths of the system, organization and the procedures that has previously been in use. This method may include a fault tree analysis (FTA) or a failure modes and effects analysis (FMEA). These are methods that can be used as a preventive tool, before an unwanted event has occurred. There are other tools and methods, but it is not relevant to for this thesis to mention these.

Fault tree analysis

A fault tree analysis is a logical diagram that shows the relation between system failure. For example, a specific undesirable event, such as the initiating event of an accident, the failure of a system barrier, or failures of the components of the system (Aven, 2015). Figure 3.2.1 shows an example of a fault tree from a phishing attack:

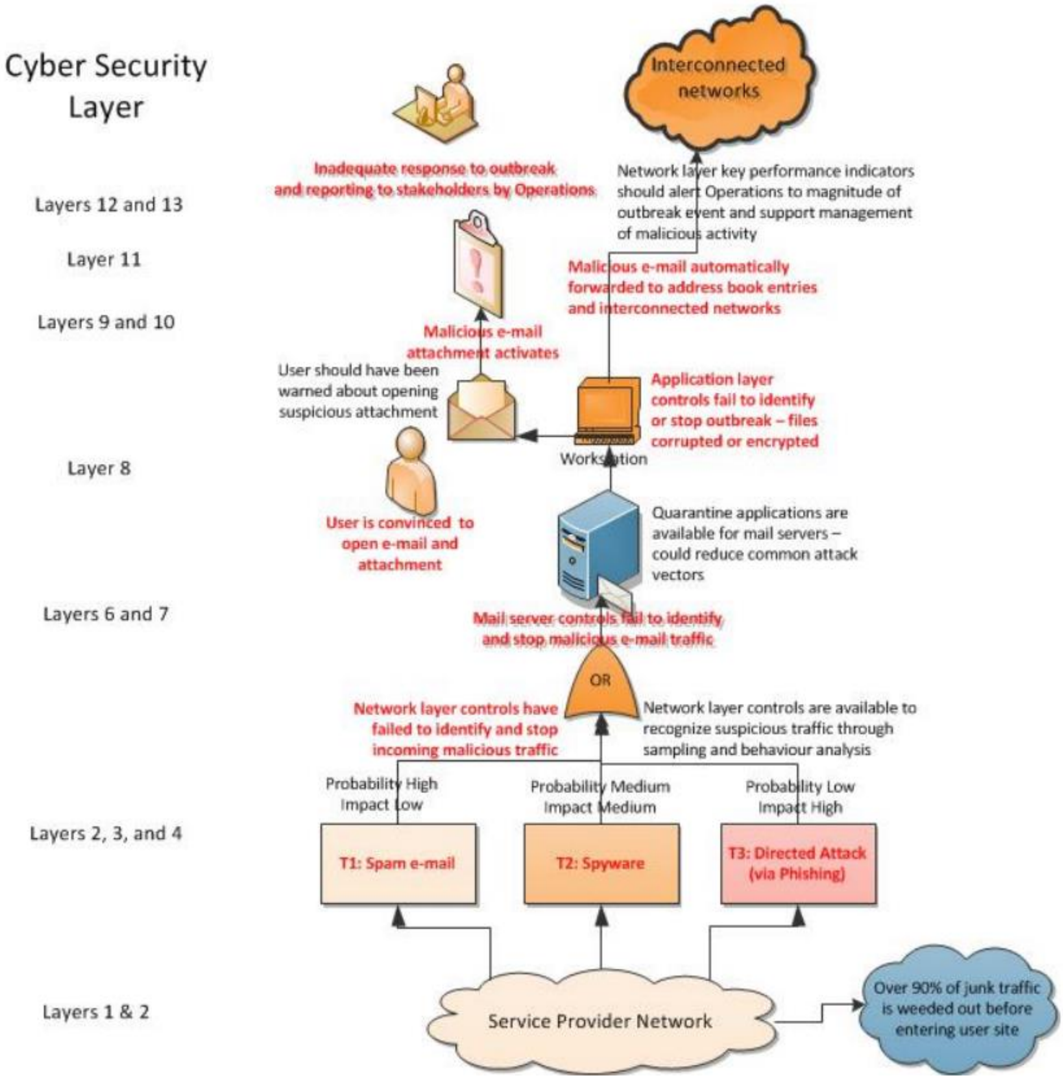

Cyber Security Layer
Interconnected networks
Layers 12 and 13
Inadequate response to outbreak and reporting to stakeholders by Operations
Network layer key performance indicators should alert Operations to magnitude of outbreak event and support management of malicious activity
Layer 11
Malicious e-mail automatically forwarded to address book entries and interconnected networks
Layers 9 and 10
Malicious e-mail attachment activates
User should have been warned about opening suspicious attachment
Application layer controls fail to identify or stop outbreak – files corrupted or encrypted
Workstation
Layer 8
User is convinced to open e-mail and attachment
Quarantine applications are available for mail servers – could reduce common attack vectors
Layers 6 and 7
Mail server controls fail to identify and stop malicious e-mail traffic
OR
Network layer controls have failed to identify and stop incoming malicious traffic
Network layer controls are available to recognize suspicious traffic through sampling and behaviour analysis
Probability High Impact Low
Probability Medium Impact Medium
Probability Low Impact High
Layers 2, 3, and 4
T1: Spam e-mail
T2: Spyware
T3: Directed Attack (via Phishing)
Layers 1 & 2
Service Provider Network
Over 90% of junk traffic is weeded out before entering user site

Figure 3.2.1 – Phishing Fault Tree (Threatalytics, 2016)

Failure modes and effects analysis (FMEA)

Failure modes and effects analysis is an analysis method to reveal possible failure and to predict the failures effects on the system as whole (Aven, 2015). This is a great tool for identifying critical systems in the organization. This is a tool used to identify the consequences if a component fails. The method represents a systematic analysis of the components of the system to identify all significant failure modes and to see how important they are for the system's performance (Aven, 2015). Its weakness is that it does not consider the connections and combinations of component failures. It is commonly used to identify failures in technical systems.

3.2.2 An Example of a Risk assessment in Oil & Gas

From the SINTEF report, Jatuun et al. (2007, page 19) presents a risk assessment process with respect to incident response management in integrated operations. It assesses the probabilities of unwanted events and consequences of potential incidents. The SINTEF report (Jatuun et al., 2007, page 3) defines an incident as: *an incident that could imply loss of availability, loss of integrity or loss of confidentiality related to the ICT or SCADA systems in production systems and thus influencing the production process (leading to a halt or deviation) or lead to an unwanted HSSE incident*.

Four scenarios to illustrate typical incidents related to Oil and Gas

The Sintef report (Jaatun et al., 2007) identified some of the major risks related to integrated operations within the oil and gas industry on the Norwegian Continental Shelf. These are typical incidents that may occur in the energy sector, but also in other industries.

1. Virus infection influencing ICT and SCADA systems

A supplier connects his computer to the production network and a computer virus is distributed to the operator through the network. This is a common cause to virus infection in offshore installations (Jaatun et al., 2007). This is mainly caused by having different security measures between the operator and the supplier. There may also be a lack of updated and patched IT components in the production network and no barrier between the supplier's computer and the production network. The virus is detected a week later after a computer was acting suspiciously and rebooting at strange times. The consequences of this is virus may result in service disruption, possible reduced production and reduced profit, possible disruption of safety instrumented systems that may lead to safety incidents or accidents.

A typical incident response would be to identify what other systems the suppliers has been connected to, and detect if the virus has spread into other systems. Isolation of components and systems, possibly shut down of system, are some of the considerations that needs to be made. Possible improvements recommended by Jaatun, et al. (2007):

- Increased situational awareness of the virus threat may lead to earlier detection and greater understanding of the problem among the employees.
- Scenario training on handling virus and worm attacks in the production systems offshore and onshore will help mitigate risk, earlier detection, and better incident response.
- Detection mechanisms for virus attacks should be in place, such as a digital surveillance system.
- Stronger barriers between the supplier and production network. For example, stricter rules and procedures for connecting suppliers' computers to production network and updating and patching offshore equipment.

2. Denial-of-service incident influencing the SCADA systems

A denial-of-service (DoS) attack targets an IT component at an offshore production site. This is caused by a malfunction or the result of a malicious attack. The increased traffic load, leads to a communication breakdown and the production stops. There is also a suspicion towards a possible impact on the SIS (safety Instruments Systems). A IT component is likely to stop if it is subjected to DoS attack or defective traffic. The attack is detected because it prevents data communication between onshore and offshore control rooms and it jams the production network and possibly the safety instrument network. The consequences are missing communication for a couple of hours, preventing optimized production or stop in production and thus reduced profit, and stop in safety instrument systems which may lead to unsafe work environment and incidents. Additional work hours are needed to restore the systems. A typical incident response would be able to detect the DoS incident fast, and locate and disconnect the affected components to reduce the consequences. Possible improvements recommended by Jaatun, et al. (2007):

- A component and system test prior to implementation
- An alert or notification if the communication traffic is above a defined limit
- Improved barriers between production network and safety instrumented systems
- Establish redundancy for critical IT components and connections,
- Increase the capacity for managing communication traffic, beyond what is expected during normal operation to improved resilience.

3. Insider

A resentful employee creates a backdoor in the production environment, enabling unwanted events such as a shutdown or a critical situation during production. The employee is unhappy with getting fired and decides to get back at the employer by implementing a backdoor or software that can harm the production network. The action may never be detected, unless it is used to launch attacks. An insider may cause incidents and it is important to be aware of this. The root cause of an incident may be difficult to identify. It is a problem that the insider may be able to observe the incident response work and can react accordingly. Possible improvements recommended by Jaatun, et al. (2007):

- Logging and reporting changes in the production environment and abnormal behavior in the system
- Establish barriers to avoid, or carefully manage, outside control of critical operations offshore.
- Regularly updated access control and an access policy based on “need-to-know”. Detection mechanisms needs to be in place for violation of access policy

4. Missing situational awareness

An external service provider is closing a valve in production on an offshore oil and gas platform. The service provider is certain he closed the valve from the test environment. A control room operator discovers the incident and manages to open the valve again, thus avoiding a critical situation. This situation is created due to poor situational awareness. If it was it not detected, it could cause serious consequences and potential loss of life. The challenge is to detect these kinds of incidents before they can cause any consequences. Possible improvements recommended by Jaatun, et al. (2007):

- Improved barriers, including permission from the central control room to do testing and changes offshore.
- Increased focus on scenario analysis/training.
- Document and learn from previous incidents.

An incident response needs to be able to manage a variety of factors and situations. It is common for all incidents that they include a combination of organizational, technical and human factors. Incident management should plan for incidents that may arise from internal misunderstandings and system error, in addition to traditional external attacks.

Table 3.2.2.1 - Key requirements for risk assessment (Jatuun et at., 2007)

Key requirements for the risk assessment
• Regular risk assessment of ICT and SCADA systems
• Involvement of resources from ICT, process control (SCADA systems) and supplier/contractor

The two requirements presented in table 3.2.2.1 ensures that the risk assessment is updated regarding the changing threat picture and that the knowledge and perspective from different individuals/experts is included. The intention of this activity is to identify what can go wrong during operations, in this case, what can go wrong during integrated operations. The risk analysis will help create barriers to reduce the probability of unwanted events and its consequences. These activities will help identify what incidents to prepare for and focus on, for example, rising cyber threats. In the case of integrated operations, which is a "borderless", diverse and virtual way of organization resources, it is important to generate a common risk perception. It is important to realize that each organization have a limited amount of resources and should prioritize the risk analysis to cover the most critical systems, and assess less critical systems as the resources allow. These systems need a vulnerability assessment which identifies any weaknesses that may present a threat to confidentiality, integrity, or availability of the system. Table 3.2.2.2 presents the activities that are commonly found in a risk assessment.

Table 3.2.2.2 - Risk assessment activities (Jatuun et al, 2007, page 19)

Risk assessment activities
1. Organizing and planning of the risk analysis
2. Description of scope - defining objects and relations to be analyzed
3. Identifying possible unwanted incidents (and if relevant – frequencies and consequences)
4. Description of risks and assessment of risk
5. Identify actions to reduce probabilities and reduce consequences of incidents – including contingency plans
6. Perform periodic assessment of the plan, and analyze relevant incidents to identify when the risk assessment should be updated

1. Plan and organize

As stated before in table 3.2.2.1 (key requirements for risk assessment) it is important to involve resources from the different disciplines in team discussions and risk analysis to ensure an assessment of the entire system and organization. Establishment of common risk perceptions is very important in a virtual environment such as in Integrated Operations (Jatuun et al, 2007, page 19).

2. Describe the scope

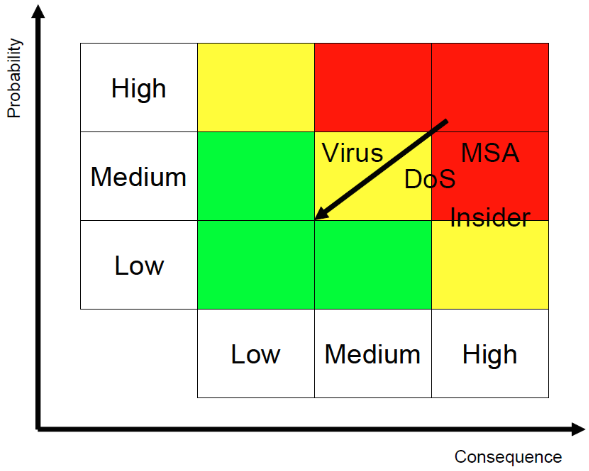
The scope identifies components and systems that are relevant for the analysis. This includes ICT, SCADA, networks and interfaces, as well as organizational and human factors.

3. Identify unwanted events and consequences

A vulnerability analysis reveals the weaknesses of the ICT and SCADA systems. Usually, there are obvious weaknesses that are easy to protect, but the analysis should also highlight the less obvious ones. In complex systems, it can be difficult to get a full overview of the system and the independent nature of such systems.

4. Risk description and risk assessment/evaluation

A risk matrix shows the relationship between probability, consequence and event. Figure 3.2.2.3 shows the risk regarding events such as virus, denial of service (DoS), insider, and missing situational awareness (MSA). The ideal situation would be if all of the events were in the lower left quadrant. The red quadrant shows what is not acceptable risk, which is based on the risk acceptance criteria of the organization. Security measures and controls can reduce the probability and/or the concequence, and reduce the risk in the direction of the arrow. Ideally, all measures would be impemented to reduce all risk, but it is not possible because of financial reasons and must be prioritized after criticallity. It is important to notice that the scale used in the presentation of the risk matrix may incluence the percived effect of the risk reducing measures.



Example of a Probability (Frequency) scale:

P-Low:	once every 10 years and upward
P-Medium:	Between 1 to 10 years
P-High:	Several times a year

Example of a Consequence Scale:

C-Low:	Up to $1,000
C-Medium:	$1,000 - $100,000
C-High:	$100,000 and upward.

Figure 3.2.2.3 Example of a Risk Matrix (Jaatun et al, 2007)

5. Identify risk reducing measures and contingency plans

Risk reducing measures are analyzed as to what degree it reduces risk. The measures are compared and the best alternative is chosen. As an example, the organization identifies an employee/supplier educational and training program is the best risk reducing measure. This program will raise the awareness of employees and suppliers and will help prevent and detect different types of cyberattacks. An incident response team is created and is responsible for developing a contingency plan for these events. Other measures are taken per the ALARP principle and as the resources allow.

6. Perform periodic assessment of the plan

Documentation and learning from incidents is important in improving the risk reducing measures and the risk assessment process. The periodic assessment of the plan needs to be taken seriously for prioritizing security activities.

Monitoring and Communication the Risk Level

Cyber-related threats require a level of preparation and most risk can be mitigated by having proactive activities such as communication with other organization. It contributes to perceive a realistic threat picture. Communication between organization contributes to monitor the threat level. For example, communication with ICT and security suppliers, authorities, such as NorCERT, and reviewing system logs, firewalls, and intrusion detection systems.

3.4.1 Types of Threats Agents

There are different actors with different motivations for performing malicious acts. The most noteworthy is that some groups are motivated by monetization of cybercrime and some are motivated by political, ideological, religious reasons. The groups' purpose and interest depend on what they want to accomplish in an attack. Marinos, Belmonte and Rekleitis (2016, page 55) presents eight different threat agents.

Cybercriminals

The cybercriminals utilize advanced methods, tools and software to profit from their illegal activities (Marinos, 2014; Marinos, Belmonte and Rekleitis 2016). This group is organized and has access to large resources, while being technically skilled. The motivation lies in monetization and "show-of-skill". This kind of highly organized crime is a large player in fraud and the collaboration enables the spread and depth of attacks. The methods and techniques evolve with the advancement in technology and business, such as e-finance, e-commerce, and e-payment. They often use ransomware that encrypts the victim's data, where the victim must pay to get his or her data back. Cybercriminals have created a business around cybercrime-as-a-service and can potentially be involved in espionage-as-a-service (Marinos, 2014; Marinos, Belmonte and Rekleitis 2016). The group is also a part of the development and delivery of malicious tools. The anonymization, encryption and virtual currencies, such as BitCoin, makes the cybercriminals difficult to identify and significantly delays or hinders detection.

Insiders

This group is identified as current and form employees, suppliers, contractors, consultants, business partners and customers (Marinos, Belmonte and Rekleitis 2016). These internal or external user have abused their system credentials or user rights. The motivation behind these acts are mainly monetization, revenge, or the convenience of bypassing the existing restrictive procedures. There is a potential risk that other threat agent groups will try to recruit insiders for their agenda. The insider are usually end-users, customers, cashiers, and executives. It is less likely that a system admin abuses their system rights (Marinos, Belmonte and Rekleitis 2016).

Online social hackers

This group has an important role in deployment of other cyber threats (Marinos, 2014). This threat agent is characterized as highly skilled in analyzing the behavior and psychology of their targets. The main tool is analysis of information, profiling of users via loggers, social media accounts, or breached data. The importance and frequency of phishing has increased and enables further exploitation (Marinos, Belmonte and Rekleitis 2016). The group are large players in identity theft and in collection of confidential personal data and user credentials.

Cyber Spies

Cyber spies are highly resourceful and have access to large budgets, whether it comes from a nation or a corporation (Marinos, 2014). This threat agent has been developing into a more resourceful group, with advancements in attack methods and the increased focus on cyber-physical systems (Marinos, Belmonte and Rekleitis 2016). The increasing threat impacts the way cyber-defenses are made in the future. Nations have developed their cyber intelligence capabilities and is motivated by gaining intelligence regarding state secrets, military secrets, and critical infrastructure, as well as information on a corporate level. This enables nations to potentially gain psychological and political advantages. There are no clear international cyber espionage policies and judicial guidelines that limits these kinds of activities.

There is a growth in corporate financed espionage that targets other corporation's information (Marinos, 2014). Generally, the corporations are involved in reconnaissance activities, intrusion, and data breach. The motivation is to gain business intelligence, steal competitive information, breach intellectual property rights, even cause sabotage or damage to competitors (Marinos, 2014). This group is also driven to buy services from other threat

Hacktivists

This groups seeks media attention for high visibility in their actions (Marinos, 2014). The common methods are DDoS, leakage and publishing information. The group is motivated by political ideologies, social injustice, and aims to influence political decisions. These groups are dynamic in the sense that their does not necessarily have a centralized organizational culture. Sometimes they consist of other threat agents, joined by a common cause, but with different motives. They can form during political decision or crises, and when there is assumed injustice or unfairness towards specific social groups. They spawn during riots, international sports events, and other major events with international attention (Marinos, 2014). In 2015, hacktivists focused on alleged wrongdoings, promotion of freedom of expression, and an open internet (Marinos, Belmonte and Rekleitis 2016).

Cyber Fighters

This group is identified as motivated citizens who possess significant striking power (Marinos, 2014). The group falls between cyber terrorists, hacktivist, and espionage. They are motivated by politics and will engage in sabotage if they feel their political, national, or religious values are threatened. The purpose of these attacks is to do harm, but also to attract media attention. Typically, these individuals are supporters of totalitarian regimes, and may act on their behalf (Marinos, 2014). This threat agent is growing and their attack methods are becoming more sophisticated.

Cyber Terrorists

This group is targets nations, society and critical infrastructure and engage in large-scale sabotage to inflict harm and promote violence (Marinos, 2014). Their objectives are motivated by influencing political decisions and actions based on their own politics or relations. Their main cyber related activities are communicating while avoiding state surveillance, recruiting new members internationally, and collect and distribute anonymous financial truncations (Marinos, 2014; Marinos, Belmonte and Rekleitis 2016). The growing threat in that this group is communication knowledge about malicious tools and attack methods. This group is a candidate to take advantage of the growing availability of cyber-crime-as-a-service.

Script Kiddies

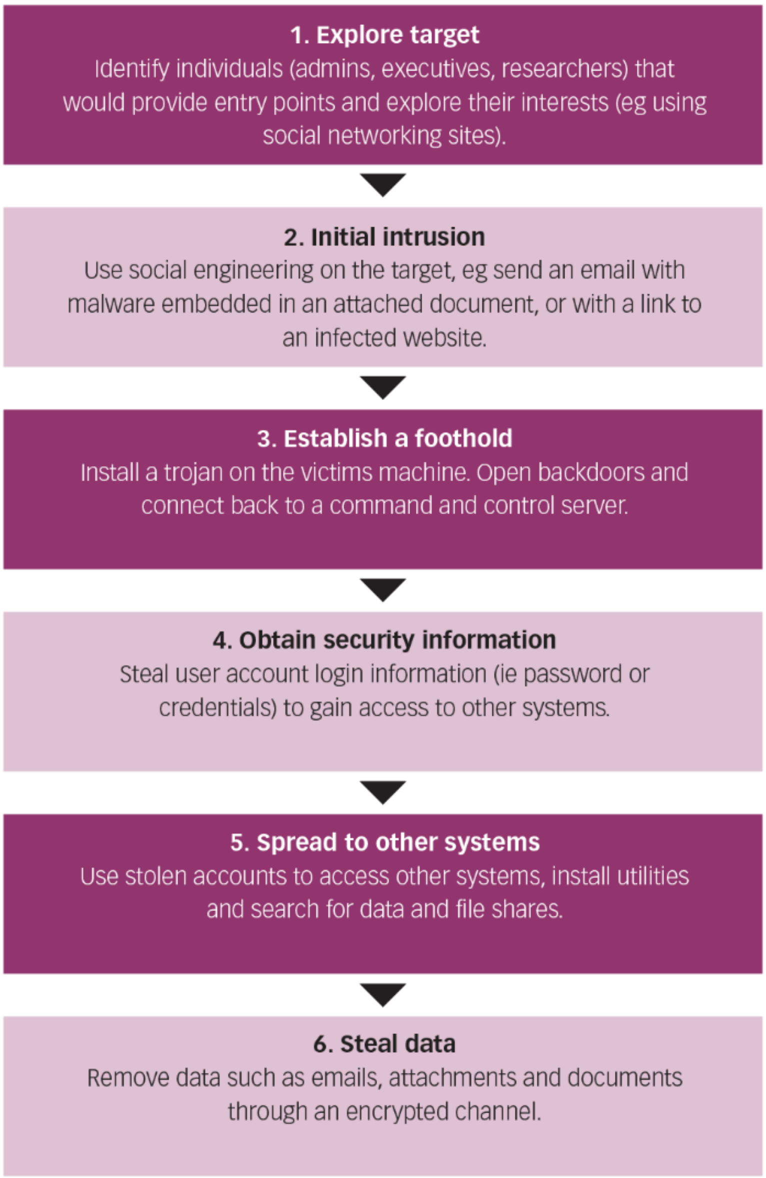
The group is identified as teenagers who are fascinated by hacking and the use of malicious tools (Marinos, 2014). They are motivated by achievements, show-of-skill, and hacking for the fun of doing it. A lot of information is available on the internet on how to perform cyberattacks and how to acquire malicious software. This group is susceptible for purchasing and utilizing malicious tools and services. The characteristics of script kiddies is that they are unpredictable because of their assumed low knowledge of consequences, overestimation of skill-level, and their lack of self-control. However, it is not expected a great impact from this threat agent (Marinos, 2014).

(In Addition) Non-malicious events

Digital systems are susceptible to human, organizational, and technological errors. Natural disasters such as fires, floods, hurricanes, and earthquakes can cause failure in systems and contributes to risk in digital systems, as well as, management decisions, technical and human errors.

3.4.2 Typical Attack Vector?

There are many ways of exploiting weaknesses in a system. The most successful exploits demand careful planning and research, as well as access to tools and software that can perform the preferred task. Figure 3.4.2 shows a typical schematic of a multi-stage attack.



1. Explore target
Identify individuals (admins, executives, researchers) that would provide entry points and explore their interests (eg using social networking sites).

2. Initial intrusion
Use social engineering on the target, eg send an email with malware embedded in an attached document, or with a link to an infected website.

3. Establish a foothold
Install a trojan on the victims machine. Open backdoors and connect back to a command and control server.

4. Obtain security information
Steal user account login information (ie password or credentials) to gain access to other systems.

5. Spread to other systems
Use stolen accounts to access other systems, install utilities and search for data and file shares.

6. Steal data
Remove data such as emails, attachments and documents through an encrypted channel.

Figure 3.4.2 - Typical schematic of a multi-stage attack, (Lloyd's, 2010, page 15)

Lloyd’s (2010) states that the attackers play the long game, with repeated attempts to successfully complete their objective. This means that the extraction of data can take many months, obtaining a little bit of information each time until the attacker can piece together enough to establish a foothold into the system. The attacks usually achieve the objectives using a mix of social engineering and malware. Specific individuals and information is targeted, and the attackers are careful to cover their tracks. Once a foothold is secured, the attacker spreads into other systems. The most sophisticated attack, often known as an advanced persistent threat (APT), follows the schematics of figure 3.4.2 (Lloyd’s, 2010).

3.5 Example of Incidents and Exposure

This section presents examples of incidents related to cyber risk exposure in digital systems. A combination of organizational, technical and human factors that contributes to the incidents. The first three incidents are related to management decisions and supply chain. Further, are examples of espionage, sabotage, ransomware and insiders.

3.5.1 Mongstad – Statoil – Outsourcing

Production stopped at the refinery at Mongstad, Norway, due to a typing error made by an Indian IT worker (Remen and Tomter, 2016). The IT services were outsourced by Statoil, the operator at Mongstad, to an Indian IT company. This put the safety and security at risk as an IT worker was supposed to complete maintenance on one of the servers. It was needed to be done as soon as possible due to some delays. A load of 50 000 cubic of gasoline was preparing to be transferred to a tanker. Due to a wrong keystroke, the IT worker accessed a different server (Remen and Tomter, 2016). This was a server he was not supposed to have access to. The server was labeled and the IT worker understood that he was not supposed to be there and restarted his computer. Even though, the system warned him about restarting. The IT worker soon realized that he had made a mistake when he started the computer and entered the server. He asked for help from his colleagues, which resulted in 22 unauthorized logins into the Statoil computer system and a failed attempt to stop the production from halting (Remen and Tomter, 2016).

This incident put many at risk. The refinery processes oil and gas which can cause fatal consequences if a technical error occurs. Luckily, when the computer controlled process halted, the control was recovered manually by the Norwegian workers. The loading could continue after a few hours. The consequences were reduced, and a small part of the gasoline mixture leaked into the sea (Remen and Tomter, 2016). No one was injured in the incident. The consequences could potentially be critical.

Underlying causes (Remen and Tomter, 2016):

- About 100 employees from the Indian IT company had “master” access to all of Statoil’s computer systems.
- The employees had access to stop the production, or the possibility to give other actors access, or make connections from the internet to the most critical control systems in Statoil’s production.
- A mismatch between competence and level of control in the tasks undertaken by the IT company.
- The IT company had full control over the operation of the digital infrastructure and the access control system.
- Poor supervision from Statoil.

Possible improvement:

- Strict access control and limited “master” access staff
- Outsourcing of tasks and function does not mean outsourcing of responsibility and lack of supervision.

- Awareness of outsourcing partner’s security measures and the risk adoption from using third party partners.
- Secure and document competence and knowledge in third party companies.
- Return the main control to internal staff, dispose of outsourcing of complete tasks and functions and go for a partial outsourcing.

Outsourcing contributes to risk exposure. In some cases, the outsourcing company is located a long distance away, in a different culture and talking a different language. This may contribute to misunderstandings and result in higher risk.

Ownership and Responsibility

It is important to have ownership and responsibility to the operation when outsourcing ICT functions. Outsourcing may be the most cost-effective alternative, due to several parameters, such as lower-wages, and less operational expenses and investment costs. However, there must exist a governing supervision with satisfactory expertise in the organization, such that the organization controls the outsourcing. If this does not exist, the organization is unnecessary exposed to risks. It should also be preparatory work, in systematic risk and vulnerability assessments before the contracts are made. Requirements and controls for information- and cyber security must be clarified in the contract. Evaluation of performance and quality should be made at a relevant frequency, as well as strict control of user access and admin rights. In some cases, it is possible to perform manual procedures, when the digital system fails. It proved to be the saving measure for this operation.

3.5.2 Helse Sør-Øst – Outsourcing

In the spring of 2017, IT workers in Asia and Eastern Europe had access and extended rights to the Helse Sør-Øst's computer system (Tomter and Remen, 2017a). They access to sensitive information and had the opportunity to change the journals of 2.8 million Norwegians. Thus, had information regarding births and abortions, mental health problems, drug use, and similar. This occurred in relation to a decision to outsource the ICT infrastructure operation from Sykehuspartner to Hewlett Packard Enterprise (HPE) (Tomter and Remen, 2017a; 2017b).

This is a great example of exposure created by management decisions. Patient information was accessible by foreign IT workers because of a lack of technical understanding, governance, and assurance. Helse Sør-Øst lacked a way to enforce the contractual requirements. For example, the requirement that all data centers and storage of sensitive information must be located in Norway. As well as, the security requirements of remote operation of these facilities. Helse Sør-Øst should have made sure they had access to all the information regarding HPE's use of sub-suppliers, contractors, and security practices. Helse Sør-Øst should have performed substantial risk assessments prior to this decision. The financial advantage of outsourcing to a low-cost nation, should not compromise security and privacy. Once international locations are introduced, so are local regulations and requirements for particularly security. For example, an employee may fail the background check in Norway, but pass in another country and organization. The responsibility falls on Helse Sør-Øst to make sure that Helse Sør-Øst and its associated partners, suppliers, etc. follows the Norwegian requirements for information and cyber security, in this case, the security of sensitive information.

3.5.3 It's Learning and Feide – System Error

A security breach was detected in the learning platform It's Learning 17th march 2017. Students and teachers had access to other users' accounts. Personal information was compromised and accessible such as grades, messages between teachers and students, and remarks. After the problem was detected, the learning platform was shut down. It's Learning is a digital learning platform used in primary- and secondary schools, high schools and universities. About 300 users of a total of 17 000 users were affected by the incident. The incident was only reported affecting schools in Rogaland, Norway. The error proved to be a system failure and not a cyberattack. The time between incident occurrence and detection was 3 hours and 25 mins. Quotes from the news articles:

- *"It would appear that users are duplicated, so they have got similar credentials. But we have four people who are working to resolve this, and they are going to work through the night to the problem is identified and resolved"*, said the IT manager Odd Bård Risvoll from Rogaland municipality after the incident was known (Heimsvik, 2017).
- *"I must emphasize that the fault lies with us* (Feide host organization)*, not with It's Learning. There have been corrupt data in our user database. This is again an error in an underlying system"*, said Risvoll after they had identified the error (Østbø, 2017).

Vulnerable

"All schools in Norway login via a database solution called Feide, owned by the Directorate of Education. We also have another management supplier named IST. Now we examine where the fault lies, whether it is with us or one of the other", said Arne Bergby CEO of It's Learning (Heimsvik, 2017). The organizations use different login solutions to reduce the amount of user accounts and password. For example, the users of Feide register once in the host organization. This means that the host organization provides the user with one username and password, and are responsible for maintaining the user's personal information (Feide, 2017). This could be universities, colleges, municipalities, counties, and private schools. The user, for example a student, can login via Feide to get access to the school's It's Learning network. In this case the Feide database is operated by the municipality of Rogaland, who's system failed to execute access control and exposed users and sensitive information.

This incident shows that an error of one systems can transfer and affect other systems, in this case from organization to organization. There should be barriers in place to prevent this from occurring. Digital systems connected beyond organizational boundaries causes vulnerability. The growing interconnectivity and complexity of digital systems makes identifying the error difficult and they are often not visible or connected to the physical world, for example, as a control system for a machine or a production line. This demands an experienced and competent staff to identify the root cause.

Consequences

This event occurred late on a Friday, which means that the school is closed. The shutdown of It's Learning in a week day would mean that the schools would suffer more consequences. The schools depend on this system, and the closes redundancy for is to utilize blackboards, direct communication, and books, although, a lot of information, such as lectures and other data, would be temporarily lost. If this was an offshore oil platform, it would be unacceptable. A stop in production would have severe financial consequences and the time to detection and identification of the incident would potentially put people in danger. Nonetheless, the digital systems connected to the learning platform, and the learning platform itself, should be regarded as important and protected thereafter.

Learning culture

Risvoll stated that he could remember that a similar incident had occurred a few months prior to this event, but that he could not remember where or in what organization or system the error originated. It is important for organizations to learn from past events, if they don’t, the event will continue to occur. This particular event shows the importance of information- and experience-sharing. The organizations have different systems, competence, etc., and their vulnerabilities can affect each other. However, they also possess experience that could benefit other organizations. The incident should be assessed, discussed, and distributed between the involved parties, so that they would be better prepared for a similar event in the future. A good learning culture could reduce the number of black swans.

3.5.4 Night Dragon - Espionage

Night Dragon is an example where social engineering, spear-phishing, SQL-injection, and exploits in commercial operating systems and remote administration tools (RAT) were used to gain access to sensitive information regarding field bids, operations and project-financing in the oil and gas sector. It is believed to be originating from China and it was detected in 2009 after a series of attacks on several companies. Companies in USA, Taiwan, Kazakhstan and Greece were affected (Kambic et al., 2013). The attacks were organized and followed a specific series of steps to gain success (McAfee, 2011; Kambic et al.,2013):

1. Compromising laptops, accounts and gaining access to the organization network.
2. Uploading tools to gain further access to databases.
3. Access sensitive documents.
4. Upload malware to exfiltrate sensitive data.
5. Move laterally and continue the process.

A simplified version of the method from McAfee's report (2011): It started with an attack on the companies' websites (SQL-injection) and the use of social engineering and spear-phishing to gain additional access to emails, internal laptops and servers. Once they had access inside the system, they could upload RAT malware and conduct additional reconnaissance and system compromises to harvest confidential data. The data was later copied from the compromised hosts and servers. Due to the SQL-injection and the spear-phishing attack they could penetrate the targeted company's defensive architectures and conduct reconnaissance of targeted company networked computers.

The attacks evaded detection of standard security software and network policies due to the simple method of using standard administrative credentials. Many of the security vendors have identified unique signatures related to the Trojan. The attack can now be identified through looking at host files and/or registry keys, anti-virus alerts, and network communication (McAfee, 2011).

Techniques

Social engineering is a way of manipulating humans to divulge information by impersonating as an employee or a legitimate person from the system in need of sensitive information, such as a password (Bawane & Shelke, 2014). This is a method that is difficult to detect. In an inattentive or unaware moment, it is easy to provide information that should not have been given. It may also seem distant that anyone would impersonate or try to deceive, trick or access information if the individual, or the victim, is unaware that this is common or possible. This is where awareness campaigns play an important role. Spear-phishing is, for example an email, that appears to be from an individual or business that is familiar, but contains a link or asks for sensitive information (Norton, n.d.). A SQL-injection gives the hacker the ability to extract and manipulate data from a web application's data (such found in websites) (Imperva, 2013). RAT malware tools provide complete remote administration allowing a remote individual to control the affected system, by screen and webcam spying, keystroke logging, mouse control, access to file/registry, etc. (McAfee, 2011). As security vendors and software learns from incidents and become more sophisticated, well known Trojans and viruses can be picked up by the standard security system. But, this requires a learning process and considerable analysis to identify signatures and patterns in the attack.

A growing and organized threat

McAfee (2011, page 13) states that "*well-coordinated, targeted attacks such as Night Dragon, orchestrated by a growing group of malicious attackers committed to their targets, are rapidly on the rise*". The attacks are getting more frequent and the potential damage is substantial. Many organizations may still think that "*it will not happen to us"*, but the truth is that the attackers does not discriminate on sector, size, or technology. In some cases, an attack against a small company can be a training ground or for monetization. The attackers go beyond the local, military, or governmental targets and seek out global and commercial organizations. Increasingly these attacks are about stealing specific data and intellectual property, rather than sabotaging machines and technical systems (McAfee, 2011). This leads to a need for prioritizing and protecting intellectual property. Performing value assessments and the identifying vulnerability or exposure associated with the values are vital for recognizing weaknesses and consequences, and identify potential targets in the organization.

This step by step tear-down of a system starts with the exploits of the vulnerabilities the top-layers of a system and the manipulation of humans. Once the hackers have access to critical servers and systems, there are many tools available for the hacker to further compromise the system. The McAfee (2011) report mentions that there were used freely available "hacker" tools from Chinese websites. These examples of cyberattacks shows that the availability of harmful tools and the sophistication and structure of cyberattacks causes a large threat to any company with valuable information. It displays a reason for investing in cyber security and secure systems, and the importance of spreading knowledge about spear-phishing and similar scams to employees and create an awareness throughout the organization. This would help reduce the risk of unwanted exposure and risk.

3.5.5 Attack on Several Norwegian Authorities

In January 2017 was PST (Norwegian Police Security Service) alerted regarding a cyberattack on several Norwegian authorities. It was believed that the group called APT29, associated with the Russian, government was behind the attack (Jørgenrud, 2017). The targets were PST, AP (laborer's political party), the foreign ministry, the Norwegian defense, Norwegian Radiation Protection Authority, and a college (Skjetne, 2017). An email impersonating Harvard University with an email attachment related to the USA election and hacking of the democratic party, was a spear-phishing attack containing malicious software (Jørgenrud, 2017). However, the attacks were reported as unsuccessful and could not access sensitive information.

Steal information for weapon of mass destruction

In a letter from the Ministry of Education (KD, 2017), sent to numerous universities and colleges after the event of January 2017, expressed concern about the increasing threat from foreign actors. Informing that actors can influence, retrieve and counterfeit information, and identify staff and their personal information. A cyberattack of this nature can be an integral part of foreign nations' intelligence operations in Norway. PST states that it is one of the most serious long-term challenges today (KD, 2017). The main purpose of such an attack is to gain knowledge about special research topics and use it in their own favor. The expressed concern in the letter was that educational and research institutions are susceptible to attempted illegal transfer of knowledge and technology that can be used to produce weapons of mass destruction, their means of delivery, or general military capacity building (KD, 2017). The perpetrators in these attacks, as seen in January 2017 where the wrongdoers pretended to be a research institution with a legitimate intention, prove difficult to identify. KD and PST states that to prevent intelligence and illegal transfer of knowledge it is important to be aware of the value in the organization, and what knowledge the organization possess, which may be of interest to foreign states (KD, 2017). Furthermore, KD and PST recommended that the given organizations assess the changes to threat level and how these affect their own risk and vulnerability analyses.

The attack and the expressed concern of the growing threat show that all kinds of organizations are vulnerable to cyberattacks and must assess their values that can be of interest to others. Spreading propaganda and fake news, fabricating and planting fake documents, exposing documents and governmental "secrets" can damage the function of a government and collaboration and trust between countries. The numerous public and governmental organizations possess information that is of interest for foreign intelligences. Universities and colleges research advanced sciences and technologies. This can be valuable information for nations or private actors. Knowledge about weapons of mass destruction and advanced weapon systems, for example nuclear weapons, is of high value and can be attractive target for malicious actors.

3.5.6 Stuxnet – Vulnerabilities in ICS – highly sophisticated attack

Stuxnet is a great example of how sophisticated cyberattacks can be. Industrial control systems are vulnerable, even when its network is isolated from other networks, a so-called "air gap". Stuxnet was a very resourceful and complex attack that targeted a specific set of Siemens control systems. These Siemens components were used to control the centrifuges in Iran's uranium enrichment plant (Mueller and Yadegari, 2012; Falliere, Murchu and Chien, 2011). It was discovered in 2010, after it had potentially done damage to about 1000 centrifuges in the Iranian plant in Natanz. The resources needed to create it points towards a resourceful creator, such as a country. Allegedly it was made by Israel and/or USA with the intent of sabotaging the Iranian production.

The attack is most characterized by the behavior of the virus. It analyzed the systems it encountered, seeking out a specific signature of the Siemens control system components (PLCs) found in the Iranian plant. Therefore, it was not harmful for any other infected system that the specific configuration of Siemens components. It had an enormous capability to duplicate and spread, for example through USB flash drives. The virus would stop spreading after it had infected three computer/units and it was programed to stop spreading itself after June 24 (Mueller and Yadegari, 2012). It could auto update the virus-version existing in the system if a newer version encountered the same system. It is assumed that the outside contractors may have transported an infected flash drive in to the plant and then infected the control computers. It was not detected at first because of the sophisticated learning system. The overtaking of the system was impossible for the operators to notice. It would learn the system behavior before it would start sabotaging the production by using a PLC rootkit.

Exploits

The tools in accomplishing this attack includes zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface (Falliere, Murchu and Chien, 2011).

How to prepare for zero-day exploits and black swans

A zero-day attack takes advantage of a non-publicly known vulnerability in a system. It is a zero-day attack because it leaves the victims with zero day to prepare this particular attack. Hence, a zero-day attack is a black swan. However, the antivirus industry can quickly update their products once they have identified a signature for the specific attack. This means every product should be able to detect and prevent it from doing any further damage. The anti-virus software vendors compile a library of different malware signatures, then they can cross reference the signatures with the local system of the user (Hammarberg, 2014). These libraries are constantly updated, which means that the user is advised to frequently update their security software. It is difficult to prepare for a vulnerability that no one or only a handful of people knows about. However, the techniques used by the security vendors reduces the exposure time and hopefully the consequences of such an attack. The two main challenges related to zero-day exploits are knowledge and resources. The resources available to an organization have an impact to its ability to defend itself. Having access to knowledgeable security personnel, software, and hardware could have positive impact on the consequences. Characteristics of different size of organizations (Hammarberg, 2014):

- Small organizations

Smaller organization are considered to have less formalized policies and procedures in regards to security. They are more exposed to black swans (unknown to some, but known to others). They are unaware of the potential risk from zero-day exploits and fail to see the importance of defending against them.

- Medium/large organizations

The larger the organization become the more formalized the policies and procedures become. They have greater knowledge of the risks, and are more likely to try to defend against them. They are more likely to implement a better defense in depth strategy using various techniques to defend against zero-day exploits. The ALARP principle should be followed by all organizations. However, it is dependent on the available resources, and that the implementation of a security measure does not cause an unreasonable financial consequence. Resources play an important role in to what extent the organization can cover or be aware of black swans.

Testing for infection

All equipment brought in by contractors and suppliers should be tested for infection. As proven by the Stuxnet virus - it is a very effective way to infect a system. It could be unknown to the supplier that their system is infected, and due to low security procedures in the supplier's organization, they are unable to tested their equipment for virus. As a rule, all staff and hired personnel can carry a USB flash drive, being unaware that it is infected with a virus. Consequently, some systems should have strict physical barriers and significantly higher security measures. It would be beneficial if the organization could exercise control over external hard drives and tools the employees use, for example by having digital identification for each hard drive and owner, but this may be difficult and too costly to perform.

3.5.7 Pipeline in Turkey - Sabotage

In 2008, a crude oil pipeline operated by BP exploded outside the town Refahiye in Turkey (Robertson and Riley, 2014). The Baku–Tbilisi–Ceyhan (BTC) pipeline was monitored by sensors and cameras along its 1768 km long range, from the Caspian Sea to the Mediterranean. However, its monitoring system failed to detect the explosion and the operators was not aware of the situation until 40 minutes late when a security worker saw flames. The Turkish government stated that the explosion was due to a malfunction, but the Kurdish separatists claimed credit for the event, some claim that the Russian government had motive. It is still not clear who was behind the attack.

The chain of events as stated by Robertson and Riley (2014): The surveillance system had control over critical indicators, such as pressure and oil flow. It was sent via a wireless monitoring system and by satellite. A large amount of surveillance video was erased by the hackers, except for one infrared camera connected to a different network. The camera show two men with a laptop computer walking near the pipeline days before the explosion. The investigation found that the hackers had gained access to internal networks via the surveillance cameras' wireless connection. The hackers identified the alarm-management-software and place a malicious program inside the software. The perpetrators had access to the industrial control system that controls the valves along the pipeline. This enabled the hackers to increase the pressure to dangerous levels without setting off any alarms. The satellite signal failed and the infiltrators tampered with the units used to send alerts about malfunctions and leaks back to the control room. Prior to the event, the operators had been warned by experts that the lines could be blown up from a distance, with the use of cyberweapons.

Oil and politics

BP lost about $5 million a day during the leak, which is a large financial loss. The attack is an exhibit of what capabilities and what damages is possible through the computer. Oil and politics play an important role in explaining why these attacks may occur. Countries and corporations have interests in manipulation the oil market and the dependency some countries have to a steady supply of energy. Such an attack can also be used in weakening a country's ability to function, prior to an offensive military attack. The access to valuable resources can create dispute between countries. To a point where there is a near-war atmosphere and the parties tries to influence the other part's success.

Transportation and long distance monitoring

When the end-product or the main resource is obtained, it may be easy to forget that it needs to be transported to the customer. The transportation phase may receive less attention that the actual production or manufacturing phase. The BTC pipeline is long and it requires a large monitoring system with many components over a large distance. The operation and quality control of the safety- and the surveillance systems may prove to be difficult considering that the pipeline covers such a long distance and passes through several countries. An operation like this requires high quality communication and procedures to maintain control.

3.5.8 WikiLeaks - Insider

WikiLeaks is a controversial international non-profit organization which publishes leaked information (Restad, 2015). It functions as a whistleblower that want to share important information to the public. This information is usually leaked from classified sources, such as the US military. In 2010, Chelsea Manning leaked classified information to WikiLeaks (Restad, 2015). She worked for the US military as an Army intelligence analyst with access to networks and containing secret information (Zetter and Poulsen, 2010). The information leaked contained a video of a US airstrike, a classified document containing an evaluation of WikiLeaks as a threat, and 260 000 classified US diplomatic telegrams. The data was smuggled out using a CD-RW, a rewritable CD.

The insider threat agent can be motivated by many factors. In this case, the insider was probably motivated by her conscience, believing that the actions of the US military were wrong and that someone needed to blow the whistle. The moral issue of this event, whether it was a right decision or not, is not discussed. The more important issue is that employees can, if motivated, misuse their system access. This event occurred many years ago and there are modern technical barriers in place for reducing the risk of successful insiders. System logs and strict access control will limit the range of system users. As the insider threat is discussed, the awareness of the potential user risk becomes clear. It changes from organization to organization and encompasses a variety of reasons for motivation.

3.5.9 WannaCry – Ransomware

Wanna Decryptor, or WannaCry, is the name of the ransomware that roamed during May 2017. NSM states that it is the largest cyberattack they have seen at a global level (Omland and Wernersen, 2017). The kind of cyberattack encrypts files on computers and hold it for ransom. It utilizes an exploit in Windows, a commonly used operating system, and has attacked approximately 57 000 users in 99 countries (Omland and Wernersen, 2017). Among the victims were Norwegian hotels, British health care services, Russian government, and a French car manufacturer. The virus is a result of the increasing threat from cybercrime.

The threat actors found a technological exploit and made a powerful malware which was distributed worldwide. Security technology companies and the software manufacturer, Windows, found a solution to the problem and created a patch. This meant that any individual or organization that updated its system with this patch, would be safe. Others, that ran unsupported software or did not update their system, would still be vulnerable. Patching routines plays an important role in these scenarios. And, if the ransomware attacks before there is an available patch, it is important with backups and recovery systems.

3.6 Exposure and Vulnerabilities

Exposure and vulnerabilities are dependent on many factors. This chapter will describe the different factors that affects the organization's exposure and vulnerability. This chapter will look at some vulnerabilities which have been emphasized by other reports.

3.6.1 Lysneutvalget - Vulnerabilities in the Value Chain

The focus on digital infrastructure in the public sector has led to a series of committees that evaluates the security and the risk of the change process, threat picture, the function and scope of legislations, and the organization's security capabilities. The digital transformation and technological change process affects how organizations operate and are structured. Both private and public organizations have a new need for knowledge and competence the following years. Due to the demand for new competence, there will be a certain uncertainty and instability in the organization's operation and structure in the creation and establishment of new procedures, requirements, structures, etc. The operating organizations and the different governmental authorities, such as the Data Inspectorate (Datatilsynet), Railway Inspectorate (Jernbanetilsynet), Ministry of Transport and Communications (Samferdselsdepartementet) etc. face a challenge in gaining knowledge and creating requirements for secure operations for the given sector. In this transformation process it is important to collaborate and communicate between the relevant parties and agree to a reasonable future direction. It is a challenging process that will take time and involves many parties. Different sectors may face the same challenges, risks and have the same vulnerabilities, therefore information sharing across sectors may lead to better procedures and form a national standardization of information and cyber security. Risk and vulnerability assessments and distribution of awareness are key tools in facing the challenge. Lysneutvalget (DNV GL, 2015) acknowledges the dependency, risk and vulnerability related to digital technology in the oil and gas sector. Lysne utvalget (DNV GL, 2015) present different digital vulnerabilities connected to different parts of the value chain, as are being described in this chapter. The observations include organizational, technical and human factors.

The exploration phase is driven by information and data. The data is the basis for future projects, decision-making and revenue. It is valuable resource for the organization. It requires experts to interpret the data and create value from it. The data is subjected to manipulation or deletion. This requires a strict information policy related to access control and protection of the data.

The field development phase is characterized as a process that has many involved parties and actors. There are many contractors, suppliers and sub-suppliers that can affect parts of the development. Information is distributed among the involved parties in the building process. This information can be of great value for the threat actors. Also, the hard competition among the suppliers and contractors makes this phase subjected to corporate espionage. The knowledge of field development in Norway is a valuable competitive advantage for international and national projects. This knowledge is sought after and needs to be protected. The exposure to digital vulnerabilities are mainly due to the lack of attention and training of employees, lack of routines for classification and treatment of sensitive information, and lack of protection and updating of software (DNV GL, 2015). Sub-supplier may have different security cultures that has the potential to affect the contractors. DNV GL (2015) states that the consequences of an unwanted event, cause by digital vulnerabilities, mainly is financial for the oil and gas business.

The production phase utilizes operational equipment such as command and control systems. These systems are changing from being proprietary systems and networks to internet-based off-the-shelf technology. The main challenge is that some automation and control systems are connected to the internet. This causes an exposure to digital vulnerability that criminal actors may use. An attack on these systems may result in major consequences, due to loss of control. Long distance monitoring and shared networks from neighboring platforms may be subjected to eavesdropping and different kinds of vulnerabilities (DNV GL, 2015). The joint network solution is a way of developing a redundancy within the network. The two cultures, information technology (IT) and operation technology (OT), are different and may cause poor understanding and communication between the two. The command and control systems are operated in-between these two cultures and may suffer from the different prioritizing of the two cultures – confidentiality in IT and availability in OT. Upgrading of old equipment is a challenge in this sector. Many installations have a long lifetime and may be outdated and may lack the same level of build in security as new equipment. Documentation of equipment and modules (or containers) is a challenge, due to the difficulty of having an overview of safety and security standards. Security standards from different manufacturers and countries may be different. DNV GL (2015) states that the consequences of an unwanted event caused by digital vulnerabilities in this phase will be of a financial nature, but can also affect the organization’s reputation. In the event of a sabotage or terror, the consequences will potentially be loss of life and environmental damage, due to the use of flammable and explosive resources.

The transport phase is characterized using long distance pipelines and tankers. The oil and gas distribution network exports a valuable resource. Large parts of Europe are dependent on importing oil and gas from Norway. The pipelines have a potential for sabotage and incidents. The command and control systems that controls the flow in the pipelines are subjected to digital vulnerabilities. In accordance with DNV GL (2015), the consequences of an unwanted event cause by digital vulnerabilities be financial, loss of reputation, potential for loss of life and environmental damage, due to the flammable and explosive material.

3.6.2 Lysneutvalget - Special Topics

Lysneutvalget's report discusses special topics beyond the value chain. These topics expands cyber security beyond the technological aspect and includes organizational aspects.

Dependent on power supply and communication

Due to environmental concerns, onshore electric power supply has been suggested as an alternative to the offshore turbine power production. It has been introduced in a several installations and it is required to present an overview of the costs of moving the power production onshore (DNV GL, 2015). Because the power requirements for offshore installations is substantial, the demand for power production and infrastructure on land increases. Any power loss or outage will affect the production offshore, unless redundant systems are in place. The power distribution network and power balance on land is affected if a large power consumer is connected to the same network. This presents a growing dependency on land-based power production and power distribution infrastructure, and creates a requirement, and is required by regulations, for secure operation and emergency response for these facilities. However, the facilities that supply the offshore installations are not part of this regulation (DNV GL, 2015).

Fiber optics, and to some extent radio line and satellite communication is the main infrastructure for network communication on offshore installations. It is considered to lack redundancy and demands several independent solutions to reduce the risk of failure.

A well-functioning safety and security culture

The safety and security culture of the organization represents the organization's ability to defend and manage digital threats. Awareness, knowledge and a general understanding of digital vulnerabilities are fundamental barriers. DNV GL (2015) recognizes that in the event of cutting costs due to difficult economic times, the safety and security culture may be affected. Loss of knowledge, competence, and resources can affect the general awareness and understanding of risk and vulnerabilities, as well as the prioritizing of maintenance and investments in security systems. The recent financial crisis in the oil and gas sector may influence the safety and security culture of the organizations.

Collaboration between business sector, stakeholders and authorities

The oil and gas sector is governed by many rules, procedures and authorities. These organizations face the same challenges related to digital vulnerabilities and digital threats. The sector is in a change prosses in which digitization presents a need for new knowledge and understanding of digital risk. For example, it is not established a formal procedure for alerting of digital threats from authorities to the corporations in the oil and gas sector (DNV GL, 2015). The organizations themselves must establish communication with the security authorities. A detailed procedure for communicating the threat picture should be established in collaboration between the organizations to find the most reasonable way of informing the right individuals and organizations (DNV GL, 2015).

International collaboration

There is a need for international collaboration and representation from the oil and gas sector related to digital threats and vulnerabilities (DNV, 2015). Digital threats and vulnerabilities are common for several different sectors. This presents an opportunity of sharing experience and information, and learn from other sectors, as well as national and international organizations.

Emergency and incident response

The establishment of an emergency and incident response plan is important. Lysneutvalget (DNV GL, 2015) found that there are some common trends in the oil and gas sector:

- Lack of emergency plan for digital vulnerabilities.
- More focus on fire and explosions that digital vulnerabilities.
- No procedures for disconnecting internet and block connections between the organization's IT networks and the production network.
- Lack of ICT emergency incident practice.
- Authorities (PTIL and DSB) are mostly focused on managing physical incidents, not on preventing and reducing digital vulnerabilities.
- The consideration of establishing their own CERT or joining other sectorial CERTs.

The focus on physical emergencies may overshadow the need for ICT and cyber related emergencies. These two different domains need to be assembled and viewed as one. The cyber incidents can be connected to the physical domain and vice versa, if for example a fire affects ICT equipment and causes greater damage to the system.

Unclarity in legislations and supervision

The Norwegian authorities have an executive role in controlling the sector. Organizations are responsible for complying with the security targets or scorecards. The Norwegian model is based on an overall audit that does less direct supervision when it comes to digital security management (DNV GL, 2015). The legislations regarding HSE is not directly related to digital threats, but does include digital security. This is where there are ambiguities and lacks clarity and an overall vision. The supervisory authorities are responsible for safety, security, emergency preparedness and work environment of its industry. Therefore, it they are also responsible for ensuring that their industry has the proper ICT defenses. The authorities should affect the sector through research projects, awareness campaigns, information about the threat picture and establish forums and meeting grounds for knowledge building and experience sharing, and stimulate for using preventive measures. Smaller actors can benefit from this by gaining experience from larger actors.

3.6.3 NSM - Human, Organizational, and Technological Vulnerabilities

The vulnerabilities can be divided into three main categories: Human, Organizational, and Technological (NSM, 2016b). This perspective on vulnerabilities will be carried through the rest of this thesis. It is common in root cause analysis to highlight these three categories, and therefore, it makes sense to look at follow the same structure for vulnerabilities.

Human Vulnerabilities

The human vulnerabilities can be categorized into these main parts - competence, compliance and awareness. NSM's (2016b) example on human vulnerabilities are:

- *Competence*
    - Not understanding why (cyber) security is important.
    - Not understanding how each employee can contribute to the security culture.
    - Poor deviation reporting culture.
- *Compliance*
    - Lack of guidelines related to social media.
    - Lack of control mechanisms which enables employees to do great damage undetected.
    - The importance of security is not motivated by leaders.
- *Awareness*
    - No distinguishing between work and private.
    - The use of private devices in the organization's network.

The employee ICT competence is the foundation for understanding why security is important and how each employee can contribute to the security culture. If the security procedures are not being followed, then they are to no use. This is also linked to how the security culture is in the organization and if the employees feel that following the security procedures is important or creates some sort of value. Awareness is the cumulative effort of competence and compliance. Once employees understand why security is important and how each employee can contribute to a well-functioning security culture, then the organization has limited the human vulnerabilities.

Organizational Vulnerabilities

The organizational vulnerabilities can be categorized into security framework, risk management, leadership engagement, and emergency preparedness. NSM's (2016b) example on organizational vulnerabilities are:

- *Security Framework*
    - Unclear roles, responsibilities and reporting lines.
    - Lack of measurable security targets and requirements
    - No requirements for security competence.
    - Lack of patching routines.
    - Lack of competence for security technology purchase.
    - Lack of internal evaluation of security activities and the review of the security condition of the organization.
    - Lack of managing and updating user system and physical access.
- *Risk Management*

    - Lack of threat overview.
    - Critical functions and components are designed as highly dependent on one other components to function.
- *Leadership Engagement*
    - Security activities does not receive enough funding.
    - Poor overview of competence needs related to security.
- *Emergency Preparedness*
    - Lack of incident and response functions.
    - No emergency response plan for managing cyber security events
    - Lack of emergency drills.

Cyber security should be an integrated part of the organization strategy, framework, and risk management. Managers can motivate employees to play their part in the security culture and encourage security procedures compliance. Managers and shareholders can in the same way as employees can lack understanding for why cyber security is important. This can influence the cyber security resource allocation. The lack of a cyber security framework, or an information security framework in general, will make the security efforts and activities scattered and lack an overall strategy or objective. The lack of clear roles, responsibilities and reporting lines will make security efforts highly ineffective and might even work against the security culture. It is the organization's responsibility to set requirements for ICT security competence, security targets, and security routines, and enforce those requirements. Risk management is important in understanding the threats and vulnerabilities of the organization. Risk analysis in cyber security should be an active, regular and knowledgeable activity, with the whole organization in focus. The lack of a rehearsed emergency response plan can contribute to enchaining the consequences. ICT emergency response may receive less focus than the physical events such as explosion or fires, but they can produce critical consequences for the organization, as seen in chapter 3.5.

Technological Vulnerabilities

The technological vulnerabilities can be categorized are physical, user & access control, and system technology management. NSM's (2016b) example on technological vulnerabilities are:

- *Physical*
    - Lack of security zones.
    - Critical equipment is place in a low-level security zone.
    - Lack of physical security in buildings, such as windows, doors, etc.
    - Long reaction time for burglaries.
    - Failure to implement alarm sensors and camera monitoring.
- *User and access control*
    - Lack of system access control.
    - Failure to remove access cards from individuals who no longer have access.
- *System technology management*
    - Lack of software and hardware upgrades.
    - Failure to implement system security patches and updates.
    - Lack of system traffic logs.
    - Failure to detect unauthorized users.
    - End-users are assigned admin rights.
    - Failure to stop unauthorized programs and software.

- Failure to use client-firewalls.
- Incorrect use of disk encryption.
- Lack of systems and network overview.
- Failure to use security systems and security programs.
- Inability to detect unwanted network activity.

The technological vulnerability is driven by ICT competence and threat knowledge. Competence and knowledge makes the risk analysis produce better threat overview, and the ICT security personnel understands how security technology, physical security works and how it affects the security of the organization. Old, unsupported software contains vulnerabilities that will never be patched by its manufacturer. Therefore, it is important to upgrade old ICT infrastructure, software and equipment. Failure to implement strict patching routines can expose the system for unwanted vulnerabilities which the threat actors are aware of.

An organization's business can involve many users from employees to suppliers. These users must be given access, both to buildings and networks. This is where the user account and access control is critical. An outdated user access list can make unwanted users to gain access to buildings and networks. The failure to have regular updates to the user account and access list, can produce unwanted events. System traffic logs can work as a platform for investigating unwanted events and incidents. A scenario could be that an incident has occurred and been stopped, but the organization does not know how it managed to penetrate the system. This leaves the organization in an awkward and uncertain situation.

Additional Organizational Vulnerability – Third Party Management

The use of third parties carries risk because of the existing vulnerabilities of the third party. It can be viewed as a risk adoption, where the customer adopts the risks of the supplier. The same vulnerabilities which are found in the customer's organization, can be found in the third-party organization. IIROC's (2016) examples of third party vulnerabilities are:

- The location of the third party implies different laws and regulations.
- Third party's history of data breaches.
- Additional outsourcing or sub-suppliers used by the third party.
- Security quality and performance history.
- Inadequate incident response plans.
- Inadequate security awareness and culture.
- Lack of system recovery functions.
- Poor use of encryption
- Lack of vulnerability testing and penetration testing.
- Lack of reviewing the possible risks of letting a third party having access to sensitive information or critical functions.

How the organization chooses to manage its service provides and suppliers affects the organization's role or ownership to the given service or operation. The foundation for third party management is the contractual requirements and the performance is dependent on the organization's ability to enforce those requirements. This is also described in chapter 2.2.5.

Chapter 4 - Cyber Security

4.1 Definition

Digitalization creates increased connectivity and dependency on ICT and digital systems. The increased connectivity increases risk. Cyber security is the natural response to this risk. Critical functions conducted by governments, authorities, intelligence services, and companies can be exposed to cyberattacks because of its importance. The impact the digitalization has on the society has increased its vulnerability, especially on information-, communication-, and industrial control systems. This creates a need for cyber security in public and private organizations.

This has caused a global attention to the rising threats and cyber security. Cyber security is not only a problem for ICT, but it includes all aspects of an organization such as overall strategy, policies, support functions, business requirements, and work tasks and procedures. Digitalization has impacted whole organizations, governments, societies and cultures. In many cases, it is a requirement in order to communicate in the 21st century, to have access to the internet, ICT and digital technology. Industrial control systems are in the digital domain and businesses utilizes tools such as cloud computing. Technology and digital systems must be safe to use and in order to achieve this one must have some sort of security and security measures in place. Cyber security is the right place to start, but the term is not clearly defined. However, there are a few definitions available and there is a general agreement to what it encompasses:

- Knapskog (2016) defines information security *as the collective term for requirements for reliability and security associated with information*. Knapskog (2016) also defines data security *as information security for digital information*.
- The Investment Industry Regulatory Organization of Canada (IIROC, 2016, page 6) define cyber security as *"at its core, cyber security seeks to protect your enterprise from those who wish to do harm to your business, steal your information or your money, or use your systems to target peers in the market"*.
- The International Organization for Standardization defines (IIROC, 2016, page 6) cyber security or cyberspace security as *"the preservation of confidentiality, integrity and availability of information in the Cyberspace.* In turn (IIROC, 2016, page 6), *"the Cyberspace" is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."*

Many countries and multinational organizations are preparing and develop strategies for cyber security with national security in mind (NSM, 2009). There are discussions on a multinational level to find solutions and build collaborations across nations to increase their defensive capabilities. UN, The Council of Europe Cyber Crime convention, EU, and NATO are bringing cybercrime and cyber security on the agenda (NSM, 2009).

4.2 Why is Cyber security important?

Cyber security is important because of the potential damage an attacker can do to a nation, company or an individual. Sensitive information and data can be lost or fall in to the wrong hands. Critical societal functions can be compromised. Disastrous consequences can occur from sabotage of oil platforms, chemical plants, nuclear plants and other high risk organizations. The dependency on digital system is increasing along with the increasing cyberattacks and cyber threats. The understanding and awareness of digital vulnerabilities and cyber risk exposure is important to reduce risk in this digital transformation.

Growing threat

In a news article (Skjeggestad, et al., 2017) reveals that individuals working for the Ministry of Foreign Affairs, *Arbeiderpartiet* (Labor party's parliamentary group), PST (Police security Services), a university college, Norwegian Radiation Protection Authority and the Norwegian Armed Forces were attacked, or tried compromised by hackers. In the wake of the news of a malicious attack, the chief of intelligence Morten H. Lunde stated in a news article (Veum, 2017) that espionage and cyberattacks are increasing and that the Norwegian intelligence services cannot stop many of the attacks. Norway is not the only country exposed to cyber threats and cyberattacks. There have been accusations of Russian interference in the 2016 presidential election in USA (Harding, 2017). This kind of interference causes a threat to the functions of a democracy if elections and other functions can be influenced by foreign forces. These events, including the Lysneutvalget report (DNV GL, 2016), has initiated the discussion of a Norwegian digital boarder defense (in Norwegian: digital grenseforsvar). This defensive measure allows the Norwegian intelligence service to collect and analyze all the digital information that crosses the Norwegian boarder. Its purpose is to identify and counter possible external threats to national security and important national interests. This kind of monitoring activity raises questions about the privacy of citizens.

The focus on cyber security has increased the recent years along with the complexity and interconnectivity of ICT and digital systems (EOS services, 2010). It is difficult to gain complete overview of modern digital ICT systems because of the many connections or couplings into other systems, units, users, networks, and databases. Latent failures and undiscovered vulnerabilities may induce unwanted events, such as system failure or unprotected access points in the system. Airports, processing plants, platforms, hospitals, governments, and banks all use a combination of digital systems perform their tasks and functions.

Threat Picture in Norway

The Norwegian Intelligence Service (2017) explains that the most serious threats against digital systems in Norway will originate from Russia and China. The tension between Russia and the West means that the extensive intelligence activities against Norwegian targets will continue to grow. It will be a more intensive and systematic identification of vulnerable spots in critical systems, while they develop operational concepts directed towards sabotage. The Chinese activity is directed towards authorities and companies involved in industry and technology. Their goal is to harvest new technology such as renewable energy, green technology, industrial production quality, and development of medicine. The activities are expected to increase and typically smaller businesses are vulnerable because of inadequate data and cyber security. Their techniques for intrusion is expected to become more sophisticated.

Viruses and phishing are the most increasing threats against Norwegian government agencies, compared to other security problems such as denial of service, loss of data due to missing backup, misuse of IT of a financial character, connection failure to the internet or other external networks, and unauthorized access to systems or data.

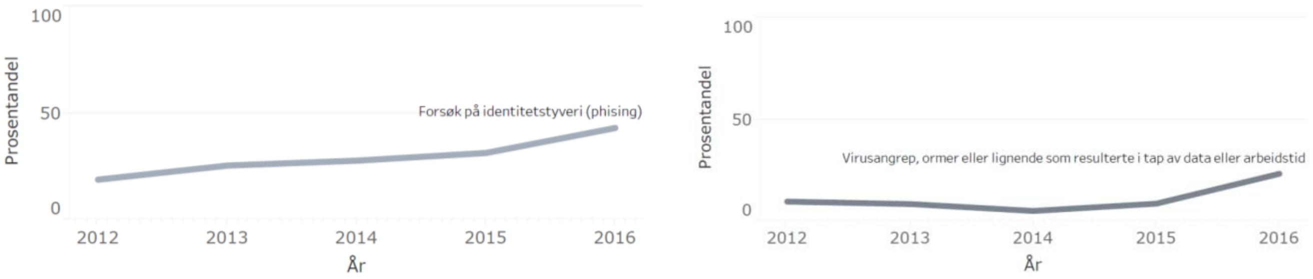


Figure 4.2A - Security Issues in Government Agencies (SSB, 2017)

Figure 4.2A shows that 43% of the government agancies where exposed to phishing attacks, and 23% where attacked by viruses, or similar, that resulted in loss of data or labor hours. Recently, a large-scale ransomware encryption virus labeled “Wanna Decryptor” hit several countries, including businesses in Norway (Omland and Wernersen, 2017). The trend is growing and the there are many private individuals and professional businesses that become victim of these events.

The oil and gas sector was in 2014 exposed to several cyberattacks. Some of them were targeting sub vendors of large Norwegian companies (NSM, 2015). The attackers gained access to several computers on the internal network of the company. From the yearly report from NSM in 2015, it displays the increase in cyberattacks from 2011 to 2014 in Norway (shown in table 4.2). The energy sector is an easy target because of the values within the sector, but these numbers are not exclusively from the energy sector.

Table 4.2 – Number of incidences managed by NSM (2009)

Year	Number of manually managed threats by NSM	Number of Serious attacks
2014	5069	88
2013	3400	51
2012	2332	46
2011	1657	23

Protecting Assets and Values

Nations, public and private organizations, and individuals have values worth protecting. These values are of interest to criminals, hacktivists, and foreign nations. The values, whether it be digital information, data, or systems connected to physical units, need to be protected in the same way that physical values, such as cash, cars, buildings, etc., are protected. NSM (2016a) derives a list of critical values and functions that vulnerable:

- The Government, society, and its functions:
  - Ensure national security
  - Ensure governance and crisis management
  - Maintain a democratic rule of law
  - Maintain health and life security
  - Maintain law and order
  - Maintain financial stability
  - Maintain basic security for stored information

These are functions fundamental to society. If a nation losses control over these functions, there will be consequences.

- Organizations:
  - Critical information, such as patents, tenders, production plans, budgets, and medical information.
  - Digital infrastructure, such as networks and servers
  - Software, such as industrial control systems that manage production and operation
  - Financial values
  - Personnel and personal data
  - Organizational structures
  - Assets, for example production equipment

A value assessment can highlight what is most important for the organization and what is most interesting for criminals, hacktivists, or other nations. The assessment contributes to the awareness of the organization.

Justifying investment costs

In a survey by PWC (2017b) 58% of the participants responded that they had been victim of some sort of cybercrime in the last twelve months. These crimes resulted in negative economic consequences for 41% of the participants. In some cases, the costs were exceeding 1 million NOK. The expenses cover investigation, improving and development of security measures and mechanisms. From the survey (PWC 2017b), the consequently most prioritized investments were to raise awareness, prevent loss of data, and vulnerability analysis. The cyberattacks can be devastating for smaller companies, where the criminals use ransomware to lock the company's digital system. This method takes the company's data or system hostage in exchange for money. The reason why smaller companies are easy targets, is because of the lack of cyber security measures and knowledge about the threats. If the organization is prepared the consequences can be reduced. These attacks are purely for economic gain and if prevented by an investment in cyber security, the damage can be controlled or minimized. If the cybercriminals can successfully attack an organization once, they can do it again if not the proper counter-measures have been implemented.

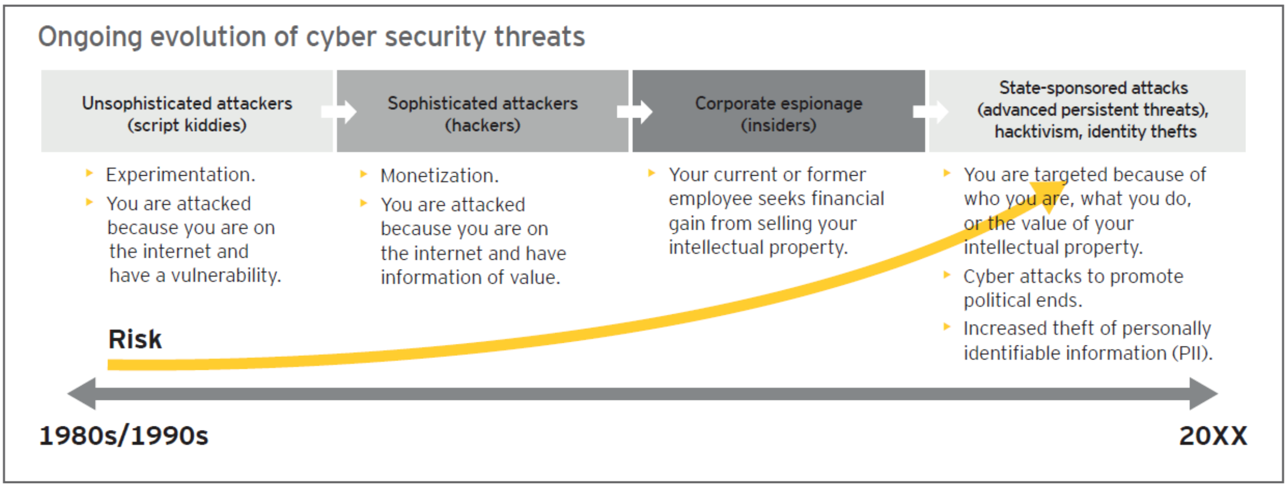

Ongoing evolution of cyber security threats
Unsophisticated attackers (script kiddies)
Sophisticated attackers (hackers)
Corporate espionage (insiders)
State-sponsored attacks (advanced persistent threats), hacktivism, identity thefts
Experimentation.
You are attacked because you are on the internet and have a vulnerability.
Monetization.
You are attacked because you are on the internet and have information of value.
Your current or former employee seeks financial gain from selling your intellectual property.
You are targeted because of who you are, what you do, or the value of your intellectual property.
Cyber attacks to promote political ends.
Increased theft of personally identifiable information (PII).
Risk
1980s/1990s
20XX

Figure 4.2B – Evolution of cyber threats (EY, 2014)

Figure 4.2b shows and increase in cyber threats. In the cases of a successful spear-phishing attack (or similar), the damage has been done and the only way to solve it is to “put out the fire”. There is a responsibility toward the organization’s customers and associates to prevent loss of data, business interruptions, poor availability, sabotage, and other consequences of cybercrime. This may cause customers to leave and damage business reputation. Damage to production equipment and servers will cause downtime and in turn, economic losses due to restoration costs and loss of production. In high risk organizations, the consequences can be fatal for the environment, equipment, people and society. If such an organization do not have a cyberattack recovery procedures the consequences can be disastrous. A modern organization that thrives for sustainability should be obliged to acquaint satisfactory measures against vulnerabilities in digital systems and critical infrastructures, and establish procedures that can reduce the risk and consequences of a cyberattack.

4.2.1 Low Entry Barrier

The threat agents are described in chapter 3.4. However, the main categories are identified as nations, cyber-criminals and hacktivists (NSM, 2016a):

- *Nations*: this encompasses foreign state intelligence and security services, but also private actors working on behalf of foreign states.
- *Cyber-Criminals*: individuals or groups typically involved in fraud of electronic payment services, e-commerce, and online financial transactions.
- *Hacktivist*: individuals or groups which utilizes illegal digital means to promote a cause or a stand in political affairs.

The interesting part of the threat picture is how it has change to become a commercial business and has a low technical entry level (Marinos, Belmonte and Rekleitis, 2016). Hacking as-a-service is a growing trend an increases the threat level. The commercialization makes the prices low and anyone can buy hacking services to achieve great damage. The dark net serves as a forum and a sanctuary for cyber criminals and their business. Marinos, Belmonte and Rekleitis (2016) states that there are low attribution levels in all the known cyber-related incidences. It is difficult to perform investigations and

4.2.2 Methods and Threat Vectors

There are numerous methods to perform a cyberattack. The attacks combine multiple vulnerabilities in the organization, technology, and human factors to create a sophisticated attack. NSM (2016a) presents some of the most common methods:

- Advanced Continuing Threats

This is a collective term for sophisticated, advanced and targeted attacks that establishes backdoors, planting and spreading malware and extract sensitive information. The attacks are characterized by its longevity and that the threat originator is resourceful (for example a foreign state).

- Insiders

An insider may be an employee or someone not directly employed, for example through a third party. This could be a business partner, client, consultant or cooperative Contractor. These individuals have gained a position where they have access to the systems and abuse their access or credentials to do harm. Typically, creating a backdoor or and opening into a system, so that external actors can get access.

- Ransomware

These are viruses that encrypts files in a digital system and will be decrypted for ransom.

- Attacks via email

These are commonly called phishing or spear-phishing. Phishing are emails with a set of instructions disused from a college or a manager. Spear-phishing are emails that contains malware or tools to steal information, gain access to servers, etc. These emails usually contain links or attachments. These attacks utilize the vulnerabilities in humans.

- Watering hole attack

This type of attack compromises a website that is frequently visited by the targeted group of individuals so that they are infected with malware.

Specific Targeted Attacks

Targeted attacks are malicious attacks that are aimed to a specific individual, company, system or software based on some specific knowledge regarding the target (Marinos, Belmonte and Rekleitis, 2016). The occurrence of targeted attacks is infrequent and involves more planning and resources than a non-targeted attack. The phases of such an attack can be described (Marinos, Belmonte and Rekleitis, 2016):

- Reconnaissance acquires publicly available knowledge about the system, organization, and/or individual. This enables a customized attack strategy.
- The initial phase revolves around gathering specific information from several areas such as the ICT environment, organizational structure and personal information. This data is used to create the attack.
- The delivery phase is where the threat actor delivers the bait. This is dependent on that the victim is fooled into the trap.
- The Exploitation phase is where the exploit code delivered the payload. The payload contains a specific set of commands that utilizes the exploitations in the system. If the exploitation is successful, the payload starts installing the malware, usually by downloading the malware onto the

victim’s system. This creates a communication channel to the “outside” which can execute command and control functions. The malware can extract data, move to other systems, and successfully perform the objective.

Risk reducing measures and barriers needs to be in place should the organization be able to defend itself from these threats.

4.3 Barriers and Security Measures

This chapter will present The Investment Industry Regulatory Organization of Canada (IIROC, 2016) collection of common best practices in cyber security, as well as, a supplement of a few other organizations. It serves as an aid in understanding how to protect the organization against cyber threats. It will be divided into organizational, technological, and human barriers and is corresponding with the vulnerabilities in chapter 3.6.

4.3.1 Human Barriers

These are barriers that include human involvement in operation and ICT systems. Humans contribute to the organization's overall cyber security capability.

4.3.1.1 Cyber security awareness and training

Cyber security awareness and training is an enabler for increasing cyber security defenses and capabilities. Awareness and training will increase the employee security procedure compliance and understanding. An alert security culture is an important preventive measure and can mitigate cyber risk. Lack of security awareness in ranked as the number one factor that prevents defense against cyber threats (IIROC, 2016). IIROC (2016) suggests these security measures:

- Develop policy that encompasses secure use of computer systems.
- Develop mandatory cyber security training and awareness for all employees.
- Describe clear employee roles and responsibilities regarding cyber security
- Employees and managers should be given special training related to phishing.
- Users should be instructed to not connect devices to the network, unless they have a reason to, follow good password routines, and practice safe use of external media,
- Dedicated education for executive management.

These measures will significantly increase the security culture and reduce the cyber risk. The organizations must ensure that these measures are performed and evaluated.

4.3.2 Organizational Barriers

These are barriers that involve management, collaboration efforts and other organizational aspects. It includes the framework from risk management and cyber security.

4.3.2.1 Governance and Risk Management

IIROC (2016, page 7) states *"Cyber security is not only an IT problem, it is an enterprise-wide problem that requires an interdisciplinary approach, and a comprehensive governance commitment to ensure that all aspects of the business are aligned to support effective cyber security practices."* ICT is incorporated in most disciplines and is a large part of organizations' operation and infrastructure. Cyber security is a multifaced challenge which requires organizational engagement and support from its management. It can be compared to how organizations value traditional operation safety, which embedded deeply into the core of most organization and acquired by industry regulations. It is important to have an active and engaged management which is concerned about security issues, notices its importance, and is capable to follow up on security initiatives. An organization will never obtain total protection from cyber threats. A risk based approach makes it possible to identify new and current threats, and mitigate risk.

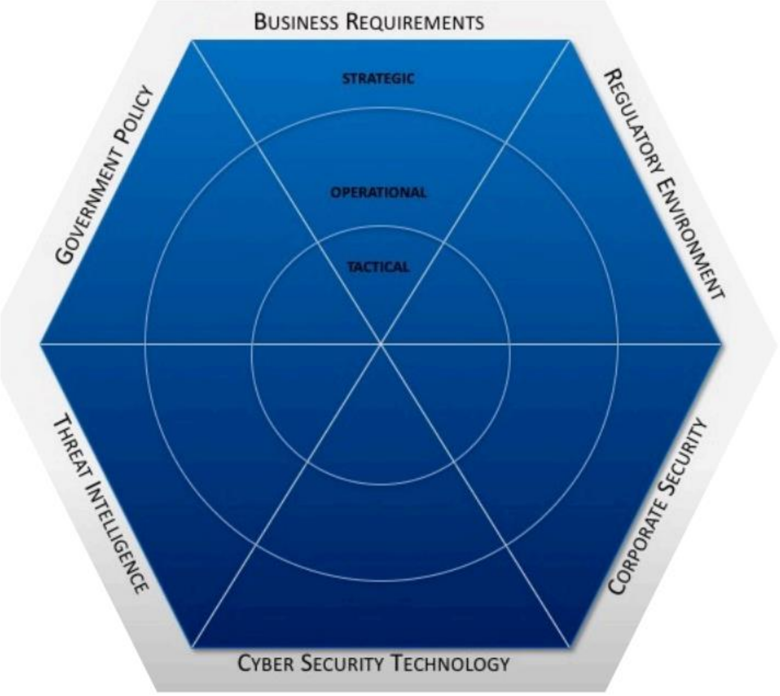


Figure 4.3.2.1 – A Conceptual Framework of all aspects of Cyber Security (IIROC, 2016)

All organizations are affected by different factors. The factors presented in figure 4.3.2.1 contribute to the level of security in organization and industry. Government policies and regulatory environment shape the basic requirements for cyber security. Business requirements affects the specific industry standard and the elements or values that makes the organization vulnerable. Threat intelligence is the basis for security measures and where the attention of the organizations must be. Corporate security are all the elements in an effective integrated solution such as cyber security, physical barriers, personnel management. Cyber security technology is a tool in which the organization can use to execute its security policies, but should not be the main driver or support for a poor cyber security understanding or management.

4.3.2.2 Governance Framework

If the organization does not have a cyber security program, it should start identifying and allocate roles and responsibilities for the establishment a program. The committee should include senior executives from all aspects of the organization. This will enable full access to the organization's knowledge and capabilities. It is recommended to select a leader that can ensure that the efforts are focused on the concerns of the organization and avoid a silo-based focus. It is also recommended to assign the Chief Information Security Officer with responsibilities to oversee the cyber security activities. The implementation of the cyber security framework is presented in seven steps (IIROC, 2016):

1) Prioritize and Scope

Prioritize the objectives around the overall strategic focus. This includes a value assessment, inventory control and identify the criticality of systems. Find the values that are interesting to criminals.

2) Orient

Identify threats to, and vulnerabilities of, systems identified in the prioritize and scope setup.

3) Create a Current Profile

Define the current state of the organization's cyber security program.

4) Conduct a Risk Assessment

Conduct a risk assessment using an accepted methodology. The risk assessments can provide with an understanding of criticality and can prioritize security measures accordingly.

5) Conduct a Target Profile

Develop a risk-informed target state profile describing the desired cyber security outcome. The desired outcome should include the organization's preferences, but also those of the stakeholders.

6) Determine, Analyze, and Prioritize Gaps

Conduct a gap analysis to determine opportunities for improvements. Prioritize gaps based upon risk assessment. The gaps are unique to each organization and is based upon business requirements, system configuration, and resources available to close the gaps.

7) Implement Action Plan

Document roadmap to achieve strategic goals. Establish reporting process to governance committee. It is important to establish a monitoring process in the organization to ensure commitment through time.

4.3.2.3 Board and Senior Management Involvement

Board and Senior management needs to understand the importance of a holistic organizational approach to cyber security. There are five principles that the top-management should be aware of, regardless of company size (IIROC, 2016):

- It is a risk management issue for the entire organization, not limited to ICT. There are many vulnerabilities with the use of digital systems, related to organizational, technological, and human factors.

- There are legal implications in cyber security that can issue lawsuits. The organization and the board should understand the contours of liability, and initiate alignment measures.
- The board members should seek advice from experts and have access to technical knowledge related to cyber security. This will enable discussions related to cyber risk management. Cyber security should be given attention to in board meetings.
- The top-management should enable and ensure the establishment of a cyber risk management framework is given sufficient resources. The board should expect regular updates and reports.
- Top management should discuss and prioritize the risk reducing measures according to criticality, the ALARP principle, and as resources allow.

In addition, NSM (2016a) presents three key concepts in establishing a foundation for a good security policy:

Foundation in leadership

- Management needs to understand that cyber security is a risk management issue throughout the organization.
- The management is responsible for setting objectives and allocate resources to achieve these objectives. One of these objectives should be to gain competence and expertise in cyber security, as well as generating a framework for cyber risk management.
- identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.
- A periodic evaluation of the security condition of the organization will keep the objectives and measures relevant and updated, and the organization can create new objectives and visions.
- The commitment and focus on cyber security from leadership should spread through the organization in a top-down manner in such a way that employees are informed and share the same information as the leaders regarding cyber security.

Commitment through documentation, responsibility and clarity

- The responsibility in planning, implementing, reviewing security activities should be clarified and described in detail to ensure commitment and feasibility.
- The documentation is important to ensure progress and that the security measures and procedures are being followed.
- A clear distribution of responsibilities, chain of command, tasks and functions will ensure the execution and reduce misunderstandings. This will ensure the prioritizing and the execution of security work and efforts.

Reduce risk through awareness

- An effective way of reducing risk is to have continuous efforts towards raising awareness, motivate and increase the understanding of security and risk in all levels and in all departments of the organization. This will raise the competence in the whole organization.

The lack of management involvement and commitment leads to poor security management and vulnerable ICT systems (NSM, 2016a). Insufficient routines, practices and security review are managerial decisions that causes vulnerabilities to grow, instead of being corrected and reduced. Basic ICT security measures will drastically reduce vulnerabilities and the increase of awareness help prevent future vulnerabilities. In some cases, security measures are implemented, but the top management lacks interest and is not involved in the follow-up process. This means that the measures are not evaluated and cannot be improved or adjusted to the present threat picture. The security activities get deprioritized and does not become a part of the organizations strategy and operation. Implementing security measure without performing a value assessment and an overall risk assessment may lead to generic and ineffective security measures. A holistic approach with leadership commitment which includes all disciplines of the organization, will lead to better efforts that include all aspects of the organization.

4.3.2.4 Information Sharing and Breach Reporting

Information sharing groups and CERTs

Organizations can benefit from sharing information and knowledge regarding cyber threat and security. Collaboration and information sharing can enable organizations to gain actionable visibility into their most relevant risks, understand the motives and tactics of adversaries and shed light on the most effective response methods (PWC, 2017a). The idea is to advance cyber security capabilities through cooperating and by sharing critical threat intelligence with business peers, industry groups and government authorities. In the USA, due to an Executive Order in 2015, there are forming private sector cyber security information sharing organizations (Cyber Threat Intelligence Network, 2016). There are two types of information sharing groups: Information Sharing and Analysis Centers (ISACs) and Information sharing and analysis organization (ISAOs) (Cyber Threat Intelligence Network, 2016). These are organizations that encourages to share information regarding risk mitigation, incident response and alert in cyber security. The goal is to provide users with accurate, actionable, and relevant information (Cyber Threat Intelligence Network, 2016). The organizations are discipline specific and are non-profit communities, membership organization, or a single company sharing information with its customers and stakeholders. An example of this is from the U.K., where four large banks have formed the Cyber Defense Alliance to work with the UK National Cyber Crime Unit (PWC, 2017a). This is a great way of making a uniformed front against cyber threats in both private and public sector.

ISAOs benefits (PWC, 2017a):

- Creating a trusted and connected network that significantly strengthens an individual organization’s capabilities for identifying and mitigating cyber-risks.
- Quickly delivering actionable cyber threat intelligence to support measurable cyber security improvements.
- Lowering cost and barriers of entry for cyber security information sharing.
- Enhancing and simplifying cyber security information management, analysis and intelligence.
- Qualifying members for legal protections from certain liability, anti-trust and regulatory enforcement actions.
- Helping meet or exceed regulators’ rising expectations for cyber-risk mitigation at a time in which company executives are increasingly held accountable for breaches.
- Transforming business models for information sharing to increase economies of scale.

Computer Emergency Response Team – CERT

Many CERTs have been established recently. In Norway, there are NorCERT, KraftCERT, HelseCERT, FinansCERT, among others. The service the CERTs provide is vulnerability monitoring, threat intelligence, detection, incident response and incident management, counseling, drills, and training (Nilsen, 2014; KraftCERT, 2017). The CERTs fulfill a need which has been increasing throughout the recent years. They provide a sought-after expertise and is a forum where organizations can share information and experiences anonymously. The CERTs collaborates between themselves, this leads to better prepared organizations across industries.

VDI - alert system for digital infrastructure

VDI is a sensor network operated by NSM's NorCERT. Its objective is to detect breaches in critical infrastructure in Norway, regardless of industrial sector (NSM, 2017). VDI is a voluntary membership and the information VDI collects from its members is confidential. The arrangement allows organizations to detect any possible breaches. The system was created because of the inconsistency and ineffectiveness of user alerts. Usually the users do not know that the systems have become compromised. NSM's responsibility encompasses operation and development of VDI, develop analysis tools, develop reporting routines for detected incidences, follow up members of VDI, analyze cyberattacks and malicious code, contribute to an updated ICT threat picture.

4.3.2.5 Vendor Risk Management

All third-party involvement includes risk. In some cases, a third party has access to sensitive information. Therefore, organizations should implement strict requirements for third party involvement. The key objectives for a vendor risk management program includes (IIROC, 2016):

- Rank vendors based on risk
- Develop clear policies which the vendor can follow
- Develop contractual conditions and requirements
- Establish a program to verify the vendor performance

These objectives are the foundation for exercising third party control. When planning and reviewing tenders, a set of standard questions should be asked and documentation should be required from all possible candidates. Penetration test of potential candidates is also a great tool of ensuring that the candidate meets the requirements for security. On-site visits are also a tool in ensuring that the candidate follows the contractual terms or requirements.

4.3.3 Technological Barriers

4.3.3.1 Physical and environmental security

There are many non-cyber related events that requires protection from human and environmental factors. To ensure system availability and reliability, there should be mechanisms in place to reduce the occurrence or the consequence of these factors. Intentional or unintentional human acts can cause damage or disrupt operations. The floods, fire, etc., can cause serious damage to infrastructure and equipment. Critical operational systems such as power supply can be interrupted or damaged. IIROC's (2016) recommendations for physical and environmental security are:

- Be aware of sensitive items and make sure it is not accessible for anyone. This applies for sensitive information and items with containing sensitive information, such as documents and computers.
- Only allow employees into the work area if they have a legitimate business requirement.
- Employees should lock the screen when moving away from the computer.
- Safeguard your information system against fluctuations in electricity or electrical power outages, by ensuring that the system has an Uninterruptible Power Supply (UPS).
- Ensure that backups are performed on a regular basis to safeguard your information against a catastrophic event such as a flood or fire.
- Small- and mid-sized organizations need to have a plan in place to address physical security issues. The physical security controls implemented should be equal to the level of sensitivity of the information being protected.

These security measures are easy to understand and implement, due to the visibility of the barriers. These are important security measures, even though most do not directly link to cyberattacks.

4.3.3.2 Threat & Vulnerability Assessments

There are continuously discovered new vulnerabilities in common software. Threat actors target these vulnerabilities when they are discovered. Therefore, it is important to be patch the system or software in order to stay secure. Regular procedures for patching will mitigate most risk related to outdated software and vulnerabilities. IIROC (2016) suggests these measures:

- Run regular, automated vulnerability assessment tool on all systems connected to the network.
- Each responsible system administrator should be given a prioritized list of the most critical vulnerabilities.
- Collaborate with vulnerability intelligence services to gain awareness to trending threats.
- Update the vulnerability scanning tool regularly.
- Perform strict patching routines on software and applications.
- Evaluate critical patches and perform tests in secure environments before applying them to production systems.

These security measures should run constantly and are a large part of the security activities.

4.3.3.3 Network Security

Network security encompasses the protection of confidentiality, integrity, and availability of the network and its connected assets. Network security performs three main objectives; protect itself, reduce the threat susceptibility of connected devices, and protect data transmissions across the network. The firewall is a multilayered defense mechanism that will greatly reduce the number of successful cyberattacks (IIROC, 2016). Modern firewalls can filter out web sites containing malicious content, protect against malware entering the network, and examine network traffic to detect and prevent malware. Two-factor authentication for all remote login access will make the remote access more secure.

Wireless Network Security

The wireless network introduces additional risks and challenges. The wireless signals can broadcast beyond the office walls and be accessed from outside the business' building. This presents a vulnerability because malicious actors can take advantage of this and install hidden unauthorized wireless access points on the network (IIROC, 2016). Additionally, it means that the malicious actors do not need to step inside the building to access the network. This requires that only permitted devices should be given access to the network. IIROC (2016) recommends performing vulnerability assessments scans of wireless networks, as well as wired networks, to identify the vulnerabilities within the network. It can also identify unauthorized networks devices. Further, the use of a wireless intrusion detection system (WIDS) can identify unauthorized wireless devices and detect cyberattacks. Data encryption will protect the data flowing across the network, typical encryptions are AES (advanced encryption standard) and WPA2 (Wi-Fi protected access 2). IIROC (2016) states that the minimum requirement for secure authentication protocols should be EAP/TLS (Extensible Authentication Protocol-Transport Layer Security).

Remote Access

Remote access is a common tool in modern operations. It is important to continuously manage and maintain these access points to keep unauthorized users from accessing the network. The remote access should be governed by a remote access policy and organizations should make sure employees comply with the given policy through training (IIROC, 2016). Secure VPNs be configured to not allow split tunneling (the ability access public networks and a local LAN at the same time) and all remote access sessions should be monitored and logged (IIROC, 2016).

4.3.3.4 User Account Management and Access Control

Access control decides what databases, applications and other network-based resources the employees gets access to. The idea is to limit all functions, and allow the functions that makes it possible for the employee to perform his/her tasks. IIROC (2016) suggests these measures:

- Implement a central account management process.
- Configure networks and security devices to use the centralized authentication system.
- Limit admin rights to those how strictly need it for business requirements.
- Perform system accounts reviews and disable accounts that does not have business purpose.
- Give all user accounts an expiration data.

- Disable accounts upon termination of an employee or contractor. Disabling preserves audit trails, if it becomes necessary to review the employee or contractor.
- Standard user re-login after inactivity.
- Strong password requirements and regular password change.
- Any account with extended privileges or access to sensitive data or functions, must have two-factor authentication. For example, by using smart cards with certificates, one time password (OTP) tokens, or biometrics.

An active user account management and access control system is a sign of good information and cyber security practice. Large organizations may have numerous users, contractors and suppliers with network access. These users and access points needs to be managed, otherwise they represent a threat.

4.3.3.5 Information System Protection

Devices connected to the network needs protection as well as the network. There are many devices connected to the network, such as phones, computers etc. IIROC (2016) recommends these security measures:

- Implement secure backup and recovery processes and perform regular system backups.
- Implement anti-malware solutions that continuously monitors workstations, servers, and mobile devices with anti-virus, anti-spyware and personal firewalls.
- Implement a policy to control all access to removable media
- Limit the use of external devices such as USB devises, only to those that have a legitimate business requirement.
- Utilize personal firewalls built into windows and UNIX-based systems.
- Scan all media for malware before importing on to corporate system.
- Install all application and operating system security updates.
- Monitor for the attempted use of external devices.

These measures form the basis for device protection. However, bring your own device (BYOD) is a concept in business (IIROC, 2016). This means that employees bring their own computers, phones, tables, etc. to work. This concept carries additional risk. Employees may lose their personal device which contains sensitive information or access, or unintentionally install malicious applications. The organization needs to decide if it can manage the associated risk and implement sufficient security measures.

Backup and recovery functions is a vital part of preparing for emergencies. Backups makes it possible to recover from an incident and restore damaged or lost data. IIROC (2016) recommends that the organization implements a plan and begin backing up data regularly. Copies of the backup should be kept in a different, secure location. The backups should include system and software settings, and be tested on a regular basis.

4.3.3.6 Redundancy

System redundancy is useful to reduce the consequences of system failure, natural disasters, cyberattacks, etc. Its purpose it to maintain production or the operation even after an unwanted event, caused by any factor, physical or cyber related. Critical operational functions should have redundancies, but these solutions may be expensive and is not possible for every organization for financial reasons. Critical infrastructure and societal functions should have higher requirements for redundancy, for example on system level and standby-operation centers. Any production should not have a single critical point which can cause catastrophe or production stop.

4.3.3.7 Manual procedures

As dependency on digital system grows, there is a need for either fast system recovery or manual procedures. These procedures are not always possible; it depends on the nature of the operation. Sometimes, digital systems functions as an aid or as an optimizer, then it is possible to switch to manual procedures during an emergency. In other operation, where the main function is based on digital function, it becomes impossible to execute the function manually. In those cases, it is best to have redundancies or system recovery functions.

4.4 Incident response management in Oil and Gas sector

As a part of the overall cyber security program, incident response plays an important part in preparing, manage, and learn from incident experience. Incident response is a well-known term in high risk organizations. It is generally related to preventing or reducing the consequences of failures in a technical system such as potential loss of lives. Nuclear power plants, chemical plants, offshore platforms and other facilities have incident response procedures in case an unwanted event occurs. It is a part of the safety management and has change over the years because of the various incidents that has occurred. The incident response is important in cyber security as well, commonly called detect and response mechanisms.

Incident Response Management in organizations

"The new approach introduced by IRMA results in a circular perspective on the incident response management process, where learning from incidents gives input to organizational processes and feedback throughout the organization as a whole" (Jatuun et al, 2007, page i, executive summary). In the recommended practice from the oil and gas sector (Jatuun et al., 2007), an incident response management consists of three phases: plan & prepare, detect & recover, and learning (figure 4.4).

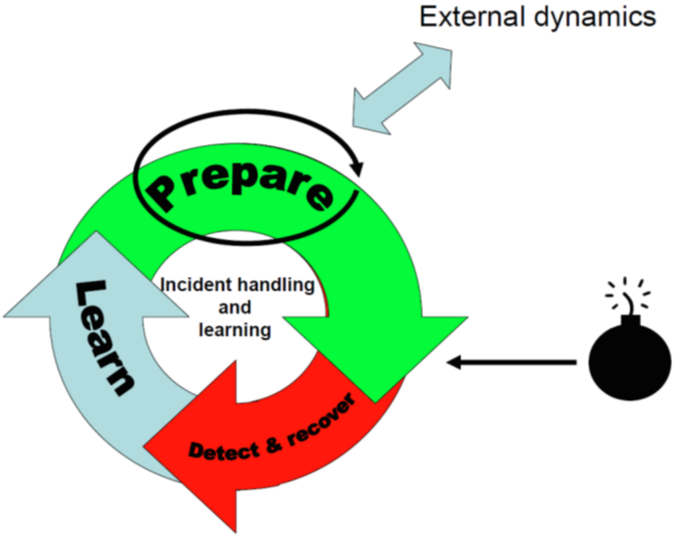


Figure 4.4 – Incident Response Management Wheel (Jatuun et al. 2007)

Three phases

The process is divided into three phases; plan & prepare, detect & recover, and learning. These phases cover the most important aspects of responding to a threat or an incident and internal and external dynamics.

4.4.1 Plan and prepare phase

This phases where the organization is focusing on preparation for incident response, which includes detection, manage and recovery from attacks and other incidents. This is where information is gathered along with performance of risk analysis. The activities in the incident management plan should be documented and communicated to all relevant employees within the organization, and optionally supplier.

The plan should consider organizational, human factors, and technical issues, and be design with the complexity of the operational situation in mind. The complexity is due to the multiple technical systems, suppliers, contractors, and the interconnectivity of the operation. It is important to point out that information security includes incident response, but they can affect each other. The activities in the preparation phase are:

Adjustment to external (and internal) dynamics

The incident response plan responds to the dynamics within the organization. The organization may be influenced by technological change, socio-technical systems, external incidents, changes in the market conditions, changes the competence level in the organization, changing political climate and public awareness. This may affect the organizational context, -strategy, and the regulations in which the organization must follow. The incident repose management activities are also influenced by other organizational processes and frameworks, such as HSSE and production processes. The adjustment to external and internal dynamics is important for the organization's incident response activities to stay updated, relevant, and continuously improving for the best practices.

Risk assessment

As described in chapter 3.2, the risk assessment for an incident response management is a periodic activity that describes the probabilities and consequences of potential incidents that may occur. The security measures may vary in accordance to prioritization, resources, and governmental regulation. Monitoring and communication of the risk level is important to generate a common risk perception. The monitoring can be assisted by external resources such as authorities (for example NorCERT), internal firewall and security software, and suppliers of ICT solutions (for example Symantec).

Roles and responsibilities

The incident response structure and work must be organization in a way that considers the dynamics, competence, structure, and socio-technical system of the organization. It must be clearly defined beforehand roles, responsibilities and who to involve in when an incident occurs. There are key functions within the incident response plan. These are (Jatuun et at., 2007, page 21-22):

1. Detect and alert: *Anyone who detects or suspects that an incident has occurred is responsible for raising alert. Everyone should be aware of this responsibility and its importance.*
2. Receive alerts: *Someone must be responsible for receiving alerts and, if applicable, who to alert next. Everyone must know who to alert in case they detect an incident*.
3. Provide technical expertise: *Someone, either inside or outside the organization, must have technical system and/or security knowledge, and this knowledge must be available in incident recovery.*
4. Manage incident and recovery: *Someone must be responsible for leading the incident response work.*
5. The authority to make decisions: *for incidents with potential serious consequences it is critical to have someone with authority to make decisions. Management must therefore be available.*

For incidents related to oil and gas and integrated operations, the platform manager, technical network manager (process/SCADA), ICT/Telecom person, and central control room operators are involved in handling the incident. These persons may be stationed both onshore and offshore. Having a dedicated incident response team is difficult to achieve. In most cases, the incident handling responsibilities and regular work responsibilities must coexist for the given person/role. It is important to have a clear and unambiguous line of reporting and it must be available in production time, which for most offshore production operations means 24 hours a day, 7 days a week. For incidents that requires the supplier's competence, there should be made a list of available contact persons made clear by the contract. Organizations have a responsibility to share incident experience so that the industry sector, business partners, and the organization itself can improve and be better prepared in incident response. This is possible via seminars, conferences, industrial and national bodies (such as NorCERT or Petroleum Safety Authority).

Planning and documentation

The risk analysis will guide the focus and prioritization of the ongoing planning process. Detailed documentation and continuous updating of all routines, configurations and systems is important in preparing for an emergency. If the person with the knowledge is not present, the remaining staff needs to rely on the documented information. The general employees' awareness around incident detection and alert is critical for the incident plan. This means that every individual need to be familiar with the details involving practical procedures of detecting a potential incident and the following alert process. Therefore, the documentation requires a level of detail and that the documentation must be available to everyone. The practices need to include clear and simple actions when detecting and responding to an incident. Jatuun et al. (2007) recommends: a plan for what to do if being the one that detects or suspects that an incident has occurred, a plan for how to detect incident with the help of tool, routines and information sharing, and a detailed plan for how to respond to different types of incidents. Such plans may be presented in a step by step diagram with clear instructions and contact information.

The learning phase needs to be taken seriously, which means that the organization should facilitate the resources and framework for learning from past incidents. Jatuun et al. (2007) recommends a team based approach and a structured incident analysis to share information internally and externally in the organization. Key factors for a successful learning procedure are commitment in management, develop a learning culture, gain necessary capabilities such as knowledge, training, guidance and support, and create a willingness to change (Jatuun et al, 2007).

Awareness creation and training

Awareness creation can benefit the organization in reducing the probability of incidents and improving the employee's ability to detect and react to incidents. In the oil and gas industry it is common to have long rotations, for example, two weeks on and four weeks off. Long shift rotations create a need for long duration awareness campaigns. If there are several organizations involved, there is a mix of security cultures. Any awareness campaign needs to address these matters in the virtual organization. Poor collaboration and communication skills may create different views on what is most important in the operations, for example confidentiality and integrity or continuous production. Many of the different specialists have their own professional “language” which can be misinterpreted when communicating with other non-specialist-individuals.

Education, learning and simulation will ensure knowledge of how to respond, what to look for, and why it is important. Different levels of knowledge are required in different groups. Security and system personnel needs a higher knowledge of system performance to look for abnormalities. This means that communication plans need to consider its target group. Training and simulation for specific incidents, both likely and unlikely events, will raise the preparedness of the organization if such an event occurs. This can reduce the probability of an unwanted event and its consequences.

Monitoring

Performance indicators can be used to monitor the incident response management. Documentation of the performance indicators will make it easier for decision-making, communication, comparison, benchmarking and learning. It can have motivational benefits as well as show compliance with company security policy, industry standards and best practices, and public regulations and requirements. The performance indicators will be presented in chapter 4.4.4.

4.4.2 Detect and recover phase

It is important to prepare for the detection and recover phase. If a proper plan is not in place, incident may be detected only by coincident and procedures for how to manage the incident are not clearly defined. Simple guidelines will increase the preparedness of the organization.

Documentation and preparing for learning

The learning phase is dependent on documentation of incidents. This is why the documentation in the detection and recover phase must contain a level of detail. However, the practical process of detecting, alerting, and responding to the incident should not be delayed by a detailed documentation process, but threated as soon as possible. For example, it should be enough to start the recovery by answering the first three questions below (Jatuun et al., 2007):

- who detected the incident?
- where did the incident occur?
- what orruced when and how was it detected?

Futher, it is important to eventually document the detailed information in to a database. The following should be answered (Jatuun et al., 2007):

- incident details, such as consequences, causes, extent of dispersal
- actions made and the reasoning behind the actions
- time and resources spent on treating the incident

It is important that the documentation tools are avaliable and easy to use. Moreover, those involved in inceident repsons must be trained in using them.

Detect and alert

The essence of the detect and alert plan is so that everybody knows who to alert and how to do it. The detection of incidents happens by coincidence or by routine. Someone notices something unusual, or it is picked up by firewalls, intrusion detection systems, anti-virus tools, or by examining logs. Contractually obligated incident reports from suppliers can help identify risk level and what kind of influence or consequences it has for the organization. Experience and skills are needed to identify when there is a real incident or just a false alert. This requires competent incident response employees. Even though there may be a large volume of false alerts, it should not be punished, but faced with appreciation for the employee' vigilance and efforts.

In a virtual organization, or an organization with a similar complex structure, it is important to communicate the responsibilities employees, suppliers, and contractors to raising alert. Considering that everyone's knowledge about cyber security is different makes it important to facilitate easy-to-use guidelines and tools to know when to react and what to do in the event of or suspicion of an incident.

Recovery from incident

A successful recovery is dependent on preparation, a plan and the access to necessary skills. Two important factors are (Jatuun et at, 2007):

- A clear distribution of responsibilities should come through an appropriate hierarchy of personnel, with assessment decision making and actions involving both security and non-security personnel
- Clear procedures provide directions for involved persons, including reviewing and amending the report made, assessing the damage, and notifying the relevant personnel.

Five steps of incident recovery (Jatuun et al, 2007):

- Assessment

Once an incident has been notified to the relevant personnel, an assessment needs to be made of the severity of the incident and how to proceed. The person who reported the incident must receive a confirmation that the incident is taken care of, and if possible, kept in the loop. This makes the individuals who report incidents aware of that they are taken seriously and that the organization cares about their concerns. Subsequently, it is important to gather information and alert those that need to be involved in handling the incident, for example, line production management, central control room, etc.

- Immediate response

Different systems would have different practices for immediate response. There is a difference between IT systems and IC (industrial control) systems. Table 4.4.2 show an example of different procedures.

Table 4.4.2 - Difference between IT and IC systems immediate response (Jatuun et al., 2007).

IT system	IC system
- Disconnect from the internet - - shut down the information system, service and/or network, or isolate the relevant part and shut it down - Activate surveillance techniques	- Isolate the ICT part of the system (if this is where the problem lies), and continue with operations of the process system in order to avoid process shut down - Disconnect the SAS (Safety and Automation System) from the internet and external networks completely - Enhance the control of incoming and outgoing traffic on the target network (segment) - Perform process shut down (PSD) - Perform Emergency shut down (ESD) - Remove power from ESD system and restore, to ensure that the ESD system has not been inactivated

- Escalation

If the organization cannot process the incident with the current staff, the organization should escalate and bring in external help. This could be adding more personnel from within the organization, involve suppliers, involve external experts, involve top management, or involve a crisis authority organization. The involvement can be due to a need for additional competence, the incident is too severe, or a need for someone with decision-making authority.

- Communication

The degree of significance of the incident depicts if it is necessary to inform additional people, such as management, press, or those affected. The organization needs guidelines for whom to communicate with should it be necessary. Social media plays an important role in today's public communication. An organization needs to be able to control and respond to social media and press. If the incident is critical, public appearance will be important in to communication with the public and press.

- Further responses

Once the incident is controlled, the systems needs to be brought back to normal. In this process, it is important to take precautions. The vulnerabilities in the system must be improved, for example, changing passwords and access data after the incident, utilize security tools such as integrity checks and perform backups, and be aware of that there may still be malicious code in the system.

4.4.3 Learning phase

The learning phase is an opportunity for improvement. The documentation of the incident creates the foundation for further learning, and the experience of those involved can be used in prevent and manage incidents in the future. Key steps in the learning phase are understanding how the incident occurred, analyzing barriers, asses the quality of the incident response, and finding improvements. The challenges in learning from incidents is that the organization is in a virtual organization or in an integrated operations environment involved with many different organization. It is difficult to coordinate a learning process and existing tasks and functions may cause the learning not to be performed. There is also a cultural difference, as well as a technical difference, in ICT and ICS professionals. It the incident involved the two categories, there may be a problem in cooperation. Once the system recovery is complete and over, many are tempted to not perform the root cause analysis, and if it is performed it does not include organizational and human factors as much as the technical issues.

Four steps in analyzing incident and suggesting barriers (Jatuun et al, 2007):

1. Performance analysis – identify usage of resources and commitment in the organization.

This step covers the need for resources and identifies if there should be given more or less resources to incident response and learning. The willingness to learn and potentially change is important and may reflect the investigation process. If the investigation only focuses on the initial failure and not on underlying causes, such as organizational culture.

2. What occurred – identify the chain of events that led to the incident.

Identifying the chain of events is critical for learning from mistakes and faults. Who was involved in the incident? What were the events that influenced the accident? How was the incident handled? At what time did the events occur? What are the relationship between the events and what caused each of them? The answer to these questions may be answered in a STEP diagram (Jatuun et al, 2007). The STEP diagram (figure 4.4.3.1) is supposed to identify the weaknesses in the system for a given scenario.

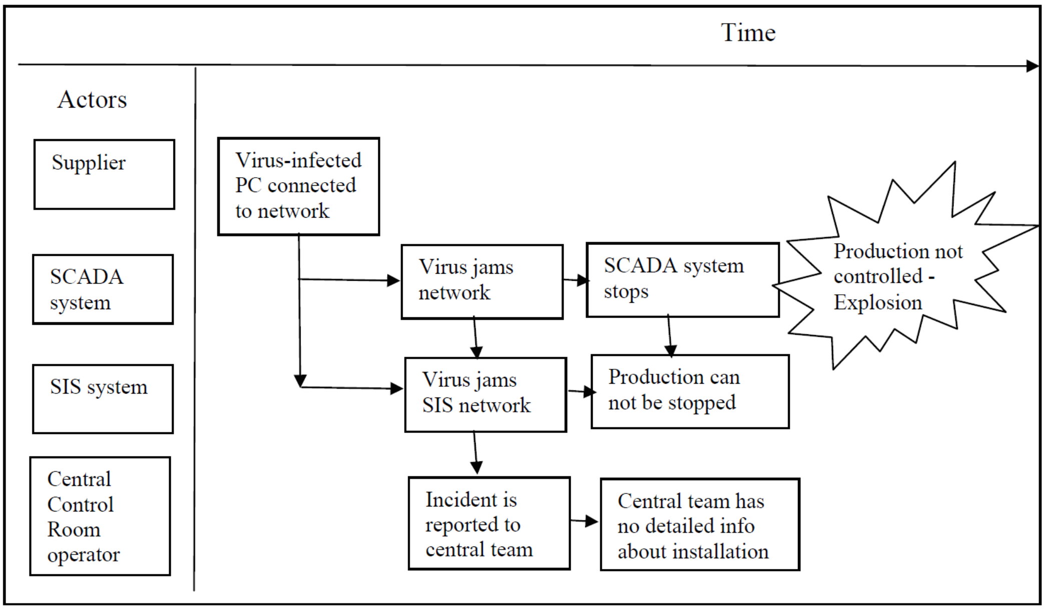

Time
Actors
Supplier
SCADA system
SIS system
Central Control Room operator
Virus-infected PC connected to network
Virus jams network
SCADA system stops
Production not controlled - Explosion
Virus jams SIS network
Production can not be stopped
Incident is reported to central team
Central team has no detailed info about installation

Figure 4.4.3.1– Schematic STEP diagram of a virus attack (Jatuun et al., 2007).

SIS – safety instrument system

3. Why – identify root causes, barriers, and technical, organizational, and human issues.

It is common to have multiple safety and security barriers and a variety of mechanism that shut down if a level reaches critical values. However, these systems can lose its function, intentionally or unintentionally. It is difficult to have full overview of a complex system with many components, units, functions, and participants, such as suppliers and contractors. Therefore, it may be difficult to detect errors caused by faulty maintenance, installation or cyberattacks. The root cause of an accident in a complex system will contain failures at several levels. A combination of organizational, technical, and human factors causes the accident or incident to occur, hence the importance of creating barriers at all three levels.

The continuation of the analysis looks at root causes, barriers and potential consequences caused by the weak points. An evaluation of existing and a proposal of new barriers should be done in a three-step process. These are steps taken from CRIOP Scenario Analysis (Johnsen et al, 2004, page 126).

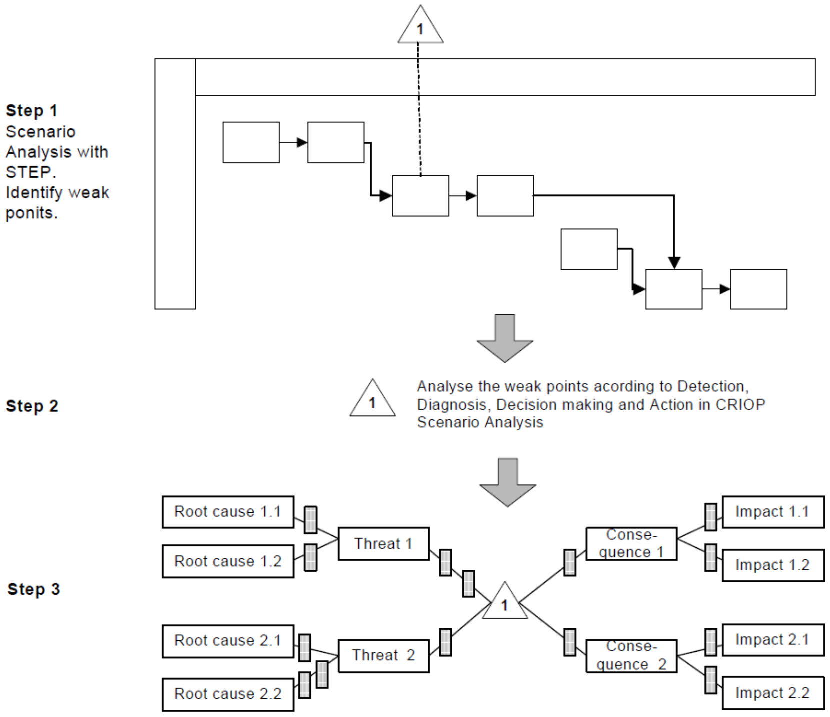

Step 1
Scenario Analysis with STEP. Identify weak ponits.
1
Step 2
1
Analyse the weak points acording to Detection, Diagnosis, Decision making and Action in CRIOP Scenario Analysis
Step 3
Root cause 1.1
Root cause 1.2
Threat 1
Root cause 2.1
Root cause 2.2
Threat 2
1
Conse-quence 1
Conse-quence 2
Impact 1.1
Impact 1.2
Impact 2.1
Impact 2.2

Figure 4.4.3.2– Evaluating weak points in combination with safety barrier analysis (Jatuun et al., 2007)

(Shaded grey blocks represent barriers)

Step 1: Identify and enumerate weak points based off the scenario analysis. It would be like a FMEA or a FMECA analysis.

Step 2: Analyze the weak points according to the ability to detect, diagnose, decide, and power to act.

Step 3: Identify the relationship between root causes, threats, weak points, consequences and impact. Evaluate existing and missing barriers to hinder root cause, reduce consequence and impact.

The process should emphasize the weak points and suggest new barriers related to the weak points. For the most part will the barriers be divided into organizational, technical, and human factors.

4. Document safety and security recommendations and evaluate the incident response process.

Once the analysis has identified weak points and suggested barriers, the prioritizing of these suggestion must be made. A cost/benefit analysis and the ALARP principle should govern the implementation of these measures. A record or a database of the incidents should then be created. Containing details such as a description of the identified weak points, suggestions of barriers and security measures, cost/benefit analysis, and a record of the persons involved and responsible for the recommendations. This falls hand in hand with the documentation of the incident. This is a document that can be utilized in sharing best practices and inform other actors. It is also the basis for further learning and the incident can be analyzed at a later point. An example of documentation is found in Jatuun et al (2007) appendix E, page 66.

The goal of the evaluation of the incident handling process is to improve future practices; the managing of incidents and the way incidents are documented. The results of the STEP analysis and the evaluation of the incident handling process can be used in the other phases to increase the learning culture. *It is important to sustain the open reporting culture, spreading information about the incident in an open and participatory way* (Jatuun et al, 2007, page 50). It is important that the relevant personnel get informed about the attacks, weaknesses, consequences, and errors in equipment. Non-technical personnel can benefit from hearing about the incident in a pedagogic way, while technical personnel should see the detailed step analysis and the barrier analysis. The learning phase's results will help create understanding, awareness and improve attitudes among the staff related to cyberattacks and digital risk (and of course other non-ICT incidents). The organization will know why the incident occurred and what caused it. Further improvement of processes and barriers will reduce the organizational, technical and human factor related issues.

4.4.4 Performance Indicators for Incident Response Management

The SINTEF report (Jaatun et al., 2007) presents 9 different performance indicators (table 4.4.4):

Table 4.4.4 – Performance Indicators for IR (Jaatun et al., 2007)

Phase of IR management	**Performance indicator**
Plan and prepare	*1. Rating system for the quality of the IR management system*
	2.Assessment of information security culture with respect to IR
	3. Average order of feedback
Detect and recover	*4. Number of incidents responded to*
	5. Average time spent on responding pr incidents
Learn	*6. Total consequences of incidents*
	7. Number of incidents of high loss
	8. Downtime of SCADA systems due to incidents
	9. Total costs related to incident response

Indicator 1: *Rating system for the quality of the incident response management systems (IRM).*

An assessment of feedback systems, goals, documentation, management commitment, and education will give an indication of the IRM system quality. Also, considerations regarding the implementation of security mechanisms and that they are functional. The organization needs to consider that the IRM plan is appropriate for the context of the organization.

Indicator 2*: Assessment of information security culture with respect to incident response.*

The information (and cyber) security culture encompasses the shared values and beliefs of the organization through its employees. This means that the organization's information and cyber security management system is visible through, for example employee commitment and deviation reporting culture. The organization should develop measures such as training and awareness campaigns to increase the commitment to the planned incident response management system (Jaatun et al, 2007).

Indicator 3: *Average order of feedback.*

The lesson learned must be communicated to other parts of the organization, such as management, employees, operators, suppliers, and others (Jaatun et al., 2007). The indicator can tell if the organization is mostly correcting deviation, or has a proactive attitude to incident response.

Indicator 4: *Number of incidents responded to.*

This is indication changes with time and external factors such as the threat picture. It is an indicator that should be considered with care. However, it can indicate that the incident repose mechanism is working.

Indicator 5: *Average time spent on responding per incidents.*

The time from incident detection to recovery can be measured. This can give an indication that the efficiency of the incident response is improving over time.

Indicator 6: *Total consequences of incidents.*

The main goal of incident response is to reduce the consequences of incidents. An overview of the total consequences related to one incident, can be scaled to financial loss, and can be used as a risk prioritize tool.

Indicator 7: *Number of incidents of high loss.*

This indicator measures the number of incidents that causes high losses. This indicator can be used to prioritize and draw attention to the need for incident response management. It functions as a great communication tool for stakeholders and decision-makers (Jaatun et al., 2007).

Indicator 8: *Downtime of SCADA systems due to incidents.*

This is a measurement of downtime due to an incident. This is relevant in combination with indicator 4 and can together indicate the efficiency of the incident response.

Indicator 9: *Total costs related to incident response.*

The incident response management requires financing, both in preparation and in active response and learning. The total cost in combination with the total consequence indicator, can determine if there is a reasonable balance between incident response investments and the level of consequences of incidents (Jaatun et al., 2007).

This concludes the literature study and the next chapter will continue with the analysis.

Chapter 5 – Analysis

5.1 Analysis Background, Structure and Approach

Background

The cyber threat is increasing towards digital systems and organizations modernize their operation with digital technology and digital infrastructures. In what way does the organizations respond to the increasing cyber threat, and what are their counter measures to reduce cyber risk? How do long value/supply chains affect their cyber risk exposure? How do they balance innovation with cyber security? How does the future of digitalization affect cyber security? These are questions that will be answered in this analysis. The purpose of the qualitative analysis is to find areas of improvement, and highlight industry similarities, key issues and challenges.

Analysis Structure

The qualitative analysis is divided into two parts. The first part will compare the three organizations to each other and find similarities in industry solutions, key issues and challenges. The second part will compare the organizations' cyber security capabilities and find areas of improvement. The analysis structure and background is shown in figure 5.1.

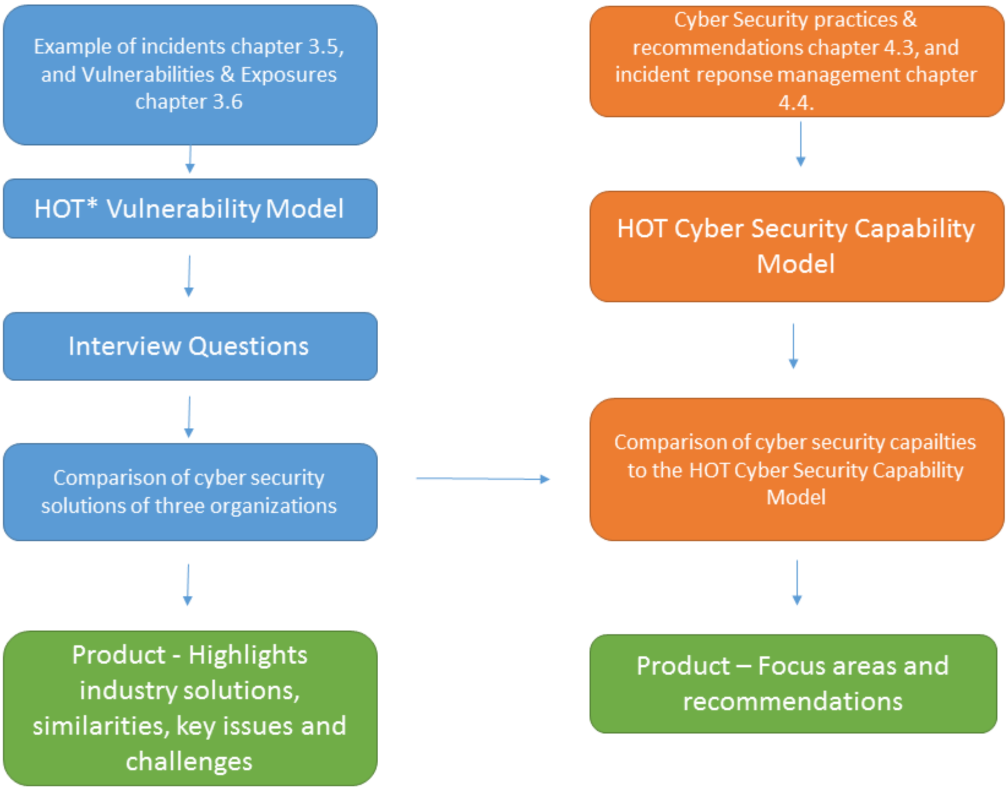

Example of incidents chapter 3.5, and Vulnerabilities & Exposures chapter 3.6
HOT* Vulnerability Model
Interview Questions
Comparison of cyber security solutions of three organizations
Product - Highlights industry solutions, similarities, key issues and challenges
Cyber Security practices & recommendations chapter 4.3, and incident reponse management chapter 4.4.
HOT Cyber Security Capability Model
Comparison of cyber security capailties to the HOT Cyber Security Capability Model
Product – Focus areas and recommendations

Figure 5.1– Analysis Structure and Background

*HOT= Human, organizational and technological

The Interview Process

The questions for the interview is based on the HOT Vulnerability Model, described in chapter 5.2.1, and additional questions are provided about cyberattacks and the future of digitalization. This is because the organizations face the same vulnerabilities and may produce different cyber security solutions. This makes it possible to compare the industry solutions. The industry solutions are then compared to the HOT CS capability model, described in chapter 5.2.2. The qualitative approach makes it possible to go in depth on each subject and gain insight into the organization. There are no definitive and correct solutions to cyber security and there are elements that are difficult to measure. Therefore, the qualitative approach will better understand why security measures are implemented and what the purpose and strategy is.

The interview process is based around a semi-structured interview guide, found in Appendix A. The interviews were conducted via Skype for Business. The interviews were conducted via skype for business during the period from 28.03.2017 to 27.04.2017. The data and information is collected from the interviews and email correspondence.

The organizations were chosen based on their importance in society, size, and their use of digital systems. Their importance or criticality means that they must have procedures for emergency, because of the potential impact and consequences their operation has for the public. Their size and use of digital systems increases the likelihood for implementing cyber security.

Limitations

The semi-structured interview process does not follow the HOT Vulnerability Model consistently, but includes the model's main points. This may present some inconsistency in the two parts of the analysis comparison. This means that some CS capabilities will be answered blank. It is also difficult to gain enough overview and insight to each organization's operation and systems. There are certain aspects of security that the organizations cannot talk about. The consequence is that some answers become "light".

5.2 Models

This chapter presents the criteria and description of the two comparison models – HOT Vulnerability Model and HOT Cyber Security Model. These models approach cyber security from a human, organizational, and technological (HOT) perspective.

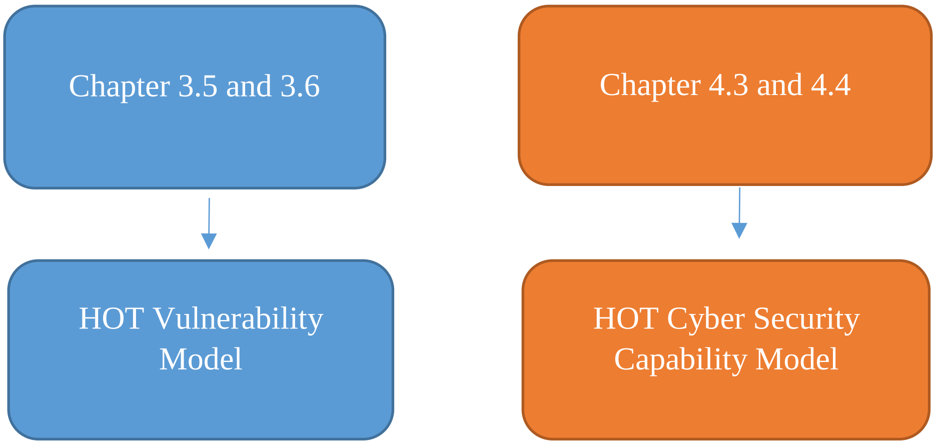


Figure 5.2 - Model Background

5.2.1 HOT Vulnerability Model

Criteria & Validation

The criteria for this model is derived from chapter 3.5 and 3.6 (figure 5.2). The vulnerabilities described in these chapters makes up the vulnerability model that encompasses the HOT aspects of cyber security. Organizations face vulnerabilities from different perspectives. Human-, organizational-, and technological factors needs to be identified to map out vulnerabilities in the organization. This is crucial in securing the values in the organization. The threat agents will attack from different vectors which concerns different aspects of the organization. The point of this model is to present the vulnerabilities in a holistic view and be a guide for organizations to follow in their cyber security work. The model looks at general organizational concepts of vulnerability and may lack the ICT technical depth. The vulnerabilities can be considered into these categories:

Human Vulnerabilities:

- Competence

Employee ICT competence is the foundation for good user behavior. This encompasses for example how to react to incidences, how to manage external media devices, and information/data sharing.

- Compliance

The willingness to comply to the security routines is important. A deviation from the security routines because of convenience or time constraints is a vulnerability.

- Awareness

Situational awareness in production areas or at the desktop can reduce the occurrence of unwanted events and contribute to a good reporting and security culture.

Organizational Vulnerabilities:

- Security Framework

This is the basis which the organization chooses to drive the cyber security work. Organizations usually have established a framework for information security management and traditional HSE (health, safety and environment). The lack of a framework will greatly decrease the quality of the security activities, and represent an organizational vulnerability.

- Risk management

The ability to perform value, threat, and vulnerability assessments is critical for gaining an overview of the organization operation and system, threats, and the ability to assess the effectiveness of the security measures and activities. The risk management and assessments should have a practical impact and should not be done out of compliance to regulations. The lack of a realistic risk assessment including the different disciplines of the organization is vulnerability.

- Leadership engagement

The leadership, meaning decision-makers, can easily lack the technical understanding of ICT and engineering systems, and therefore affect the security activities in a negative way. The organization may get into unwanted situations due to lack of understanding related to the use of third parties. The lack of resource allocation to cyber security activities and technology is a decision-maker's responsibility.

- Collaboration

Lack of cooperation may cause the organization to lack understanding of the threat and lack the ability to find useful safety measures. Organization is at risk of becoming outdated as it lacks external input from organizations that have different experience and solutions.

- Employee Training

Employees can contribute to a more secure organization. ICT behavior, awareness and competence is an organizational responsibility. The lack of ICT competence and awareness can lead to unwanted events due to lack of situational awareness, technological competence, and reporting routines.

- Emergency Preparedness

The lack of ICT emergency preparedness, meaning emergency drill, documented procedures, reporting channels, will affect the organization's ability to reduce consequences.

- Value/supply chain management

As value/supply chains become fragmented, it is important to understand how organizations and systems are connected. Additionally, the use of third parties may challenge security assurance, control and quality management. This means that the gap between the customer and service provider, can reduce the customers ownership to the operation/system.

Technological Vulnerabilities:

- Consequence reduction

The organization's ability to reduce the consequence of ICT incidents. This includes functions such as system recovery, redundancies, and the ability to proceed the operation with manual procedures.

- Incident Detection and response

This encompasses the organization's ability to detect incidences and escalate the response according to the situation. This includes general intrusion detection systems, incident response, and emergency response functions.

- User and access control

This is the organization's user and access control capabilities. This includes a general overview of system users, their access and regular overview revisions.

- System technology management

This is the organization's ability to secure its equipment, software, hardware, system, and operation. This includes for example utilizing modern security technology, patching routines, and decommissioning of old ICT equipment.

- Physical security

The organization's ability to implement physical barriers, security zones, and security measures.

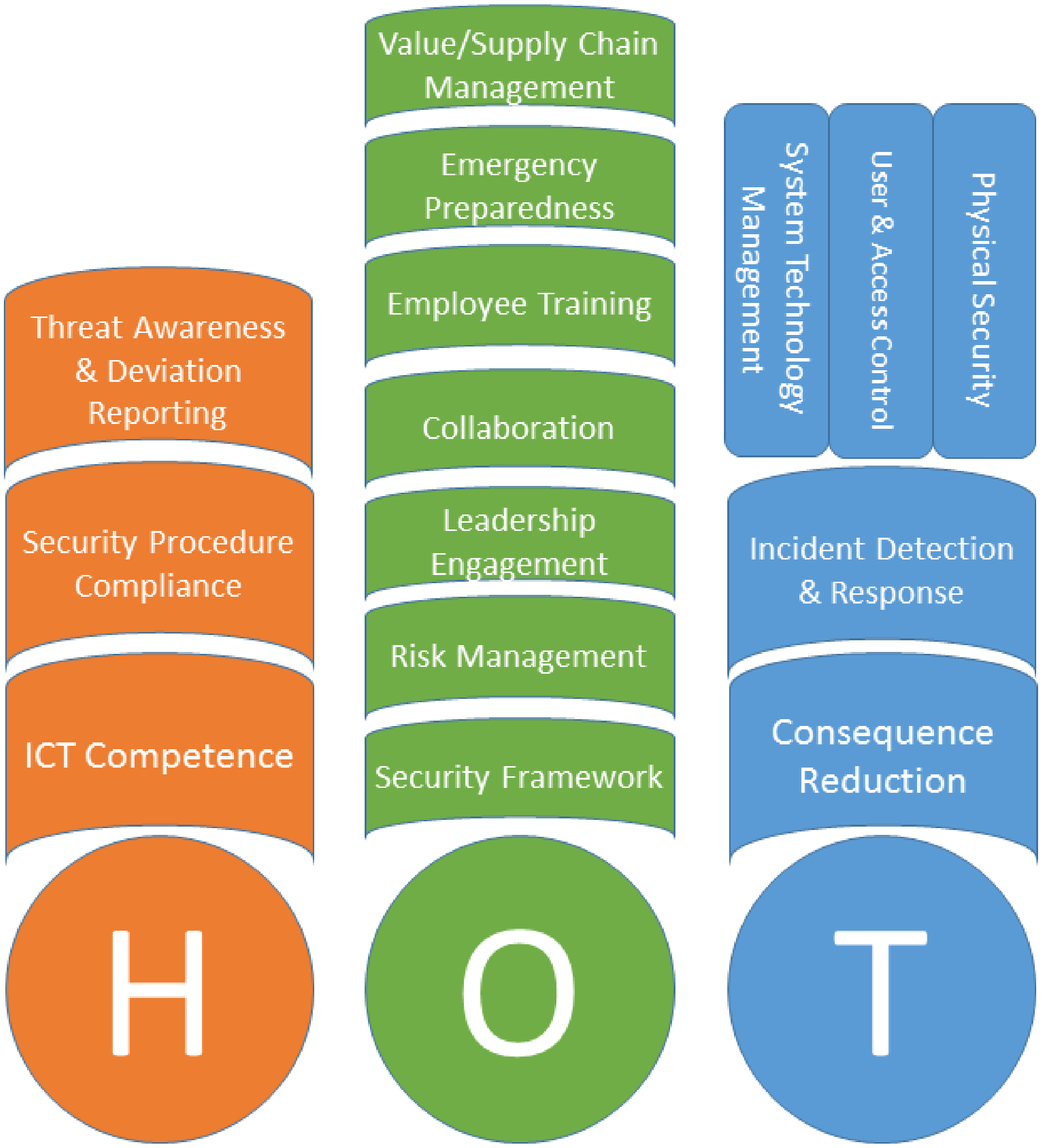


Figure 5.2.1 – HOT Vulnerability Model

*The vertical boxes in the technological part represents the three main attack vectors.

5.2.2 HOT Cyber Security Capability Model

Criteria & Validation

This model is based on the security measures and recommendations from chapter 4.3 and 4.4 (figure 5.2). It combines the cyber security practices and recommendations to make the HOT Cyber Security Capability Model. The model continues the HOT perspective in order to encompass a holistic organizational approach to cyber security. The HOT capability model is not a benchmark, but a guide for cyber security capabilities.

The HOT Cyber Security Capability Model is a self-assessment tool for organizations to find improvement areas and approach cyber security from a HOT perspective.

Human Cyber Security Capabilities

Humans play an important role in ICT security. Employee behavior and competence contributes to the organization’s security culture and can be a good preventive and risk reducing measure. Phishing attempts and other attacks will at some point always succeed, but the success frequency can be reduced by implementing human barriers. Employee’s social media profiles can be an information source for threat agents. This creates the need for social media guidelines, as well as general information and data sharing guidelines. The organizations should devote resources to employee training programs and threat awareness campaigns. A safety culture that runs throughout the organization, motivated by leaders, allows more people to understand the importance of following the safety procedures. This will increase employee security procedure compliance and can produce an effective reporting culture. Table 5.2.2A describes the human cyber security capabilities.

Table 5.2.2A – Description of Human Cyber Security Capabilities

1) End-user ICT competence & behavior

The end-user’s ICT capabilities and general ICT-related behavior. The end-user ICT competence is the foundation for good user behavior. This will increase the general security culture.

2) Awareness and willingness to learn

Employee’s willingness to learn and contribute to the security culture, as well as their situational and threat picture awareness.

3) Security routine compliance

Employee’s ability to follow the security routines, even with time constraints. Managers should motivate security routine compliance. This is an important part of the overall organizational security culture.

4) Incident and deviation reporting culture

Employee’s ability to report deviations and incidences through the right communication channels. This is an indicator that the safety culture has gained a foothold in the organization.

Organizational Cyber Security Capabilities

Organizational vulnerabilities can be difficult to notice as there may not exist any evaluation procedures. Most employees are not involved in formulating a strategy or making investment decisions, and those who do are not necessarily capable evaluate themselves or the organization. It is important to have a framework that evaluates the effectiveness of leadership and security measures, and ensures the improvement of unsatisfactory security measures. This means that the organization needs to ensure that there are measurable parameters for security and that there is allocated resources for security implementing, operation and evaluation. There should be an overview of the competence needs in the organization's ICT and cyber security, ensuring that the competence correlates with the use of technology in the organization. This will also be important when purchasing technical solutions for security. Value, threat and vulnerability assessments should make the organization capable of evaluating the security condition of the organization.

Strict access control routines are needed to avoid users with unnecessary access. Strict patching routines will ensure that the security technology and systems are resilient to current threats. Emergency plans should be documented and practices on a regular basis, and there should be clear roles, responsibilities and reporting channels for incident response and security activities. Organizations should avoid designing critical components or functions without redundancy. This is visible in systems where a critical point has one connection to the rest of the system, also, in situations where the organization is dependent on third parties, such as business partners or suppliers to perform a critical function. System logging and a management for system change, incident and deviation will increase the system overview and the organization's ability to find errors, deviation, and perform measures such as system recover.

The security of an organization or an industry is a collaborative effort between the organization, supervisory authorities and security partners. The CERTs provide a professional cyber security community across industrial sectors and comes with many benefits. International seminars can provide professional discussions of the threat picture and can be an opportunity to share experiences. The industry regulators and legislators have a responsibility to engage in industry cyber security conversations and interact with the different organization. The use of third parties presents a challenge in security assurance, control and security quality management. This is a risk the organizations must evaluate thoroughly. There are technological and business aspects that can present unseen vulnerabilities to the organization. Table 5.2.2B describes the orgnaizational cyber security capabilities.

Table 5.2.2B – Description of Organizational Cyber Security Capabilities

1) Ownership

The organization’s ability to exercise ownership of the operation. Regardless of how the operation is performed, for example by utilizing ICT services, outsourcing, etc., must the organization own the responsibility and govern the process.

2) ICT and Cyber Security Competence

The organization’s understanding of digital vulnerability and their ability to implement and evaluate protective measures against digital threats.

3) Cyber Security Framework

The basis for all cyber security activities. Often an integrated part of the information security management framework.

4) Risk Management

The ability to perform satisfactory value, threat and vulnerability assessments, implement and evaluate practicality and effectiveness of barriers and security measures. This is presented in chapter 3.2.

5) Security Management & Incident Response Management

The ability to manage, evaluate and improve security activities, leadership, and incident response capabilities. As well as, the organization’s ability to develop and evaluate security objectives and targets.

6) Documentation and formalization

The documentation and formalization of routines, emergency procedures, security activities & objectives, roles, responsibilities, and reporting channels.

7) Security Resource allocation

The organization’s allocation of resources to cyber security activities.

8) System overview

An overview or visualization of the operation systems, networks, etc.

9) Leadership engagement and security culture

The leadership’s ability to visibly engage in security activities and the organization’s security culture.

10) *Collaboration*

The organization’s collaboration partners, for example international and national industry organizations, CERTs, security technology producers, and authorities.

11) Supervisory authority engagement and industry regulations

The perceived engagement of industry supervisory authority and the practicality of industry regulations and legislations.

12) Third party security assurance, control and quality management

Awareness of supply chain/value chain risks and the organization’s ability to acquire third party cyber security assurance, control and quality management related to exposure to cyber risk.

Technological Cyber Security Capabilities

The technological innovations create both increased dependency and interconnection. This forms the basis for the vulnerabilities in digital engineering solutions. The ability to maintain the core function after or during an event is vital for critical organizations in society. This can be achieved by having system redundancies in critical systems or at component level, system recovery functions, or manual processes that take over once the digital system fails. Complete duplicates of critical systems may be too expensive to sustain for some organizations.

The physical aspect of security is also important. Separation of networks and domains, security zones and protection against burglaries provides security in the link between the physical and digital domain. System access control and a limited distribution of admin rights prevents unauthorized changes to the systems. System traffic logs enables the recovery functions, and serves as a tool for detecting strange system behavior. Application whitelisting and role-based end-user access allows the end-users to access preapproved applications, which prevents unauthorized programs (for example malware) to run. Modern firewalls, email filters, and other security technology which is in line between the organization and the internet are most effective in prohibiting most cyberattacks. Detect and response functions are the mechanism that makes the organization capable of managing cyberattacks that bypasses the traditional security measures. This is an important dynamic barrier and is a key element in reducing the consequences of cyberattacks and an element in continuous improvement. Table 5.2.2C describes the technological cyber security capabilities.

Table 5.2.2C - Description of Technological Cyber Security Capabilities

- _Manual procedures*_

The organization’s ability to perform the core operation without digital systems. For example, if a hospital’s digital journal system fails, the hospital continues to treat their patients.

- _System redundancies*_

These are redundancies at component or system level for critical functions of the operation. For example, overlapping wireless zones, multiple data centers, hot-standby duplications of operation centers.

- _System recovery functions*_

This is enabled by the system logs and makes it possible for the organization to roll back the system to a previous secure state.

- _Incident Detection and Response functions_

The organization’s technical ability to detect and form a response to incidences. This is an active and dynamic function that detects and responds to unauthorized activities (for example malware) or odd behavior in the system. This mechanism utilizes sensors that are placed in the digital system and alerts if it detects any suspicious behavior. The initial response function is commonly performed by a on duty security officer. The situation is escalated based on the severity of the event.

- _User/role-based access control_

The organization’s technical ability to securely manage users and user access. A user has been given system access based on the user role. Which means that the system access is limited to the relevant applications, databases, etc. The access control register must be frequently updated to ensure that the right users have the right access.

- _Application whitelisting_

This function allows preapproved applications to run. Any application (malware) which is not approved is terminated, unless it can bypass the application whitelist.

- _Decommissioning of old ICT software and architecture_

The use of old, unsupported software and hardware is a weak point in the organization. These assets must be decommissioned and replaced with new, supported and secure assets.

- _System traffic logs_

The system traffic log is a register and a tool for managing system change, incidents, and problems. It also enables the system recovery functions.

- _Strict Patching Routines_

Once an exploit has been detected by security technology companies or system manufacturers, it must be patched. The time from detection to the release of the patch is most critical, and is a perfect time to perform a cyberattack. The organization must have strict patching routines and assess the criticality of each patch.

- _Limited distribution of admin rights_

The organization should have an overview of distributed admin rights and make sure that the individuals that have these right, need them. This is a challenge when using third parties and outsourcing.

- _Modern Security Technology_

The organization must orient themselves in the modern security technology market. Basic and traditional security technology, such as firewall and email filter, prohibits most cyberattacks.

- _Separate networks and domains_

The separation of administrative networks and production (SCADA/ICS) networks reduces interconnectivity and access points.

- _Security zones and physical distinctions_

The physical distinction between publicly accessible areas, employees only, and limited access. This translates into for example publicly accessible wifi vs sensitive networks, offices vs common room vs control room, etc.

- *Protection against burglaries*

Physical barriers and alarm systems in critical rooms, data centers, equipment in the field, etc.

*consequence reduction/last resort solutions

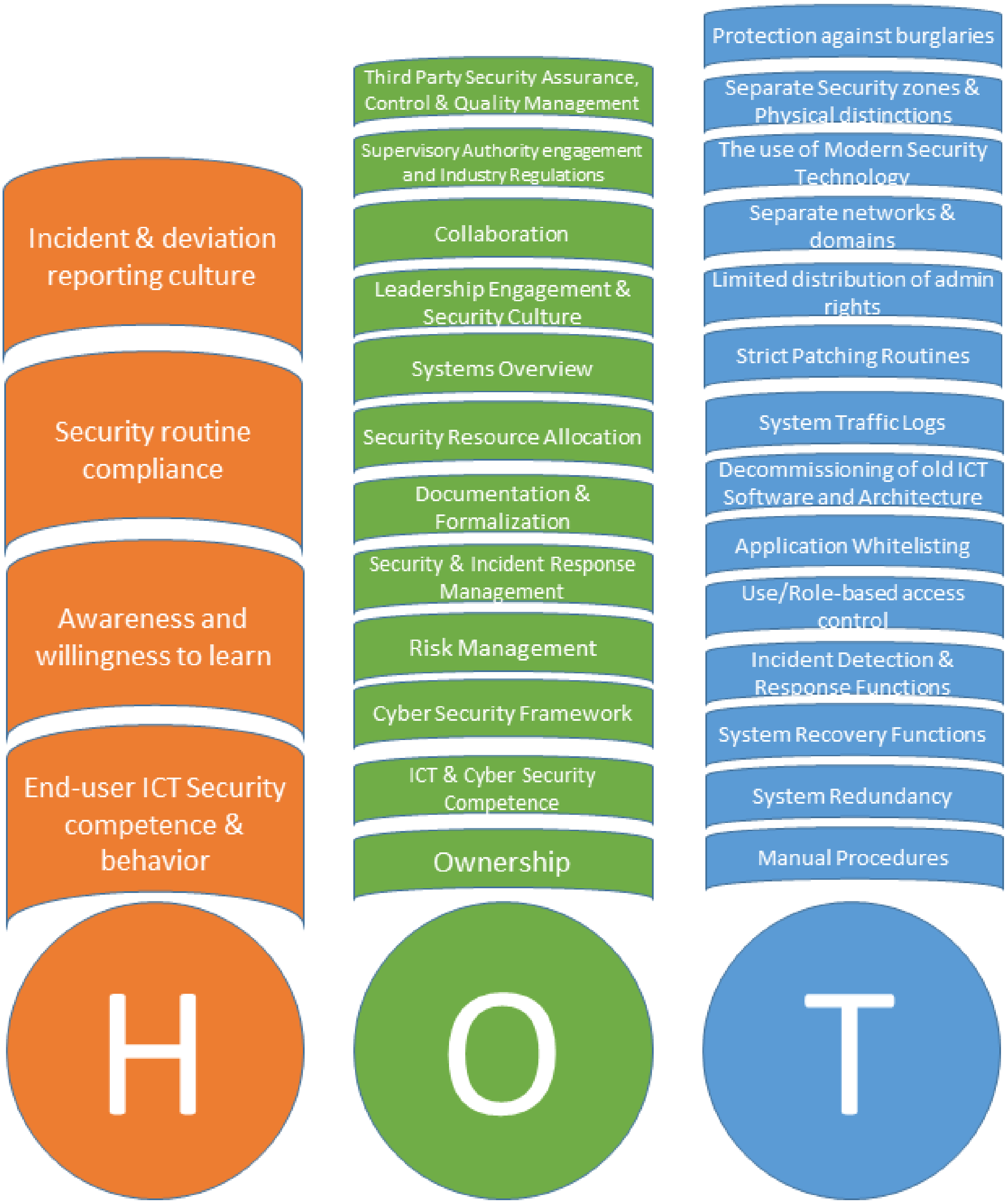

Incident & deviation reporting culture
Security routine compliance
Awareness and willingness to learn
End-user ICT Security competence & behavior
H
Third Party Security Assurance, Control & Quality Management
Supervisory Authority engagement and Industry Regulations
Collaboration
Leadership Engagement & Security Culture
Systems Overview
Security Resource Allocation
Documentation & Formalization
Security & Incident Response Management
Risk Management
Cyber Security Framework
ICT & Cyber Security Competence
Ownership
O
Protection against burglaries
Separate Security zones & Physical distinctions
The use of Modern Security Technology
Separate networks & domains
Limited distribution of admin rights
Strict Patching Routines
System Traffic Logs
Decommissioning of old ICT Software and Architecture
Application Whitelisting
Use/Role-based access control
Incident Detection & Response Functions
System Recovery Functions
System Redundancy
Manual Procedures
T

Figure 5.2.2 – HOT Cyber Security Capability Model

5.3 Three Organizations, Three Industrial Sectors

5.3.1 Helse Vest IKT – ICT Partner for the Helse Vest

The organization deliver ICT services for and is owned by Helse Vest. They are using innovative ICT solutions to improve health services. Its customers are public hospitals and private healthcare providers in the region. Helse Vest IKT has an estimated revenue of 950 million NOK and has 489 employees. The interviewee is ICT Security Manager Lars Erik Baugstø-Hartvigsen.

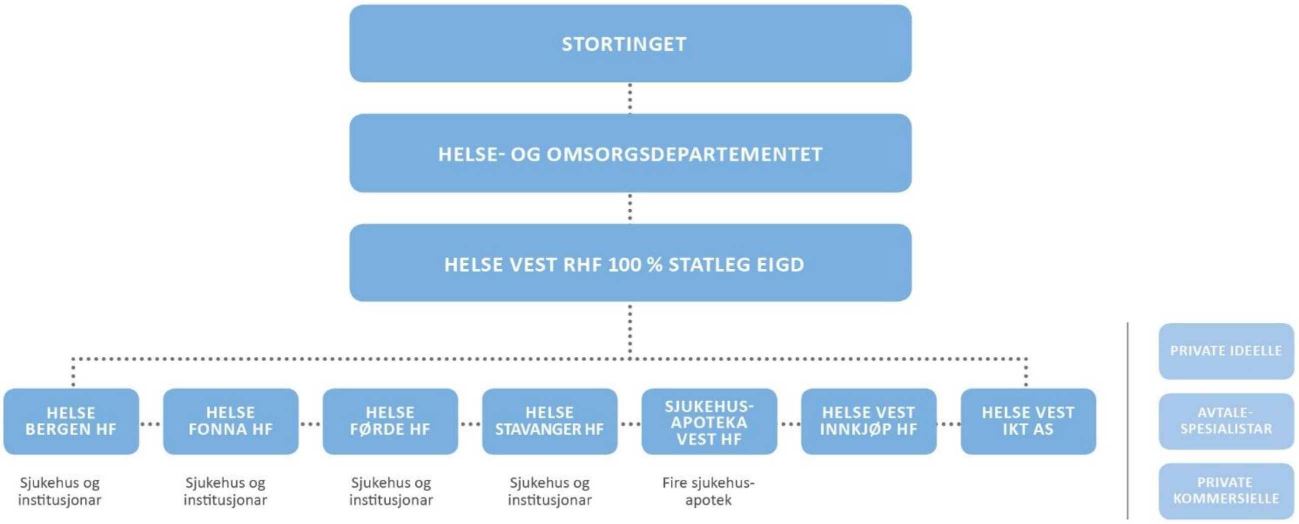


Figure 5.3.1 - Helse Vest IKT Organization Chart

Helse Vest IKT are involved in services within operation, production and user support, user equipment, system management and system integration, introduction, training, phasing out and system change, and counseling and project management.

5.3.2 Bane Nor SF – Railway Developer and Operator

Bane Nor is the main railway infrastructure developer and operator in Norway. The previously named Jernbaneverket, became Bane Nor in 2017. It is now a state enterprise. The ongoing organizational and technological change causes the operation and administration to be in development. The organization has 4 500 employees and has change from being government officials to employees of a state-owned enterprise. This has impacted the way the organization is structured, with a board and corporate management, and has given a different financial basis and business model. The organization's projects are mostly financed through the Ministry of Transport and Communications.

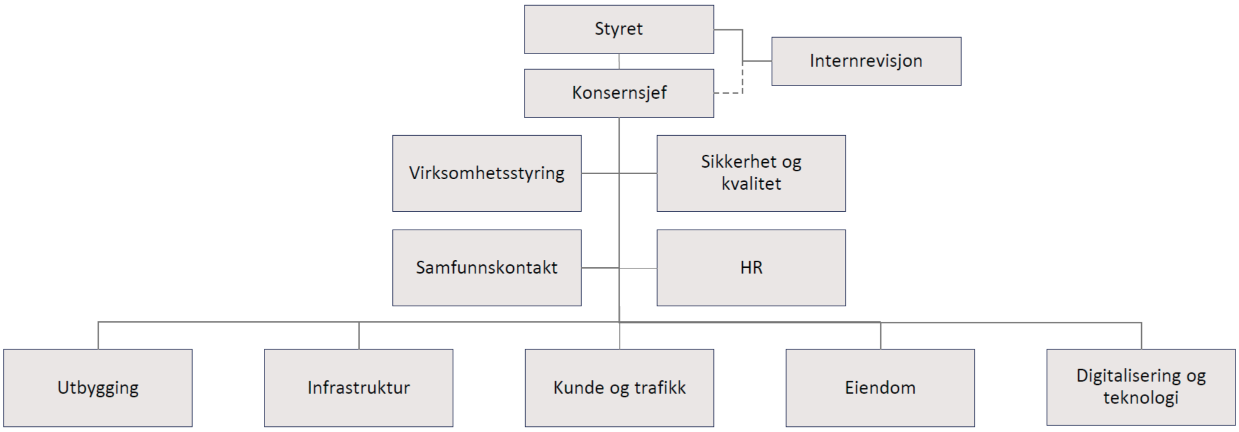


Figure 5.3.2 - Bane Nor Organization Chart

The Digitalization and Technology Division is responsible for development and deliveries within digitalization and technology for the entire enterprise. The interviewees are Arild Nybrodahl, FDV Manager (Asset Management, operation and maintenance) and Lars Strømmen, Operational ICT Security Manager. They are responsible for operations and Rail ICT security. The administrative ICT network is a separate operation.

5.3.3 Hafslund Nett – Power Distribution Company

The interviewee is Jon Andreas Pretorius ICT manager for Hafslund Nett. Hafslund Nett is responsible for the power distribution for the three municipalities Oslo, Akershus and Østfold. The energy company have 340 employees and have a revenue of about 20 billion NOK. Shortly before the interview did Hafslund announce that the municipality of Oslo were to by the entire organization and separate the operation. Hafslund Nett's operation will continue as before, and not be substantially affected by the event.

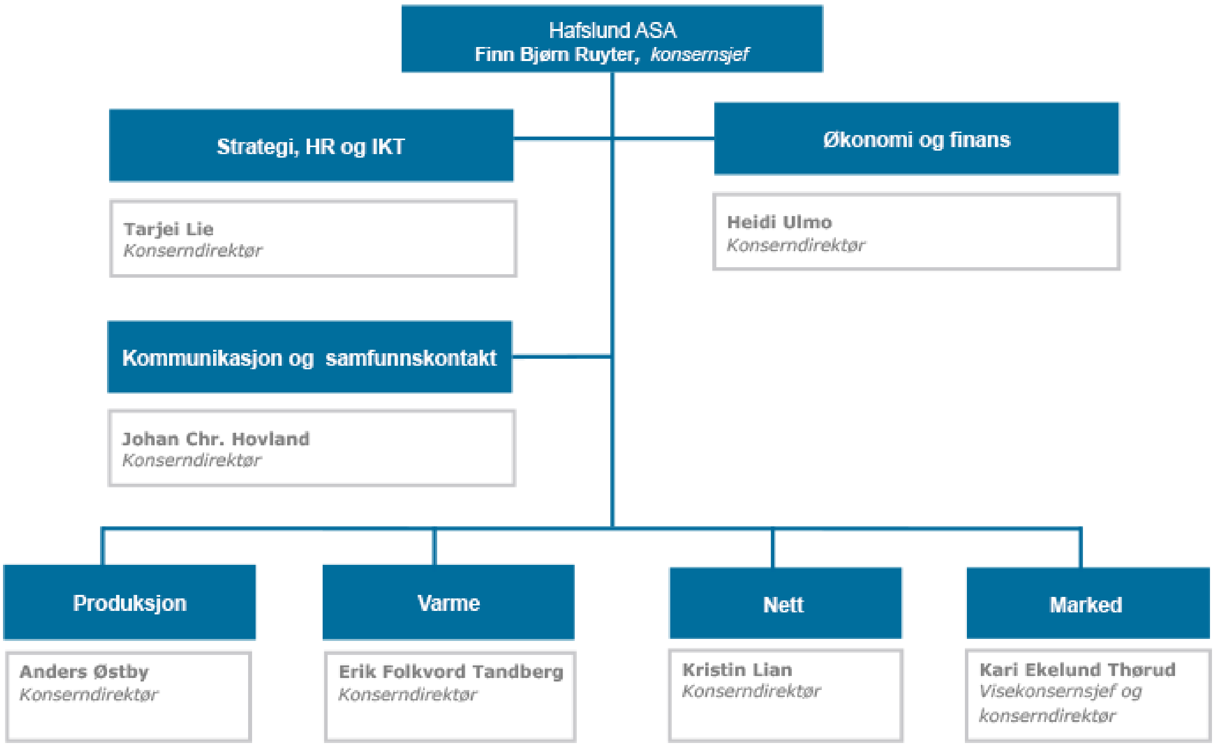


Figure 5.3.3 – Hafslund Organization Chart

They have a department dedicated for SCADA, automation and remote control. Jon Andreas Pretorius is responsible for the overall ICT architecture and security, which also include the SCADA network. They experience that the separate professional environments increasingly overlap.

5.4 Part 1 - Comparison of Industry Solutions

5.4.1 Digitalization and technology

Technology and Benefits

Helse Vest IKT:

The organization adopts new digital technology. In collaboration with its customers, the hospitals, health authorities and other service recipients, they carry out new projects. These projects include:

- Rule-based process automation (RPA)

This is a software robot that perform repetitive work processes. These are tasks that are very repetitive and monotonous for a human to perform. Which means that employees can focus on other, more important tasks. The RPA performs two task, the first is an automated resending of epicrisis, the second is an automated planning process for x-ray referrals. These tasks include sensitive personal information and it is beneficial that no humans are involved in the process. This preserves privacy. In addition, the RPA is proven to be very cost-effective. As an example, the resending of epicrisis was paid back within two months.

- Digital patient journals

The change from paper journals to electronic journals have been for many years. But, it is a significant improvement in the work flow and employees prefer the electronic process over the paper process. The digital patient journals are stored and operated in a system called DIPS. The patients overview of who has had access to their journal, via an access log.

- Electronic pharmaceutical logistics (in Norwegian: elektronisk pasientkurve)

Health personnel use this document for documenting medication dosages, what treatment the patients get, and other information. This is an important tool in health care. The digitalization of this process increases the quality, information security and availability due to the constantly updated data, access control, and the potential for collaboration between several health personnel. The former paper process made the document exposed for bystanders, which the electronic version does not. The patient safety is increased by avoiding wrong dosages and avoiding that combinations of medicine gives unwanted consequences. The system itself is also compatible with other patient treatment systems, meaning that the information does not have to be transferred manually.

- Digital media archive

There are massive amounts of media files in hospitals. These files need to be centralized, stored and structured in a secure place. The digital media archive makes it faster to access data and increases the availability.

- Interaction with patients online

This allows patients and health personnel to have a dialog, change meeting times, etc. This is a part of a larger project called Vestlandspasienten (patient of western Norway).

The new technology benefits the patient by improving treatment quality, information and patient security, and data and communication availability. The causes the health services to be made around and for the patient. The success of Helse Vest and Helse Vest IKT will also benefit the other regional health care services by transferring knowledge across the regional organizations. In the end, this synergy effect will benefit the patients and patient treatment quality.

Bane Nor:
Bane Nor's operation encompasses many different technologies. The disciplines include power supply & distribution, signal systems, SCADA systems, and transmission technology. The digitalization is a large technological project, but it is an even bigger organizational project. The future needs are different than previous. There will be developing of the existing assets and resources and some must be gained through new competence and knowledge. The digitalization impacts a large part of Bane Nor's operation and production. It is believed that Bane Nor has the largest digitalization project in Norway. The digitalization impacts functions, technologies and projects such as:

- KARI

KARI is a project that include different ICT-services related to customer information placed in railway stations. These are, for example, real-time updates and alerts of deviations, delays, and expected arrival.

- ERTMS

ERTMS is a European standard for digital software-based signal system. Signal failure are a common cause for delays. The new system will decrease failures and delays, as well as increase security. Most of the signal systems are old and requires renewal. This will impact the railway efficiency and security. The project ends in 2030 and is fully financed for the whole period. The project size is 26 billion NOK. This include the implementation of the signal system and the decommissioning of the old equipment.

- FIDO

FIDO is the traffic management system which communicates with the drivers. The traffic management system is found in 8 different locations in Norway. It shares the same function as compared with traffic control in aviation. Traffic lights and signs will be replaced with direct electronic communication with the driver. This information will be distributed through mobile networks and data connections.

- GSM-R and fiber optics

Bane Nor has a large transmission technical infrastructure with its own full service mobile network operator, and 5 000-kilometer fiber cable lines running through the country.

- Several power production sites

The trains run on power and needs a reliable power supply. There is a separate SCADA system for distributing power to the railway, which is going through an upgrade.

- Condition-based monitoring

There is an initiative to adapt to the future of maintenance. This initiative includes installing sensors on objects to enable monitoring. These objects have not previously been monitored and has a great potential to lower the maintenance cost.

The benefits are increased efficiency and operational stability. Condition-based monitoring dramatically decreases cost of maintenance. The standardization of IP and the ERTMS makes troubleshooting and finding faulty components easier than before, as well as facilitating for better system overview and monitoring. It will also make it easier to create redundancies, such as several connection points for critical components in the system. In the old analogue system, the maintenance would be costly and it would be difficult to identify faulty components, the accuracy would be limited to a subsystem. These benefits cause increased customers satisfaction.

The transition to digital technology is highly visible in cost efficiency. However, if the organization does not develop and evolve its way of operating, the potential can be lost in poor management and cumbersome procedures. This creates new requirements for investing as much in personnel and competence as hardware and equipment. A change in mindset is a part of the transition, also regarding cyber security. There is a lack of conceptual framework and understanding of this discipline. The relaybased systems have not previously been exposed to the risk of cyberattacks. The old copper systems were mostly exposed for local sabotage. The challenge is to understand the new threat picture and how it affects Bane Nor's operations.

Hafslund Nett:

Hafslund Nett has traditionally run ICT-operations with a SCADA system and a standard administrative domain with classic major core systems and an integration bus of some kind. These functions have been characterized as monolithic and "silo-based". Today**,** the focus is on information orientation. The development of a central data management system, called dataNav, breaks down the silos. It processes all the available data from the different systems and makes it available. This is a datahub-driven or an information centric architecture which is the basis for what Hafslund Nett sees as the future of power distribution. Most of the future activities revolves around analyzing and utilizing the data to make better decisions related to investment, operations and maintenance. For example, predictive maintenance, customer self-service, and automation of processes.

Hafslund is using Lean startup for development and testing of hypothesizes and learning. This helps create a system understanding and in-house competence of new technologies. Hafslund prefers this way of developing technology to purchasing a service form a third party. For example, the management of predictive maintenance. This enables the organization to learn during the process and develop system understanding among employees.

Hafslund is in the process of installing Smart AMS (power meters) in all the customer locations. This is required by regulations from NVE (Norwegian Water Resources and Energy Directorate) and must be completed by 2019. The AMS collects a variety of data from the customers and the distribution system, such as customer consumption, ground faults, voltage level, etc. This gives Hafslund Nett 700 000 extra sensors in the network. This data can be used in predicative maintenance and to look for consummation patterns. Example of changes:

- The Distribution Management System (DMS), which previously was a SCADA operation, is more influenced by ICT. The DMS is responsible for managing error situations and corrections in the field, alerting customers, etc. It is still some uncertainty in figuring out what specific parts of the system that should be automated by ICT, but there is a large potential for optimization.
- Automation of simple tasks will be applied to customer service. A large volume of automated simple tasks can benefit the customer with a shorter processing time.
- The invoice system is going through a change. It will be a module-based system for each system segment compiled, integrated and operated by Hafslund Nett, instead of purchasing one large system from a supplier.

There is uncertainty to what the future brings, and Hafslunds investments will be affected by large trends in electric energy and local political decisions. For example, other renewable energy trends such as solar and wind power and batteries, but also the "electrification" of Oslo.

Observations

Similarities:
All three organization have invested in projects that are information oriented and uses ICT. The implementation of new technology has its benefits related to customer service and experience, effective work flow, system automation and optimization, and increased availability. There is an increased focus on gaining competence and experience, due to the new requirements created by the technology. This is accomplished by innovating and customizing solutions for their own operation, take advantage of a growing service market, and hiring new employees. There is a common trend to standardize procedures and centralize operations. This is due to the increased possibility of making data available and organized, as well as increase control.

Key topics and challenges:
As the technology changes, the organization must change too. It can easily become technology oriented and forget that the technology needs a well-functioning organization to manage it. Digitalization creates new requirements for management, expertise and mindset. The core function stays the same, but the process around it changes. The organizations must also adapt to manage the new challenges and exposure to vulnerability related to digital systems, as well as how to utilize the available data.

Dependency

Helse Vest IKT:
The hospitals have Helse Vest IKT as a service partner. The hospitals have a variety of digital solutions to increase work flow, effectivity, information security and privacy. Which means that the hospitals are dependent of these digital solutions while operating. The hospital is a high-risk organization and it is said that they are always dealing with emergency. This raises the question "what do they do if the digital systems fail?" Well, when the hospitals enter an emergency, there are manual procedures to manage failure in a digital system. The hospital cannot stop functioning, but it will be difficult to operate if one or more systems fail. The acute incidents are easier to comprehend than planned treatment, such as follow-up of cancer patients and treatments that require access to history, data or tests.

There was an incident in June 2016 were the DIPS system failed after a scheduled update. This was a serious event. During this incident, there was a casualty. It was later proven that the patient would have died even if the systems were working. This displays a possible vulnerability towards the dependency of digital systems. And that the work flow and quality of the hospitals can be seriously damaged if such an event occurs, and that the patient can suffer the consequences.

Bane Nor:
Bane Nor is very dependent on the digital systems. However, as a part of the vision, it will never be a single critical point in the system that has the potential to cause catastrophe. All components or units with potential for disaster or major accident, will have several connection points in the network or process chain. This creates a variety of redundancies in mobile networks, data centers, and core processes and

systems. For example, duplications of entire operation centers and core processes and equipment in a different geographical location.

Hafslund Nett:

Hafslund Nett is dependent on digital systems to run an optimal operation. However, in the short term, it is possible to maintain a basic power grid operation without any digital system. It is an important aspect to be able to sustain and provide the core product without the use of any digital system. This means that the ICT system can be shut down and manual processes perform the core functions. It is a part of being prepared for the consequences of a critical failure or a cyberattack. However, the efficient and cost-effective operation is highly dependent on digital systems. It can lower out maintenance costs and make it possible to operate with less staff.

Observations

Similarities:

The digital systems provide benefits such as an optimized operation and it greatly improve work processes. The organizations are aware of how dependent they are, and thus have invested in redundant systems and security. Emergency drills and planned manual procedures ensure that the organizations are prepared for any system failure or cyber related incident. The core operation can proceed with limited or without any digital systems.

Key topics and challenges:

The health sector is always in an emergency and are well prepared. The main function of the hospital is manual labor and the hospital can proceed with its operation without digital work aids or system. The other two organizations must have a different association with redundancy and emergency procedures. The core function is command and control based with the use of SCADA systems and could result in production stop if these systems fail. This makes redundancy important in ensuring that production can proceed by changing to a functioning system. Although, this may be an expensive solution. If it is possible to operate the core function with manual processes, then the organization is not as vulnerable to failure and it is prepared to manage a critical unwanted event.

5.4.2 Cyberattacks

Experiences

Helse Vest IKT:

Helse Vest IKT experiences that the cyberthreat is increasing and that there is always someone who is trying to break through, but they usually fail. 95% of all emails get thrown away and never read. These are email from suspicious correspondents. The client-platform is tough and has many levels of security systems in place, such as an application-blocker and firewalls. This software is available on all clients (users, computers, phones). It will only run preapproved programs, which means that any unknown program file from a virus will not be able to run. However, there has been two noteworthy attacks in recent years:

- Ransomware

There is an increase in ransomware. These are criminals who locks data and in exchange for money will unlock it. Helse Vest IKT experienced such an attack in one of the terminal servers, that later spread to Bergensklinikkene and Nordhordland emergency rooms, in December 2016. At that time the terminals was not uploaded with the application-whitelist-software. The crypto-locker virus was taken care off and failed in obtaining its objective. However, the affected services experienced loss of service and access to their journal database.

- Ddos-attack

There was a ddos-attack against Helse Bergen's webpage in November 2015. This caused the main webpage breakdown. The "sub" webpages were still operational, but was only accessible through direct links/bookmarks. Helse Vest IKT had to block foreign traffic to the website, which had consequences for communication with for example foreign research partners. The users experienced loss of availability to the system, which are many in a large heath organization such as Helse Vest.

These attacks had small and limited operational consequences for Helse Vest. But, the users of this terminal server experienced some loss of availability. Situations like this can trigger emergency situations, as in the event of the ransomware. These situations are unclarified and the damage potential is uncertain. In an emergency, the ICT-staff are informed and they do not stop working until the problem is solved. Users and customers are also updated. For a hospital or any other health service, emergencies are common. Procedures are made for dealing with situations like this. The largest consequence of such attacks is that the availability of the services decline and that the health services must operate without the digital aids.

Bane Nor:

Bane Nor has not had any successful cyberattacks on the operative production (Rail) network. There is a focus on monitoring the networks and paying attention to attempts to breach the firewall. But, there has been more failed login attempts from employees than targeted cyberattacks. However, there has been registered some incidents of outsider activity. No one has successfully entered the network and done unauthorized acts in the system. Some parts of the operative production network, in some contexts, have connections to the internet and is therefore exposed to cyber threats. Suppliers must also sometimes have access to the network. There have been some episodes of "whaling", where criminal actors pretend to be a director and asks for urgent payments. The methods used in email scams and vulnerabilities linked to employees can be used to create backdoors and encryptions in the system.

The operative ICT system had 39 incidents in 2016, compared to 51 in 2015. In the management's review, it concludes that few of the incidents caused a consequence, but several had the potential for an unwanted event cause serious consequence, for example downtime or partially unavailability in the system. The incidents are not cyberattacks, but events that has the potential to be exploited. The incidents are categorized as:

- Access and physical security
- Change regime and ITIL-processes
- Surveillance on system level
- Routines and quality deviations
- ICT vulnerabilities, for example missing patching

Patching occurs regularly, but rarely there is a need for immediate system update. It is impossible to chase every available patch from all suppliers. But, every new patch requires a criticality analysis. There are also different systems that are closed off from the internet and is not exposed to the same vulnerabilities as other networks.

Hafslund Nett:

Haflsund Nett has not experienced any targeted attacks, but experiences a high frequency of crypto-locker viruses and similar.

Observations

Similarities:

All three organization are experiencing an increased cyber threat, mostly non-targeted attacks, such as phishing. None of the organizations has experienced any attacks with major consequences for the organization or operation. The increased threat has led to an increase in resources and cyber security focus.

None of the organizations has experienced any targeted attacks. Targeted attacks are the main concerns of the security authorities. The non-targeted attacks are perceived as “noise” and does not represent a major threat to these organizations, mostly because of their preventive security measures and their ability to detect and respond to any attempt. Preventive security measures, such as firewall, email-filters and user awareness, will capture most threats. The detect and respond capability covers the threats that the preventive measures do not manage.

Increased Threat

Helse Vest IKT:

In 2009, there was an outbreak of a virus that infected almost all the systems in Helse Vest. The network had to be shut down to gain control. This was probably an eyeopener for many in the industry and has been used as an example of what can go wrong if one does not focus on cyber security. There are currently many resources dedicated to information security and privacy. Helse Vest IKT works with patient information and critical systems in hospitals, and must respect the information- and cyber security aspect of the operation. The health services and hospitals have their own ICT-personnel who focuses on information security, and data protection and privacy officers who focuses on patient rights. The three main principles of information security are maintained - integrity, availability and confidentiality. If there is a violation of privacy, it is reported to the Data Protection Authority (Datatilsynet). If violations cause consequences for a patient, it is reported to the health control and supervision authority (Helsetilsynet). If something needs to be clarified, it goes through the safety representative (verneombudet). Enrollment of new processes of data/personal data, it goes through the Data Protection Authority (Datatilsynet).

Bane Nor:

There is an increased focus on building competence in the organization. Consultants has been used in security previously, but Bane Nor has not benefited from this long term. It has lacked ownership in the energization and continuity. Bane Nor is acquiring new expertise in security, but ensures that the existing system environments can relate. Security-as-a-service is a growing business. This presents the opportunity to create relationships with security partners and share expertise, rather than managing all aspects in-house. These decisions are based on a risk assessment and a cost-benefit analysis. Bane Nor still needs assistance with penetration testing, training, and to some degree detection and response. However, it is important to maintain ownership and reasonability for the system security. Bane Nor has a partnership with NorCERT and is a part of the alert system for digital infrastructure (VDI).

Hafslund Nett:

No specific comment.

Observations

Similarities:

There is an increased focus towards employee awareness, ICT and cyber security related competence, and threat picture knowledge.

5.4.3 Leadership

Framework, Goals and Visions

Helse Vest IKT:

Helse Vest has a Regional Information Security Management System, which applies to the whole organization. This is the basis for information security and quality assurance. It is based on the Norm for Information Security in the health sector. The Norm is based on ISO 27005 and Norwegian law. Which it adapted for operating in Norway, thus it has more requirements and control points than the ISO-standard. Helse Vest IKT tries to standardize procedures and interfaces as much as possible. This will ensure that the overall health services provide the same level of availability, information security and privacy. Risk and vulnerability assessments are done regularly on a larger scale, but also done in relation to changes in systems and procedures, as required by the Norm. Lars Erik Baugstø-Hartvigsen states that the:

- Vision of Helse Vest: "*We will promote health and quality of life. Helse Vest shall provide robust user-friendly solutions that provide adequate security, and help to facilitate patient care and increase self-service and involvement.*"
- Vision of Helse Vest IKT: "*We will continuously improve the safety culture in Helse Vest. We shall help to support patient treatments.*"

This means that the ICT security and general procedures should be guided by the a "*it should be easy to do it right and difficult to do it wrong*" mentality. There are emergency exercises, desk-top drills and larger drills, for example TYR – a national anti-terrorism exercise.

Bane Nor:

Parts of Bane Nor's operation is ISO 27000 certified. This ISO includes a set of requirements and controls that ensures quality in the security activities, such as a management review. Additional security regulations have similar and other requirements. These are combined in to guidelines for the organization. These include:

- Security Management Guidelines
- Guidelines for contingency in security management.
- Guidelines for Information Security in Railway
- Requirements for information security management
- Instructions for safe use of the railway information systems
- And, an overall continuity plan.

These cover the requirements related to security regulations, the Security Act, object security, personnel security and security clearance.

Bane Nor's overall strategy includes building a robust system to manage cyber security. It is an objective to bring cyber security and the threat picture on the agenda. The Department of Digitalization and Technology is responsible for creating a cyber security strategy and a plan of action for managing the digital threats, this includes development of detection and response capacity. It is also an objective to establish a constantly updated overview of the threat picture, and communicate with relevant authorities. It is stated that the detection and response will contribute to the awareness of vulnerabilities and exposures in the system, increase the knowledge of threats, increase the expertise that contributes to reducing risk with preventive and reactive measures, and increase the quality of guidelines and procedures that can decrease incident management duration.

In practical term, this means to implement the already planned activities from 2016, and formalize and document procedures. For example, creating and approving the overall information security strategy and requirements for projects that will make changes to infrastructure. Every department have own goals that will support the overall strategy and long term goals for the organization.

Hafslund Nett:

Haslund Nett ensures that their suppliers are ISO 27000 certified, but is not certified themselves. They are governed by the Contingency Regulation (Beredskapsforskriften). This regulation covers information security and the SCADA network is subjected to these regulations. It is a very general regulation with unspecific requirements. For example, it requires that organizations protect sensitive data, but it does not explain what sensitive data is or encompasses. It is open for interpretation. It could focus on important functions that influence the quality of security, such as patching routines and other measures that have a documented effect against cyberattacks. The requirements could be more specific and updated to fit the current threat picture, as well as modern security technology. Perhaps a more updated focus in the regulations and more expertise in the effort to establish a revised version.

Short term goals and security activities include:

- Cleaning up the ICT-architecture.
- Implement system sensors and logging.
- Clarify patching and emergency processes.

- Perform penetration test on systems in an 18-month cycle with external actors, and perform follow-up activities related to the findings of the test.
- Standardization of the ICT-architecture and disposal of old outdated systems.
- Training and increasing the awareness-level of employees related to cyber security, especially phishing.
- Perform fake-phishing attempts to acquire statistics of how well the organization manages phishing attacks. This include time to detection, alert and response.

Overall goals include:

- System availability
- Cost-efficient operation
- Acquiring and changing the competence in the organization to fit future expectations and the increase of ICT in several parts of the operation.
- Customer experience

Observations

Similarities:

ISO 27000 forms the basis framework for information security and quality assurance for the organization and suppliers. Laws and regulations provides requirements for each industrial sector, emergency response, and is an adjustment to the Norwegian environment. There are organizational guidelines which are "summaries" or both ISO and regulations. These makes it easier to follow the requirements. Security is visible in the short-term objectives and is visible in that the organizations focus on improving the existing procedures, acquiring expertise and security technology, and distributing awareness to manage information and cyber security. Security is embedded in the long-term strategy as a premise for a successful strategy. Bane Nor has not previously had a system that could manage cyber security.

Key topics and challenges:

It is difficult to ensure information security and quality assurance of suppliers, contracts and outsourcing. This is a challenge that needs to be reviewed because of the growing market for security-as-a-service.

Vague explanations in the regulations. The term sensitive information in open for interpretation. It is difficult to know what is meant by the general unspecific requirements. Closer communication between legislators, regulatory authorities and organizations can enable realistic requirements for regulation, such as patching routines.

Visibility of Management Engagement

Helse Vest IKT:

The engagement from the leaders or top management is visible through board meetings and through larger information meetings with staff and employees. In addition, there is an obligatory e-learning course in information security with a requirement of having a completion rate of 90% of the employees and a retake every second or third years. There is an information campaign for the revised management system and new employees are informed of information security practices. The director of Helse Vest IKT and the ICT Security Manager has ongoing meetings and communication.

Bane Nor:

The management review is the main tool for engaging the management. It occurs once a year and is used to set the direction for the security activities. It is required by the "e-forvaltningsforskiften" (the regulation of e-management) to have a management system that is based on the ISO. There are also internal routines that require the management review. The recommended security plan for the next year is presented and reviewed. It includes future activities, for example, the revision of recertification of the ISO.

Hafslund Nett:

Hafslund's management did not hesitate to provide equity into kraftCERT without knowing if the partners, Statnett and Statkraft, would join. Security is a management concern and the shareholders are briefed on security topics. Hafslund perform management reviews. Security is a large part of digitalization and competence in the organization. Security is not a direct part of the overall strategy, but serves as a requirement for fulfilling the overall strategy and goals. The collaboration with NorCERT, kraftCERT, and other security partners supply Hafslund with relevant reports and information related to risk and risk picture. This information is distributed to relevant security personnel via email. There are three employees working with security fulltime.

Observations

Similarities:

The management is engaged in security. it is visible through meetings, management review, and the prioritizing of security activities and the resources spent on competence and security measures.

5.4.4 Risk Management

Risk Management

Helse Vest IKT:

In 2016, Helse Vest IKT conducted and documented 39 extensive risk and vulnerability analyses. About 30 employees analyzed and evaluated cases, scenarios and possible threats and consequences. The risk and vulnerability activities are characterized by:

- Documentation of risk and vulnerability activities in SharePoint (a Microsoft tool).
- Having meetings through skype, because of the geographical difference of the participants.
- Conducting risk and vulnerability analyses by the "Proximity principle" – the people who utilizes the process, technology, equipment, or similar, must be included in the risk activities. This means that clinicians and ICT-personnel are responsible for, respectively, functional risk and technical risk.
- Having a core of 5 people who works as facilitators for the meetings and ensures that the right language and methodology is used, as well as acting as interpreters between disciplines and creating the scope.

Smaller risk and vulnerability analyses must be conducted when making changes to a system that may have consequences for information security or handles personal data/patient information. The ICT-personnel at the hospitals conduct their own risk analyses, this does not concern Helse Vest IKT.

Bane Nor:

Bane Nor uses risk management as a part of the quality assurance process. Bane Nor's risk and vulnerably activities include:

- Risk and vulnerability analysis at system level and overall level
- Risk and vulnerability analysis with focus on security related to incidents, change procedures, and failure modes.
- Software tools to document risk assessments

The organization is mostly project-driven. This causes each project to run their own risk assessments and RAMS-requirements. As a part of the project end-delivery process, there is a transfer of identified risks and hazard logs. One of the procedures for information security, when detecting risk as very serious (highest level), is treated directly by the railway director (top management).

An evaluation of the need for system patching is done when new updates are available. The person responsible for the system and the change manager, or the person responsible for patch planning, makes and evaluation if it is critical to update the system instantly or if it is possible to do it in the scheduled update. It is always at least two persons in this evaluation. In larger changes, there are several people involved. The operative ICT security manager performs a control function where he communicates with the system supplier or the company responsible for the patch to find out if this patch must be updated right away or before scheduled patch regimes. How the update affects other systems is also included in the evaluation.

The benefit of performing risk assessments is the insight and attention to risk it provides in process. However, it is difficult to have an overview and a connection to all the disciplines and systems, such as transmission, fiber networks, transport and connectivity. This causes very few to perform a qualified assessment when the systems become complex. It may cause an oversimplification of lesser known subjects, and an exaggeration of well-known subjects. Full overview is near impossible to have, but a lot of this problem can be solved with training and repetition. It has been created analyses that has no use because of poorly composed composition of expertise within the team. The purpose of these analyses is to identify risks and find risk reducing measures. In most cases, the risk reducing measures did not cover the full risk picture. Bane Nor wants to be aware of what risk they want to balance with these measures. Not throw baseless-measures around.

Hafslund Nett:

Risk and vulnerability analyses are a part of Hafslund's operation. Previously, it was done out of compliance to the Contingency Regulation (Beredskapsforskriften), but now the analyses and the findings is utilized to a greater degree. It is a good systematic working methodology, but in the end, it is the sensors and patching processes that is the most important. The risk assessments are a great tool for providing a process that makes observations and the highlights does and don'ts. However, it does not provide any value unless the findings can be used. It must have a practical utility and impact. Hafslund

Nett has chosen to focus on penetration tests, rather than desktop risk analyses. All changes to the system is processed by the change- and release management. This system manages the changes done to a system and is supported by a risk analysis done by several staff members. The risk analysis becomes a part of a greater process - the change- and release management.

Observations

Similarities:
Risk assessments are an integrated part of the organizations' operation. Extensive overall risk assessments and smaller assessments related to systems, patching, change procedures, incidents, and failure modes. Risk assessments are separate in functional and technical aspects. Itil-processes, contingency regulations, and other regulations require an active risk management. All three organizations document the assessments using software tools.

Key topics and challenges:
There is a focus on utilizing the risk assessments to a greater degree. Sometimes the quality of the assessments suffers due to lack of knowledge or overview. The risk assessments are presented as a great tool for making observations and assess the different aspects of the system in a systematic way. However, the risk assessment does not provide any value by itself. The risk reducing measures and barriers must have a practical impact. However, it is a challenge to ensure insight and system overview to connect all the different sub-systems and disciplines and create reasonable risk reducing measures that encompasses the total risk picture.

Perception of risk and a common language

Helse Vest IKT:
There is a difference in professional expertise and this applies to language as well. To avoid any misunderstandings, is the scope usually divided into a functional risk (clinicians) and technical risk (ICT staff). The health services and especially the hospitals throughout Helse Vest may have divergent practices. This becomes visible when Helse Vest tries to standardize procedures and find common solutions.

Bane Nor:
Gurus and experts that are involved in everything are often created. The specialized risk or quality units/departments can decrease the overall perception and awareness of risk. It is more important to spread knowledge and expose people to the methods. It is important to associate with the risk processes and knowledge of procedures described in the quality system and use it. This can decrease the gap between the written processes and how it is performed. A large part of the core operation is based on risk assessments. Actions are not made without having considered risk.

There is a technological difference between conventional railway engineering and ICT which may cause a mismatch in professional language and technical understanding. The risk assessments done by the ICT discipline are based on organizing around standardized frameworks. Whereas, conventional railway engineering will focus on physical events and safety. It is a challenge combining the two "cultures" and draw the best from each discipline. However, there are different phases in the projects that take care of functional risk and information security risk separately.

Hafslund Nett:

There are great differences in risk perception. Hafslund Nett is heavy on the electrical power engineering-side, while the threat picture is aimed at ICT. Cyber security is an expertise not known to many, and Hafslund Nett keeps most of the security mechanisms secret. A common language does not exist in this sense. For many employees in the organization it may seem mystical and not a part of their every day job description. However, it is still important to train and educate the employees of the main threats, such as social manipulation, phishing, and general secure use of external media and sensitive information. If the user knowledge is high, then it is a large step in securing the entire organization. If an organization uses modern firewalls and intrusion detection systems, then it would be difficult to find a way in, except for via social manipulation and phishing.

Observations

Similarities:

There is a common focus on separating the risk assessments into functional risk and ICT technical risk.

Key topics and challenges:

The use of risk experts and specialized departments can decrease the overall employee and management understanding of risk. Organizations must try to distribute a common perception of risk across different departments and keep in mind the potential "professional language" barrier. There is a professional difference between traditional engineering and ICT. This may cause a misunderstandings and mismatches in language and understanding of risk. Cyber security is a specialized expertise and is not incorporated into traditional engineering disciplines.

Most risk is reduced or managed by using modern ICT security technology, except for social manipulation and phishing. This makes user behavior and awareness an important risk reducing measure.

5.4.5 Awareness and cooperation

Activities and collaboration

Helse Vest IKT:

It is important to build a front against attackers. It is a task done by collaborating with HelseCERT. The threat actors are organized and seek valuable information they can sell. Health information is worth about 20 times as much as financial information on the black market. This means that Helse Vest is an attractive target for malicious actors. A lot of the documents are publicly available, but there are certain issues that are secret, such as overall risk assessment of infrastructure. This information can be used to find vulnerabilities and commit criminal acts.

Knowledge and awareness is distributed through the organization by:

- Having an obligatory e-learning course for all employees
- Having a ICT security directive for all suppliers and third parties, as well as a requirement for being aware of Helse Vest IKT's security strategy and goals.
- Participating in NorSIS security month.
- Communicating with HelseCERT

Cooperation with the CERT-communities, sharing information with suppliers and customers. HelseCERT is cooperating with other CERTs. Most of the documentation, for example board meetings are publicly available. The things that are not available are information that can be used to commit crime or easily find weaknesses in the system, for example using the overall risk assessment of infrastructure. This is bound by Norwegian law.

Bane Nor:

There has been a change in awareness the last year. From being a subject not talked much about, to a daily matter. The awareness and collaboration activities are:

- Participation in "security month"
- The management team (including ICT director and FDV manager) are focused on cyber security. Cooperation regarding use, use patterns and awareness in cyber security and technology.
- Had an external driven project by a consulting firm on awareness. It did not live up to the expectations. The new information security strategy is to manage awareness and internal competence.
- E-learning courses and attitude programs regarding cyber security. Courses are brought from external corporations.
- Bane Nor is communicating with its suppliers about cyber security. It is visible in contract negotiation, request for quote (RFQ) processes, and in remote access situations. They have communication with NSM, NorCERT and PST.

Hafslund Nett:

Hafslund cooperates with KraftCERT and NorCERT. KraftCERT contributes with information and reports regarding the threat picture. Its other function is to share information, experience or incidents anonymously. This makes it easier to share information about incidences without thinking about reputation or other consequences. This contributes to the preparedness of the entire sector. The

KraftCERT members are competitors in business, but are partners in security. Recently, there has been an increased flow of organization willing to join the different CERT communities. It is incomprehensive why some organizations choose to not be a part of this initiative.

Observations

Similarities:
The three organizations have similar awareness activities and collaborates through the same channels. They are members of NSMs alert system for digital infrastructure (VDI). There is a focus on awareness on an employee-level, as well as a management level. There is communication between employees, ICT security managers, and CEOs. The CERTs role is important and the different CERTs contributes to raising the awareness across industrial sectors.

Key topics and challenges:
The CERT's function is valuable for the organizations. The CERTs are contributing to information- and experience sharing and an updated threat picture. The organizations rely on the CERTs for information and they will probably be dependent on the collaboration in the future.

5.4.6 Threat picture and exposure

Exposure

Helse Vest IKT:
Helse Vest acknowledges that the threat picture has changed over the last 4,5 years. It is becoming easier to be a cybercriminal and there are a lot of smaller actors than before. It is possible to buy "hacking" as a service and the black market for cybercrime is escalating, it has been commercialized. At the same time, targeted attacks have become more frequent, as seen with smarter frauds and scams, for example whaling. The Norwegian language was previously a kind of "encryption" that made it easy to identify frauds. Translation software makes email-frauds more believable.

The value chain can affect the system's vulnerabilities. Customers/end users have limited access. This means that each user has been given enough access to do his or her tasks. The application blocking and device identification ensures that open networks, available network ports (for example in an office) are available for approved devices and software. This means that patients, health personnel and visitors can only use approved programs. Suppliers have agreements that ensures access control, limited timeframe, confidentiality and awareness of the security procedures. They are also monitored when accessing Helse Vest IKT's systems, via the supplier VPN. Helse Vest IKT does not use outsourcing, due to internal cost-effectiveness and to maintain in control over infrastructure. The use of cloud-based services is justified by strict supplier contracts and a substantial risk assessment of data-processing contracts with third parties. Standardized platform ensures the same overall security level across the board.

Helse Vest IKT pays attention to the evolving threat picture by:

- Having staff working with security technology on networks and clients.

- Using Nessus as the main supplier of security technology in the server network, which updates and sends new signatures from known threats regularly.
- Patching the Operative system frequently as supplier (Microsoft) advices.
- Updating other software regularly.
- Having weekly safety and security scans on servers. Occasionally a larger scale and more extensive scan.
- Having frequent communication with HelseCERT.
- Attending yearly security forums and professional conferences

Bane Nor:
Bane Nor manages threat picture by:

- Recruiting people with relevant experience in security
- Communicating with NSM and other authorities
- Participating in international conferences related to cyber security
- Establishing contact with other railway infrastructure owners in Europe, for example Network Rail in England, Deutsche Bahn in Germany, and Denmark.
- Having the Department Manager participating in international organs

The administrative ICT operation is outsourced to Sopra Steria. Other parts of the organization are mostly operated in-house. The future trend is to buy services based on a competition model (quote/tender). The reason for this is to develop the market and prioritize the operation of the core business. Information security and cyber security are an issue in these processes. For example, ensuring quality and performance of the outsourced services. Services associated with construction development are brought. For example, physical activities such as adding fiber cable along the railroad tracks. Configuration of networks and activities associated with the core operation are always managed in-house. Mostly because of security reasons, but also because of the organization's tradition.

The operative competence in Bane Nor is high, but it lacks specialization in cyber security. Other services are brought from companies that specializes in the given area, because it is not always purposeful to have all aspects of expertise within the organization. The knowledge and competence around operating the technical system are in place. Building system understanding is difficult and takes time, because the process chains (or value chains) become long and complex. The different disciplines are coupled in a different way. It is important to develop a system overview, knowledge and see weaknesses and different scenarios clearly. This is a challenge in the future operation.

Hafslund Nett:
The main source of updated information about the threat picture is KraftCERT, NSM, and other security partners, such as Mnemonic.

Hafslund Nett has not experienced any targeted cyberattacks, nor in the sector. However, PST and NSM clearly states that critical infrastructures, such as power and telecom, are exposed. As well as, a high probability that a targeted attack will occur in Norway. It is something Hafslund Nett must consider and adjust to. There is an increase of non-targeted cyberattacks, such as phishing, micro-Trojans, and crypto-locker viruses. The email filter captures almost everything, but some attacks can get past the filters. The sensors detect these threats and countermeasures can be initiated. These attacks can create hassle, but should not be a problem for a professional ICT organization. They are a larger threat towards private individuals, where private documents and pictures can be lost. Also, smaller organizations that do not possess proper back-up/ recovery systems and other security measures, or lacks ICT expertise, can lose vital information.

Security technology contributes to reducing the exposure and consequences of the cyber threats. Application blocker only allows approved processes or programs to run. A role-based access control gives no user excess rights or access. The threat actors will always be a step ahead of the security companies, in that they can launch an exploit that penetrates the system. Similar systems around the world must then be updated. This creates a time-gap between detection and patching. Separation and disconnection of the infected area is a common procedure. This requires that manual processes are in control if the threat is being managed and the system is updated. Detection and response will be the most important tool in the future, based on how the situation is today. It is the mechanism that makes Hafslund Nett capable of managing all attempts at compromising the operation. In most cases, the sensors detects and reacts before the user knows about the threat.

Hafslund Nett’s operation can operate manually without any digital systems. This allows for a complete shut-down of the any digital systems if necessary. It is a mechanism that ensures core operation even if critical failure or a cyberattack has occurred. With this in mind, the value chain can impact the exposure for risk and vulnerabilities. It in an increased risk related to AMS. They are small computers installed in all customer locations and has the potential for remote control. This presents the risk of remote control by unauthorized actors. The systems are becoming more complex, and the risk increases along with it. Parallel to the digitalization of parts of the operation, there has been a focus on security, especially the use of sensors. This allows Hafslund Nett to get ahead of the risk.

Large organizations with resources and technology does not face an imminent problem with an overview of complex systems. This is more visible in smaller companies with 10 000-20 000 customers. The digitalization and security aspect requires special expertise, which can be difficult to justify compared to other expertise requirements in the organization. They do not possess the same organizational machine to manage these threats. However, the CERTs may contribute in a positive way.

Suppliers are governed by contractual requirements, which include access control, simple background check (nationality, etc.) and an overall approval. These formal requirements make it possible to monitor and control the supplier. There are many suppliers involved in the operation, but Hafslund Nett governs the activities. Hafslund Nett has a hybrid approach to outsourcing, where the reasonability, ownership, and control lies with Hafslund Nett.

Observations

Similarities:
The organizations have experienced a changing threat picture the last three years. There has also been a change in organizational focus towards cyber security. Competence and knowledge has become a part of the strategy in the organizations. There has been an increase in collaborations with CERTs, security partners and authorities. These organizations provide valuable information concerning the threat picture.

There is an awareness towards vulnerabilities in the value chain and an emphasis on managing supplier and system user rights. There are performed substantial risk assessment of data-processing contracts with third parties.

Key topics and challenges:
The commercializing of security, for example detection and response function. This should be done with a substantial and systematic risk and vulnerability assessment before engaging the market. The ownership and responsibility should always be in the organization. This means acquiring satisfactory expertise and system understanding to be able to manage the outsourced or purchased service. Exposure to unforeseen events related to outsourcing ICT, include too little knowledge about real system access, admin rights, and the ability to change /affect the system. Organizations holds the technical knowledge, but may find it difficult to have system overview and understanding because of the long and complex process/value chains. The time between an exploit is detected to the patch is released and installed is experienced as critical and vulnerable.

Insiders, sabotage and espionage

Helse Vest IKT:
Insiders are a part of the risk and vulnerability analyses. What will it take for the person to be able to do harm? The technical barriers are in place to minimize consequences, such as application blocking, surveillance and logs. There are 1015 different systems, 38 159 users and 32 846 computers. This is a lot of users to comprehend therefore it is best to limit everyone's access. It is important to note that no computers have extended rights. Helse Vest operate from a firewall principle of restricting everything and only open access to what needs to be accessed. There are a lot of persons connected to for example a hospital. Patients may have bad internet habits, even criminal habits, and this must be considered in the assessment. In such cases, the police are involved in handling the case. Suppliers must go through a dedicated VPN and have access in a predetermined duration. The reason for the work, for example replacement of equipment or a construction work, and the number of individuals and what they are performing must be documented.

The larger cases of sabotage and espionage are difficult to think about. There is a habit of not look at these events as probable in the public sector. However, after Lysneutvalget and a new public focus in preparing for large critical events, it is seen more in the risk assessments. For example, malicious acts from larger actors such as nations. These events can be a bomb in proximity of data centers. That is one of the reasons Helse Vest IKT has several data centers and triple redundant communication lines, physical barriers, alarms and surveillance. The hospitals must be able to continue their operation in an event of complete system failure. There are manual backup solutions for all digital systems. Emergency procedures are store locally on laptops and are available in the event of a power outage. Overview of hospitalized patients are stored in a redundant common encrypted server.

Bane Nor:
Bane Nor' acknowledges that the threat picture has changed, as well as the understanding of the threat picture. Ransomware did not exist three years ago and it was not talked about. It is important to note that Bane Nor is not attractive to cybercriminals in the same way such as banks or other financial

organizations. Bane Nor is primarily a target for nations and planned, resourceful attacks. Large actors can penetrate the system to identify weaknesses and plan a future attack, either directly or indirectly connected to the railway infrastructure. It is not unlikely that the transport sector could be means to inflict more damage in an attack against the public or the government of Norway. For example, in an attack against Oslo, where a non-functioning transport system can cause difficulty in evacuating large amounts of people. There are many scenarios like this, where the railway infrastructure can be utilized as a tool indirectly or directly.

Motivated insiders have the potential to cause harm or be pressured to cause harm. Employees can consciously, or under pressure, cause an unwanted event. Bane Nor discusses if employees are considered a threat actor or a risk. Employees are a resource and an asset, but to list them as a threat may be wrong. It may be a risk associated with if employees are or can become a threat. Sabotage is most likely to occur on local facilities near the rail. These "cabins" are secured with alarm systems. Any attack here will have local consequences, and would not affect the overall operation because of redundancies in the network coverage.

Hafslund Nett:

The same focus applies to insiders, sabotage and espionage, as for the management of users and suppliers. The role-based access control ensures that everyone has limited access and system rights. These are revised regularly and will ensure that users with access still need access. There are less than 10 employees with access to the functions of the AMS. The sensors and system logs monitors the internal users, as well as the external users. There are physical barriers and redundancies in data centers and vital infrastructures. These facilities have "hot-standbys" that are full duplicates of vital infrastructures. This does not apply for the administrative network. The SCADA network is operated from an undisclosed location. The different malware attempts may be about espionage and gathering information of networks structures and functions. However, it is difficult to know and it is best managed by the intelligence services.

Observations

Similarities:

A common trait is that the organizations have done an assessment of these issues. They have similar security measures, redundancies and physical barriers. Many of the measures that are applied in managing the system and reducing failures, also works against insiders, sabotage, and espionage. The mechanisms that manages system users and suppliers, applies to insiders and espionage. The redundancies can manage critical incidents of physical sabotage, cyberattacks or natural disasters. Local sabotage is not a major concern and will not create major consequences, due to the redundancies. The concept of employees being a resource and an asset, not a threat, is a good distinction. There is risk associated with the potential employees have of becoming a threat, due to external pressure or internal motivation. To list them as a threat can damage the internal workings of an organization. The other aspects of insider threat: suppliers, customers, or anyone with potential access to the system, are managed by the same security measures that manages general system users, by role-based access control and application blocker.

The organizations are aware of the risk of being used as a part of a larger attack, or that their function can be used directly or indirectly used to cause additional consequences. It is difficult to know everything about the threat picture, especially related to critical attacks from nations and counter intelligence. The organizations do not have the same information as the intelligence authorities and must rely on their guidelines and recommendations.

Differences:
Helse Vest IKT and the health sector is in an extraordinary situation, where emergency is a daily issue. This means that the operators (clinicians, nurses, etc.) are well-trained in emergency. The core function will still be performed while the ICT staff manages any system failure or cyberattack. This means that the framework for emergency routines, both in health care and in ICT, are practiced and has a high priority in the daily operation. The organizations have a different value assessments. The different values attract different malicious actors. Yet, the security measures and procedures are similar.

Key issues and challenges:
It is difficult to relate to the unlikely scenarios such as large scale cyberattacks, or similar. It is difficult to acquire information related to actual likelihood of these events and the organizations must manage a high level of uncertainty. The organizations must think of "paranoid" or extreme potential events and how to respond to them. This touches upon topic of managing black swans. The "foolproof" mechanisms that reduces many consequences, such as the high level of redundancies, is an expensive way or ensuring availability. The level of redundancies found in these organizations can be difficult to afford for a smaller organization. However, the daily operation is built in a way that the measures that manages smaller events and failures, can manage larger events. The most effective and important function is the ability to detect and respond to any system irregularities related to cyberattacks or system failure.

5.4.7 Preparedness and emergency response

Emergency response

Helse Vest IKT:
Helse Vest IKT has clear responsibilities, continuity processes, emergency processes, and recovery (backup). The hospitals have manual backup solutions and emergency procedures if the digital system shuts down. It is performed emergency drills and run-throughs. There is also a different system where the emergency response organization is managed. This is a robust and redundant system outside of the normal operation. This is to ensure that the emergency response can operate while the other systems are down. The alert routines are planned and tested. There are different systems that can notify employees and users. Documentation of risk and vulnerability assessments are available through software tools. Emergency response communication paths are prepared in advanced and rehearsed. There are staff- and daily meetings, by telephone or otherwise. Automatic SMS and telephone for the persons with a leadership role in an emergency. End users must be advised in such cases, and there will be an information flow from the incident (system failure due to cyberattack or other events). The most important aspect is to allow the recovery team to work and identify and solve the problem.

The main source of information is the intranet; it reaches all the organizations within Helse Vest. Users are aware of the level of emergency by looking at the color of the intranet interface – green, yellow or red. If the organization is in a state of emergency, it is important that the users are aware, and that it is not performed any changes to the numerous systems operated by Helse Vest IKT. It is generally one or more systems with a scheduled change of the total 1200 systems each week.

Increase the number of risk and vulnerability analyses by 20% each year. At least 90% of all employees must have completed the e-learning course in information security. It has become easier to flag/report security issues and the alert/notification culture has increased from previous years. Debriefs are performed after a comprehensive incident. These meetings perform a root cause analysis and are a part of the problem management in the ITIL process. These activities contribute to avoiding future events by highlighting the issues that led to the incident (cyberattack or system failure). Some of these activities led to the implementation of the application blocker on the health care terminals. There are also change-processes that analyses the impact the change has on other systems.

Bane Nor:

There are other emergency response organizations active in the event of non-information security related incidents, such as power outage at a station, or a landslide. The contingency plan for information security for Bane Nor was recently completed. Bane Nor has alert exercises to confirm that all communication channels are available and that the responsible individuals know how to respond and react. The plan for drills in 2017 has been set in the management review. The drills include cyber-related incidents, loss of infrastructure and loss of a service. They are mostly "table top" exercises. Bane Nor participates in cross-agency exercises, such as "IKT 16". It exposed some weaknesses and a missing coherence between governing documents and the actual operative routines and procedures. Which caused the management to not fully understand the capacity of the emergency response organization.

The quality requirements of ISO 27000 are the main quality assurance in security activities. The standard has become clearer on the requirements. There are many written documents, processes and procedures, but the challenge is to develop usable and practicable KPIs. There is a need for setting requirements for quality in the security activities, especially when Bane Nor is looking for tenders and negotiating the detect and response function. A measure of maturity is the ability to learn from previous incidents and improve weaknesses. This include the ability to use the root cause analysis to learn and produce better countermeasures. Bane Nor has hired a person to correct and follow-up measures after a major incident in September 2016. His job includes making sure the incident does not occur again, by implementing and follow the performance of 18-19 measures.

Hafslund Nett:

There is a focus on emergency preparedness and response in Hafslund. Hafslund performs exercises and have predefined roles and clear routines for how to act in an emergency or incident situation. The core product is a 24/7 operation with a 24/7 operation center. There is a lot of manpower because of the large customer area, which makes it easier to manage a situation because there are always operators at work who can manage the initial phase of an emergency. All the events are documented and the post-event debrief forms the basis for future exercise and learning. At 100% emergency response, will alerts reach the CEO, security partners and authorities. These include the emergency response unit in NSM and NVE. KraftCERT and NorCERT can be assisting in the response.

The exercise, security meetings and post-incident analyses is the main quality assurance. The exercises are performed with other actors, such as Nkom and Statnett, as well as industry exercises. External advisors are also used. There are requirements or key performance indicators related to time used before detection, reaction, and to when a deciding and communicating emergency organization is operating.

Observations

Similarities:

The three organizations have 24/7 operations and perform a critical function in society. The first common trait is that they are well prepared for an emergency response. There are planned, prepared and rehearsed procedures and communication channels. There are different escalation procedures for different level of severity. They all have 24/7 operation centers which manages the initial response. From there, the emergency response organization and other authorities can be informed. The second common trait is the high level of redundancy in critical system functions, such as data centers and core functions. The distribution of incident information occurs via available means, such as phone, email and intranet, to relevant staff and to general stakeholders. The third common trait is the use of sensors. This is the main mechanism to detect any incident or unwanted event. The sensors usually detect an incident before any system user. The fourth common trait is the focus on post-incident activities, such as root cause analysis. The ability to learn from the incident is visible through the usable measures produced by the post-incident activities. Even though this does not reveal the quality of the post-incident activities, nor the actual emergency response, it shows that the organizations focus on the benefits of these activities.

Key issues and challenges:

The emergency plan and framework is the main quality assurance mechanism. Emergency drills, security meetings, and post-incident assessments are all a part of the emergency plan. The organizations also utilize penetration tests, external advisors, and the cross-industry emergency drills as a way of measuring performance. The main indicators related to incident response are detection time, and the time it takes to establish an operational emergency organization. There is not a wide variety of performance indicators related to emergency preparedness or general security activities. This is an area where there is room for improvement, especially related to specification of what functions needs to be monitored, in what way is it monitored, and how to establish an evaluation of performance that is comparable to other organizations. The researcher's opinion is that it is difficult to ensure quality and performance in security activities without testing the mechanisms as close to the real situation as possible. This will approach the problem in a more practical way.

5.4.8 Tradeoffs between innovation and security

Balancing Innovation and Security

Helse Vest IKT:

Some security measures, such as the supplier-VPN is perceived as slow and unnecessary from the supplier's point of view. It interrupts the work flow and may be less convenient, but it is important for security reasons and reduces the exposure. On the other hand, it does not dramatically change the quality of the work or the time to completion. A key issue in the health service industry is the tradeoff between availability, privacy and patient security. If a doctor has very good knowledge of a patient health, the doctor can give the patient the best treatment available. On the other hand, if the doctor did not need all the excessive information, and sensitive information was accessible, then personal information has been leaked. These are issues that are supervised by Helsetilsynet (Health inspectorate) and Datatilsynet (Data Protection Authority).

Bane Nor:

Bane Nor states that it would be wrong not to pursuit the possibilities in technology because of the challenges and possible negative consequences. For example, being afraid of using fire because you may get burned. The process of acquiring knowledge and insight creates the ability to manage the responsibility of safe and secure innovation. Mechanisms and barriers can prevent the negative consequences from overshadowing the potential of new technology. All changes related to digitalization face opposing forces that say it is a threat to jobs. Without change, there is no progress.

Hafslund Nett:

Hafslund Nett believes that it is not a security measure to avoid using the cloud or disconnecting internet access. It is important to utilize new technology. Modern ICT carries less risk than old ICT, mostly because of modern solutions and the ability to patch. There are effective security measures in using sensors and modernizing the ICT architecture. More time should be spent revising solutions and to consider what is being used and what is not being used. There are domains where security is always the highest priority, but there are domains where security is not the main issue. It is important to allow for testing of new solutions in order to progress, innovate and develop. These tests should be performed in a "sand box" (such as Lean Startup) where security is not an issue.

Observations

Key topics and challenges:

The organizations show the willingness to innovate and utilize new technology, but are also aware of the potential drawbacks, such as exposure and security issues, replacement of job functions, and a focus on information and privacy management. Information availability and security are sometimes contradictory. This can cause pressure from different parties that have different attitudes towards security. Compliance to strict procedures and a prominent security culture can avoid any quick decisions that may compromise security. Automation can replace old job functions that were previously done by humans. This creates a need for motivating and retraining employees through education and courses. The role of the employees becomes less hands-on and more supervision and control. The utilization of new digital technology creates new vulnerabilities. But, the focus should be on maximizing the benefits from new technology, while still ensuring safety and security. This may be accomplished by building expertise and have a constant practical association to risk.

5.4.9 The Future of Digitalization

New Technology and Challenges

Helse Vest IKT:

In health care, welfare technology is the next trend in the technological evolution. The main goal is to transfer the treatment closer to the patient. The technology can transfer information from the device and send it to a for example hospital for dosage or equipment parameter adjustment. This decentralized way of doing health care is an information security challenge. The second trend is to coordinate information and make it more available. It is mainly a political target, and it is far from realization. There are many journal-systems in all the hospitals and health care services. The merging of these systems requires information tracking, authentication procedures and an awareness of information security. The biggest challenges of the future will be authentication and making sure that the information is treated securely and with privacy in mind.

Bane Nor:

There is nothing better suited for being driverless than trains. It has the potential for increased safety, security and is less affected by human factors. Condition-based monitoring (CBM) has a large potential for cost-efficiency. Bane Nor has a high cost in maintenance, and CBM can liberate those resources. Automation and visual simplification of alarm systems in operation centers can reduce the impact of human factors. The biggest challenge of digitalization is to consider it as an organizational change, rather than a technological change. How to develop employees and convince the organization to come along on this journey without seeing it as a threat. How to motivate employees and staff to see things differently and change mindset, and applaud development. The technology is very simple. It is not difficult to create a server with 100% availability, but having people with system understanding, technological and organizational knowledge is demanding.

Hafslund Nett:

There are new opportunities in automation and artificial intelligence. These utilize the available data to decide and initiate automated measures. The future of the threat picture is uncertain and is affected by many different factors. However, general threats are relatively easy to defend against, if the organization have resources and ownership to the security activities. The main challenge lies with targeted attacks. It is affected by many factors, such as the political situation in Norway, exposure, and importance or criticality of the organization. When the first industrial targeted attack occurs, it will gain a lot of attention. However, the operation of Hafslund Nett and its security measures would not change dramatically.

Observations

Similarities:

The three organizations draw attention to important challenges; organizational change, future uncertain threat picture, and the authentication of users. These are challenges that include preparedness and planning.

Transparency, Information Sharing and Communication about Cyber Security

Helse Vest IKT:

It is beneficial for others to know what someone has done to counter a threat. In that case, it is smart to share with the "good guys". On the other hand, one must be vary of what information is shared and to whom. It is important not to share critical vulnerabilities. The threat actors can adjust their methods to fit the shared security strategy/measure. Sharing is caring, as long as it is reasonable. Some information needs to be secret out of security concern. The CERTs share information between themselves and is a valuable information resource.

Bane Nor:

Communication is the solution. Efforts made behind closed doors, for a limited number of people, will decrease the synergy effect. Without communication organizations stand to miss what others have done and thought. Contributing and receiving good ideas can contribute to increase the preparedness of organizations and sectors. There will be a potential for benchmarking and awareness of own shortcomings and weaknesses. At the same time, some subjects must be kept secret due to security concerns, such as sharing network topology and IP-addresses. However, sharing and discussing cyber security strategies and how to prepare for incidents is positive. Discussions in international conferences are valuable and can be translated to Norwegian conditions. This can increase the insight of exposure, vulnerabilities and create a grown-up perception of risks.

Hafslund Nett:

An open discussion is exclusively positive. It is all about awareness, initiating processes, prioritizing, learning, understanding, helping, and sharing. The threat actors are always ahead and sometimes the security activities include putting out a fire. A lot of proactive initiatives will keep most things from burning, but eventually there will be a fire and the firefighters must intervene. Sharing and transparency will help the "firefighters" prepare for the situation and future incidents. The CERTs communicates with other international CERTs and security organizations. Hafslund is not directly involved in these communication channels. The most important communication occurs between the CERTS, security partners and Hafslund. This is where updated information about the threat picture is shared. The international conferences on security in the energy industry works as professional input, opportunities to build professional relationships and networking for employees. The most valuable information is when an exploit is detected and a new patch or ways to defuse the threat is distributed, either through security partners or KraftCERT.

The different authorities do not appear to coherent. For example, NSM, PST, NVE, and different part of the legal system. It is affected by a lot of politics and is characterized as very boreoarctic. The regulations could benefit from professional opinions and input. There may be a gap between the real vulnerabilities and the vulnerabilities that the regulation-makers believe as important. An involvement of the industry can set a realistic direction for improving security and supervision. However, there has been a visible change in NVE's engagement in the industry. They are participating in industry conferences, are actively communicating with organizations, and appear more collegial than before.

Observations

Similarities:

There is a common consensus that information and experience sharing related to exposure and cyber security is utterly positive and that it is an important mechanism in being prepared. All the organizations are dependent on an updated threat picture from the CERTs and updated patches from the security technology companies. These are valuable communication channels that transport time-sensitive information. The different industrial CERTs can communicate threats that are abound in an industrial sector to others. This increases other organization's ability to prepare for a similar threat. The less time-sensitive knowledge can be acquired at international conferences. These conferences present opportunities to discuss issues at a professional level and may provide insight to more overall organizational and technical aspects of operation and security. There will be aspects of an organization's operation or architecture that needs to remain secret. However, there are many similarities in the use of technology, organizational structure, and ICT infrastructure across organizations and industrial sectors. This means that organizations can learn from sharing security strategies and discuss challenges related to digitalization and vulnerabilities in digital systems. The CERTs distributes information anonymously; this makes it easier to share and there is less consequences for the organization that shares the information. Smaller organizations with less opportunities for researching and develop security solutions and strategies can gain knowledge from larger, more resourceful organizations. As well as, contribute to expand and grow the security community by sharing incidences and experiences related to security.

Key topics and challenges:

The authorities face the same problems as the organizations. How to gain expertise? What are the right parameters, functions and measures to regulate? How to communicate and collaborate with the industry and set a realistic direction for future requirements in information and cyber security? These are questions that are best solved with communication and an open discussion between the industry and the supervisory authority.

5.5 Part 1 - Results

5.5.1 Industry Solutions and Security Measures

Human Security Measures

All three organizations are trying to solve the awareness issue, and has identified it as an important challenge. They solve it by conducting e-learning courses, employee training, awareness campaigns, cyber security emergency response exercises, and hire new workers with new knowledge and expertise. The main goal of awareness is to raise user knowledge and threat awareness (for example phishing and secure use of external media) and to change the mindset of the organization to focus on cyber risk and cyber security. The combined human part of the cyber security is summarized in table 5.5.1.

Table 5.5.1 - Combined Human Security Measures

Preventive Measures	Consequence Reducing Measures
E-learning courses	ICT Security Personnel
Threat Awareness Campaigns	
Deviation Reporting Culture	

The e-learning courses and the threat awareness campaigns provide a general employee ICT and cyber security understanding. The important aspect of employee ICT behavior and knowledge is that they know how to behave in an emergency/unwanted event, how to manage ICT devices (such as computers, phones, etc.), and be aware of what information they share in social media. The deviation reporting culture is an indicator of employee situational awareness. It may not always result in the detection of an intruder, but it is a measurement of how well the security culture is established in the organization.

Technological Security Measures

Data-driven technologies and digital infrastructures can be exploited through organizational, technological and human factors. Social manipulation and phishing are issues that involves human factors, which means that there will be a successful phishing attempt one time or another. Zero-day exploits create a need for detect and response mechanisms. A set of basic technological security measures can prevent most cyber threats. The combined technological part of the cyber security is summarized in table 5.5.2.

Table 5.5.2 - Combined Technological Security Measures

Preventive Measures	Consequence Reducing Measures
Intrusion Detection Systems	Incident Response
System Traffic Logs	System Recovery/Backup
Modern Security Technology (firewalls, email filter, etc.)	System Redundancy
Role-Based Access Control	Manual Procedures
Application Blocker/Whitelist	

Upgrading Old ICT/ICS Equipment & Infrastructure	
Separate Networks and Domains	
Remote deletion of lost or stolen devices	

Redundancies in critical functions related to the core operation, often real-time duplications at a secure undisclosed location with physical barriers. The detect and response function is important. The organizations states that this function makes it possible for them to intercept all the threats and reduce the consequences. It is a mechanism that becomes more important in the future because real threats are often surprising and very sophisticated. System recovery functions and redundancies are great assurances, but is not appropriate for all organizations.

Organizational Security Measures

Cyber Security is driven by the management engagement and the competence within the organization. The organizations' management understands the importance of cyber security. Therefore, there are resources dedicated to cyber security and it becomes a part of the overall strategy and objectives. The combined organizational part of the cyber security is summarized in table 5.5.3.

Table 5.5.3 - Combined Organizational Security Measures

Preventive Measures	Consequence Reducing Measures
Collaboration with CERTs, Security Technology Partners, and Authorities	
Risk Management	
Incident/Emergency Response Drills	
Documentation & Formalization of Procedures	
Prominent Leadership Engagement & Overall Security Culture	
Third Party/Supply Chain Management	
Cyber Security in overall strategy: Gain Cyber Security Competence & Threat Picture Knowledge	

Interesting Industry solutions

There are some interesting observations. For example, Hafslund Nett performs fake phishing attempts on its employees. These attempts are anonymous and creates a data basis for evaluating the employee competence and awareness. Hafslund Nett and Bane Nor has "extreme" redundancies in certain parts of their organization. These are related to critical function, such as operations centers, and are expensive solutions. Hafslund Nett has a sandbox environment for innovating and gaining experience with new technology solutions. This environment allows innovating while not affecting the security of the operation. The three organizations agree that communication and information- and experience-sharing is the way to face the cyber threats. Helse Vest IKT is collaborating with PST and Scotland Yard to hinder threat actors. ITIL processes are widely used. Helse Vest IKT and Hafslund Nett has dedicated personnel working with security technology.

5.5.2 Key Issues and Challenges

There are some key issues and challenges that needs to be addressed based on the interviews and the literature study. These include how supply chains affect risk, how technology changes the organization, and how the legislations are ambiguous.

- *Innovation vs Security*

Hafslund Nett's use of secure domains to innovate, learn and get experience with new technology is a great example of combining innovation and security. The "sandbox" approach makes sure that the organization can innovate in a domain that does not affect the main operation. This allows for testing solutions before they are implemented and the innovation increases the experience and knowledge of the "innovators". Helse Vest IKT and Hafslund are less interested in buying a full-service "box" from a service provider, more interested in using generic ICT technology to create specialized solutions and innovate in-house. Since one of the challenges of digitalization is data management and finding uses for new technology, as well as security, it is a good way to test the technologies and functions in a secure environment in order to build experience, competence and system understanding.

- *Assurance and Control of Service Providers*

Several businesses can be involved in an organization's operation. This can be for example, partial or complete outsourcing of ICT operations or the use of technical support. These fragmented supply chains require clear communication, visibility and quality assurance. It can be difficult to audit, control, and communicate with service providers based on their location, culture, language, but also their use of sub-suppliers. There are legal and regulatory issues associated with location of service provider and sub-suppliers, when dealing with international businesses. Especially for when sensitive information is managed or accessed by foreign service providers or suppliers. Governance is a key factor in quality assurance, this means that the customer must have an active role in ensuring that contractual requirements for information and cyber security, operation, etc. are met in a satisfactory way. Additionally, the organization should remain in control of and have ownership of the service or operation that is performed. Customer and suppliers may have different standards and procedures for information and cyber security. Implying that there can be dissimilar procedures for employee background checks, salary, work environment, and general security culture. This will affect the overall vulnerability of the operation. Further, an involvement of international suppliers and their sub-suppliers may increase the risk of exposure to risk because of the additional links in the chain, given that the suppliers manages or has access to valuable sensitive information. Access control and authentication will be challenged. The governance can be less effective as the supply chains become longer, such as when additional sub-suppliers are acquired to manage the work load. Inspections and audits can become costly and time-consuming because of the increase in sub-suppliers and geographical/cultural difference.

- *Financial Flexibility*

The future involves large data streams from production systems and similar. This requires sophisticated analysis and data management tools. The use of service providers, suppliers, and outsourcing of ICT security or data management (for example cloud services) can be a cost-efficient decision, but it carries risk. The first aspect is that it can significantly reduce operation costs and add otherwise unattainable expertise to the organization. As the market is stimulated, the services can become better as the competition increases. The second aspect is that these suppliers are susceptible to market conditions that can lead to the loss of service or bankruptcy. The organization can lose ownership or lose of the data, or the data leaks to unknown sources. The third aspect is that large ICT service providers is a target for threat agents. Based on that these organization contain information from many different organizations.

- *Technology-oriented Organizations*

It is easy to focus on the technological change of the digitalization. New technology presents new opportunities in business, operation and maintenance. However, the future of the organization impacts the infrastructure of the organization and has requirements for new expertise, work methods. This means that there are several aspects of the organization that needs to change or adapt to the new conditions. However, it is important to make sure that the technology serves the overall organizational goal and does not undermine the existing values of the organization. To achieve the visions and objectives of the organization, there needs to be a foundation in information and cyber security. New technology creates new requirements for availability, confidentiality, integrity, and reliability. From a security perspective, it is important to acknowledge that the threats evolve, which create a need for continuous security improvements and the need for active barriers, such as detect and response mechanisms.

- *Ambiguities in the Legislations*

The legislations in Norway are vague and prioritizes the wrong elements. This presents ambiguity and uncertainty towards what is meant by the non-specific requirements. This leaves it open for interpretation and can cause gaps and divergent practices. Closer communication between organizations, legislators and regulatory authorities can improve and update the focus of security. This means that the critical aspects of security are prioritized, such as patching routines, decommissioning of old ICT and SCADA equipment, utilizing modern security technology, and performing access control. The focus can change towards specific risk reducing measure that has been tested in operations and is proven to be effective against threats. As the legislations remain vague, it becomes the organization's responsibility to ensure that the security measures are effective and up to standard. This is based on the organization's knowledge, competence, resources, etc. These are factors that changes from organization to organization. This is where gaps are created.

5.6 Part 2 - Comparison to HOT Cyber Security Capability Model

The organizations' cyber security capabilities will be compared to the HOT Cyber Security Capability Model in a qualitative analysis. The analysis will uncover focus areas for each organization and provide recommendations. The model description and criteria is described in chapter 4.5. The questions from the interviews are based on the HOT Vulnerability model, which means that the questions are not completely compatible with the HOT Cyber Security Capability Model's indicators. However, the analysis should be able to highlight focus areas that need attention or improvement. Due to nature of the semi-structured interview process, there will be some indicators left blank. This is because the interview did not cover that specific element.

5.6.1 Human Cyber Security Capabilities

1) *End-user ICT competence & behavior*

The end-user's ICT capabilities and general ICT-related behavior. The end-user ICT competence is the foundation for good user behavior. This will increase the general security culture.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Helse Vest IKT operation includes many end-users from different health care organizations within Helse Vest. It is difficult to verify everyone's ICT competence and user behavior. However, their system logs make it is possible to monitor user behavior deviation. *Within Helse Vest IKT:* They have an obligatory e-learning course for all employees and a ICT security directive for all suppliers and third parties, as well as a requirement for being aware of Helse Vest IKT's security strategy and goals. This ensures their user's ICT competence.	Bane NOR is focusing on raising the threat awareness level of the organization, which in turn will increase the ICT competence of end-users. Bane NOR experiences that lower-level (technicians) have the greatest ICT and threat awareness knowledge.	Hafslund is working on increasing the threat awareness of the employees through e-learning courses. They perform fake phishing attempts on employees to gather anonymous data of the overall threat awareness level of the organization.

2) Awareness and willingness to learn

Employee’s willingness to learn and contribute to the security culture, as well as their situational and threat picture awareness.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Shows a great understanding of the threat picture and of vulnerabilities of its operation and organization. However, the interview does not cover awareness and willingness to learn at an employee level.	Shows a willingness to better understand how the threat picture affects its operation. Their railway tradition has a high attention to risk. However, the interview does not cover awareness and willingness to learn at an employee level.	Shows a great understanding of the threat picture and of vulnerabilities of its operation and organization. However, the interview does not cover awareness and willingness to learn at an employee level.

3) Security routine compliance

Employee’s ability to follow the security routines, even with time constraints. Managers should motivate security routine compliance. This is an important part of the overall organizational security culture.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Difficult to gather sufficient data.	Difficult to gather sufficient data.	Difficult to gather sufficient data.

4) Incident and deviation reporting culture

Employee’s ability to report deviations and incidences through the right communication channels. This is an indicator that the safety culture has gained a foothold in the organization.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Helse Vest IKT has focused on raising the reporting culture. It has been a successful objective and the increase in reporting culture of Helse Vest IKT’s users have been documented.	Difficult to gather sufficient data.	Difficult to gather sufficient data.

5.6.2 Organizational Cyber Security Capabilities

1) Ownership

The organization's ability to exercise ownership of the operation. Regardless of how the operation is performed, for example by utilizing ICT services, outsourcing, etc., must the organization own the responsibility and govern the process.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Difficult to gather sufficient data.	Difficult to gather sufficient data.	Focuses on having ownership to the operation and the service providers. Hafslund makes the decisions and controls how the service providers work through their contracts.

2) ICT and Cyber Security Competence

The organization's understanding of digital vulnerability and their ability to implement and evaluate protective measures against digital threats. This means competence level for all employees and managers, as well as, their own ICT specialist functions.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Helse Vest IKT's ICT and cyber security competence is high due to their specialist function within Helse Vest, and their employee e-learning programs ensures employee. It is also a part of the security strategy to raise the overall threat awareness level and competence.	Raising the organization's cyber security competence and capability is a strategy objective.	Raising the organization's cyber security competence and threat awareness is a strategy objective

3) Cyber Security Framework

The basis for all cyber security activities. Often an integrated part of the information security management framework.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Helse Vest IKT is ISO 27000 certified and follows industry	Bane NOR is ISO 27000 certified and follows industry	Is not ISO: 27000 certified, but all their suppliers are. Hafslund is governed by the

regulations, which includes cyber security.	regulations, which includes cyber security.	Beredskapsforskriften (Emergency Regulations)

4) Risk Management

The ability to perform satisfactory value, threat and vulnerability assessments, implement and evaluate practicality and effectiveness of barriers and security measures. This is presented in chapter 3.2.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Has a risk management system.	Has a risk management system.	Has a risk management system.

5) Security Management & Incident Response Management

The ability to manage, evaluate and improve security activities, leadership, and incident response capabilities. As well as, the organization's ability to develop and evaluate security objectives and targets.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Helse Vest IKT has Security & Incident response management capabilities. Performs penetration test and cross-industry drills.	Bane NOR has a security management framework. Bane NOR is in development of detection and response functions, but has emergency response functions. Performs penetration test and cross-industry drills.	Hafslund has Security & Incident response management capabilities. Performs penetration test and cross-industry drills.

6) Documentation and formalization

The documentation and formalization of routines, emergency procedures, security activities & objectives, roles, responsibilities, and reporting channels.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
All risk analyses, roles, responsibilities, security activities, emergency routines are documented.	All risk analyses, roles, responsibilities, security activities, emergency routines are documented.	All risk analyses, roles, responsibilities, security activities, emergency routines are documented.

7) Security Resource allocation

The organization's allocation of resources to cyber security activities.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
There are allocated resources to complete necessary security objectives.	There are allocated resources to complete necessary security objectives.	There are allocated resources to complete necessary security objectives.

8) System overview

An overview or visualization of the operation systems, networks, etc.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Difficult to gather sufficient data.	Difficult to gather sufficient data.	Difficult to gather sufficient data.

9) Leadership engagement and security culture

The leadership's ability to visibly engage in security activities and the organization's security culture.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Attending security forums and professional international conferences.	Bane NOR performs a management review of security. Cyber Security has an anchor in the overall strategy and management.	Cyber Security is anchored in top management and owners (shareholders). Hafslund performs a management review of security.

10) *Collaboration*

The organization's collaboration partners, for example international and national industry organizations, CERTs, security technology producers, and authorities.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Helse Vest IKT collabotrates with HelseCERT and other security technology partners. Helse Vest IKT contributes to shut down cyber criminals with PST, Europol, and Scottland Yard.	Attending security forums and professional international conferences. Collaborates with NorCERT and PST.	Hafslund collaborates with KraftCERT, NorCERT, NVE, and its security technology partners.

11) Supervisory authority engagement and industry regulations

The perceived engagement of industry supervisory authority and the practicality of industry regulations and legislations.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Data Inspectorate, Health Inspectorate, Safety representative (Datatilsynet,, helsetilsynet, verneombudet) are involved in the operation, due to privacy and patient safety.	The railway supervisory authority is in an awakening and they are convinced that they are underdeveloped in this area (cyber security). They developing requirements and are evolving.	The industry supervisory authority, NVE, has increased their engagement the last years. There are still ambiguities in the legislations concerning clarity in definitions and scope.

12) Third party security assurance, control and quality management

Awareness of supply chain/value chain risks and the organization's ability to acquire third party cyber security assurance, control and quality management related to exposure to cyber risk.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Helse Vest IKT requires its suppliers to be ISO 27000 and that they are aware and comply with Helse Vest IKT's security policy.	Bane NOR requires its suppliers to be ISO 27000 certified.	Hafslund Nett has strict third party contractual requirements, related to background check, sub-suppliers, and supplier technology. Hafslund requires its suppliers to be ISO 27000 certified. The requirements contribute to Hafslund's ability to audit and control the third party.

5.6.3 Technological Cyber Security Capabilities

1) *Manual procedures*

The organization's ability to perform the core operation without digital systems. For example, if a hospital's digital journal system fails, the hospital continues to treat their patients.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
The hospitals continue to function without digital systems. There are emergency procedures and plans stored "offline" in all Helse Vest computers.	Difficult to gather sufficient data.	The core function of the SCADA network will function without, or with limited use, of digital systems.

2) *System redundancies*

These are redundancies at component or system level for critical functions of the operation. For example, overlapping wireless zones, multiple data centers, hot-standby duplications of operation centers.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
General redundant network connections and redundancy for critical equipment, such as critical data centers.	A high level of redundancies of connection points and for critical physical equipment and systems, such as operation center.	The SCADA network is operated from undisclosed locations, with redundancies (connection points, equipment, and operation centers) at an industrial standard. The administration network does not have the same level of redundancy.

3) *System recovery functions*

This is enabled by the system logs and makes it possible for the organization to roll back the system to a previous secure state.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Has backup and recovery functions for its networks.	Has backup and recovery functions for its networks.	Has backup and recovery functions for administrative & SCADA network.

4) Incident Detection and Response functions

The organization’s technical ability to detect and form a response to incidences. This is an active and dynamic function that detects and responds to unauthorized activities (for example malware) or odd behavior in the system. This mechanism utilizes sensors that are placed in the digital system and alerts if it detects any suspicious behavior. The initial response function is commonly performed by a on duty security officer. The situation is escalated based on the severity of the event.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Helse Vest IKT has sensors (intrusion detection systems) in their systems. They are capable of incident response and escalation.	Bane NOR’s security strategy includes the development of detection and response functions.	Hafslund has sensors (intrusion detection systems) from a variety of security partners, including their own, in their systems. They are capable of incident response and escalation.

5) User/role-based access control

The organization’s technical ability to securely manage users and user access. A user has been given system access based on the user role. Which means that the system access is limited to the relevant applications, databases, etc. The access control register must be frequently updated to ensure that the right users have the right access.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Has role-based access control functions and performs regular revisions on the “user access rights list”.	Has role-based access control functions and performs regular revisions on the “user access rights list”.	Has role-based access control functions and performs regular revisions on the “user access rights list”.

6) Application whitelisting

This function allows preapproved applications to run. Any application (malware) which is not approved is terminated, unless it can bypass the application whitelist.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Has application whitelist functions.	Has application whitelist functions.	Has application whitelist functions.

7) Decommissioning of old ICT software and architecture

The use of old, unsupported software and hardware is a weak point in the organization. These assets must be decommissioned and replaced with new, supported and secure assets.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Helse Vest IKT uses new, innovating technology and makes sure that all systems are supported.	Bane NOR has a several projects in development. One of the largest projects is to modernize the railway. This include decommissioning old equipment and systems to make place for new technology.	One of the focus areas has been to decommission old ICT architecture and apply modern technology.

8) System traffic logs

The system traffic log is a register and a tool for managing system change, incidents, and problems. It also enables the system recovery functions.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Has an high system traffic log capacity.	Bane Nor has system traffic log capacity.	Has an high system traffic log capacity. All system history is stored, with the mindset "traffic today can be dangerous tomorrow."

9) Strict Patching Routines

Once an exploit has been detected by security technology companies or system manufacturers, it must be patched. The time from detection to the release of the patch is most critical, and is a perfect time to perform a cyberattack. The organization must have strict patching routines and assess the criticality of each patch.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Performs strict patching routines.	Performs strict patching routines, and evaluates the criticality of implementing new patches.	Performs strict patching routines.

10) Limited distribution of admin rights

The organization should have an overview of distributed admin rights and make sure that the individuals that have these right, need them. This is a challenge when using third parties and outsourcing.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Limits the admin rights and system rights to the employees who needs it to perform their tasks.	Limits the admin rights and system rights to the employees who needs it to perform their tasks.	Limits the admin rights and system rights to the employees who needs it to perform their tasks.

11) Modern Security Technology

The organization must orient themselves in the modern security technology market. Basic and traditional security technology, such as firewall and email filter, prohibits most cyberattacks.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Helse Vest IKT uses modern security technology, such as firewalls and email filters.	Bane NOR's uses modern security technology, such as firewalls and email filters.	Hafslund's uses modern security technology, such as firewalls and email filters.

12) Separate networks and domains

The separation of administrative networks and production (SCADA/ICS) networks reduces interconnectivity and access points.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Separate domains and networks.	The administrative network and production network is separate.	The administrative network and production network is separate. There are some domains that require high levels of security and some that requires less security, for example innovation "sandboxes".

13) Security zones and physical distinctions

The physical distinction between publicly accessible areas, employees only, and limited access. This translates into for example publicly accessible wifi vs sensitive networks, offices vs common room vs control room, etc.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Critical location, functions and equipment have security zones and access control.	Critical locations, functions and equipment have security zones and access control. The different security zones have own cabled networks.	Critical location, functions and equipment have security zones and access control.

14) Protection against burglaries

Physical barriers and alarm systems in critical rooms, data centers, equipment in the field, etc.

Helse Vest IKT:	***Bane NOR:***	***Hafslund Nett:***
Most heath care locations are open to the public. However, special locations have physical security, surveillance, and alarms at an industrial standard level.	Locations that need it have physical security, surveillance and alarms on an industrial standard level.	Locations that need it have physical security, surveillance and alarms on an industrial standard level.

*consequence reduction/last resort solutions

5.7 Part 2 - Results

5.7.1 General Areas of Improvement

The organizations' cyber security capabilities have been analyzed. Here are some general areas of improvement for all three organizations:

- *Long-term vision*

The main objective of cyber security is to provide updated threat picture knowledge, understand how it affects the organization and its operation, and implement security measures or adjust to external threats, then measure the performance of the security measure and evaluate. This is an active risk management mechanism and is a constant improvement cycle. Additionally, the organization must understand how internal decisions and behavior affects the cyber risk exposure. As the external threat picture evolves, the organizations must follow. The test is: does the organization have the capability to adjust to the evolving external threats, and does it understand how internal factors affects the organization's cyber risk exposure? As a recommendation, all three organizations must ensure that this cycle is performed regularly and strive for better quality and performance.

- *Lack of performance indicators for security*

A critical point in this cycle to create measurable security targets and requirements. All three organizations stated that they lacked specific performance indicators for security activities. However, there are performance indicators and requirements for emergency response. This is probably due to what they identify as a performance indicator. A security strategy has objectives, and each objective has requirements or targets. In some cases, these requirements are difficult to concretize and measure, such as increase employee threat awareness, or management engaged. The requirements for performance can be represented and measured quantitatively or qualitatively. All security measures or activities should have a directly or indirectly measurable indicator to ensure progress, performance and quality. The indicators can provide data which the organization can use to develop statistics and review the security measure. In some cases, the security measure itself can be used as a statistical basis, such as the firewall log, system traffic log, etc.

The organizations should carefully develop requirements and directly or indirectly measurable indicators for intangible security measures, such as the effectiveness of collaborations (CERTs and authorities), operation or service ownership, and third party security assurance. Two good examples of measurable indicators are Helse Vest IKT's increase in reporting culture and Hafslund Nett's fake phishing attempts on own employees. Both provide a statistical basis for evaluating the awareness and skill of the employees, and it can be used in evaluating the effectiveness of e-learning courses.

The development of measurable security performance requirements and targets is an indication of cyber security understanding and awareness.

5.7.2 Individual Areas of Improvement

Helse Vest IKT

Helse Vest IKT is an organization which understands the importance of cyber security. The management is engaged in the security activities and has developed some security targets. They have covered the main parts of HOT vulnerabilities model and performs well according to the HOT CS model. Their strengths are a high-level of ICT competence in the organization, a strong risk management system, collaboration efforts, leadership engagement, emergency preparedness, innovation, and their technological cyber security capabilities. Their areas of improvement are:

- *End-user ICT competence & behavior*

It is difficult to make sure that each end-user has the necessary ICT competence requirements in such a large organization as Helse Vest. However, every user carries the risk or making an error or causing an unwanted event, for example low user knowledge about phishing may increase the probability of successful phishing attempts. Non-ICT personnel to think more about the risks related to their job description (patients and patient treatment), rather than the cyber risks. This means that it is not a priority for non-ICT personnel to pay attention to this. However, a general awareness campaign of relevant cyber threats (such as ransomware) and good ICT behavior can improve the general security culture of Helse Vest and make cyber threats a common subject.

Bane NOR

Bane Nor understands the importance of cyber security and devotes focus and resources to the area. Their organization is in a change-process and they are developing digitalization projects. Their operation becomes more digital-based. Because of this, they have raised attention to understanding how cyber risks affect their operation and organization. Their strengths are the technological cyber security capabilities, their ICT and engineering competence-level, risk management system, and emergency preparedness. Their areas of improvement are:

- *Threat picture understanding & systems overview*

Bane Nor's operation is affected by cyber risk, due to their variety of systems and equipment. The organization is developing threat picture understanding. This is an excellent time to develop a visual representation of the systems and the associated cyber risk/threat. This is a tool which can provide greater cyber risk understanding and systems overview.

- *Third party management & ownership*

Bane Nor should develop measurable third party security requirements and find ways to review/enforce these requirements and performance. It is common to use service providers and outsource parts of the operation, and it seems as this is the strategy of Bane Nor. Therefore, is third-party management and operation/service ownership important in the future.

- *Collaboration*

Bane Nor should be a member of a CERT, in addition to the existing collaboration with NorCERT. The benefits of a CERT will increase cyber security knowledge and threat picture intelligence. Due to the variety of engineering disciplines, systems and equipment found in Bane Nor, the national CERTs may not seem relevant. Then, it is possible to create an international railway CERT between, for example Norway, Sweden, Denmark, and the UK.

Hafslund Nett

Hafslund Nett understands the importance of cyber security. They are dedicating resources to employee awareness, technological security and collaboration efforts. Their strengths are their technological cyber security capabilities, collaboration efforts, ownership to the operation, ICT and cyber security competence, and emergency preparedness. Their areas of improvement are:

- *Risk Management*

Hafslund Nett stated that the risk and vulnerability analyses has been previously performed out of compliance to the legislations, but has changed the focus become a more practical tool. These analyses require experience and practice to become a reliable tool. It is challenging to include all aspects of the operation and still maintain a sense of objectivity while representing the uncertainty of the risk analysis. Hafslund Nett should pay attention to the quality of the risk analyses, as ICT becomes a more integrated part of its operation.

Chapter 6 - Discussion

The Analysis

The nature of the subject cyber security is limiting the depth and detail of the analysis. The organizations cannot share system "secrets", or specific information which can be used to initiate a cyberattack. The first part of the analysis makes a considerable effort to compare the industry solutions and highlights the similarities, key issues and challenges in an understandable manner. The second part of the analysis is difficult gather sufficient data to make a detailed analysis and express comprehensive individual improvement areas. However, all three organizations should strive for better solutions and continuous improvement, even though this analysis does not discover any critical flaws.

The author's current level of understanding the subject impacts the way the technological solutions and terms are presented. It is mostly based on a "function-level" and moves away from the detailed ICT technological terms. The benefit is that non-ICT individuals should be able to understand the content of this thesis.

The Results

The three organizations leave a great impression and it was rather unexpected to see how they well approach the security challenges. They are future-oriented and have a practical association with risk and vulnerabilities in digital systems. There is a will to invest in security technology and measures, develop competence and experience in the organization, and collaborate with other professional organizations and authorities. This is a change and development in response to the growing threat towards digital systems. The organizations innovate, develops and utilizes new digital technology to perform more efficiently and applies ICT to improve security. The focus on vulnerabilities in digital systems has evolved.

All three organization have no experience of large-scale targeted cyberattacks. However, there is an increase in cybercrime related events, such as phishing and ransomware. This is considered as noise, and does not represent a critical threat. Although, it would be a different matter if the organizations did not have detect and response mechanisms. The technical barriers, such as modern firewalls and recovery functions, reduces most consequences related to generic cyberattacks and user or system errors. Even though, there are barriers and mechanisms that reduce the risk of human factors, the main challenge, or weakness, is still user behavior and awareness. And, the threat agents are aware of this. Another element which is not usually discussed is how management decisions impact the vulnerability of the organization. The impression from the interviews is that the organizations' management is involved and are aware of the risks related to long and complex supply chains, the use of third parties and outsourcing.

There seem to be little difference in security measures between these three organizations regardless of their industrial sector. They have a modern focus on implementing risk reducing measures, technical barriers, and promote user and management awareness. Their overall strategy has security as a premise or as a main objective. Emergency response is a part of the organizations' operation, whether it is cyber-related or not.

Procedures and documentation for roles, responsibilities, and communication channels have been made. It is tested/rehearsed in larger cross-sector drills or in smaller desktop drills.

All three organization have an active association to risk. There are risk assessments made related to system change, incident, and failures. The main goal is to have risk assessments that has practical value and lead to usable risk reducing measures or barriers. A good example of where security activities have practical value, are the external system penetration tests. These functions as a practical assessment of system vulnerability and the results presents clear areas of improvement. Risk assessments is a tool for making observations and systematically assess the risks of the system. The challenge is to ensure insight and system overview to connect all the different sub-systems and disciplines to create a reasonable risk assessment and risk reducing measure that encompasses the total risk picture. This requires practice and expertise.

As supply chains become long and complex, the focus on risk assessments grow. The three organizations are aware of the potential threats in outsourcing and the use of cloud services. However, the organizations do use these services to some extent. The challenge is to have ownership and control over the service providers and be aware of who have access to what, in terms of sensitive information and potential exploits.

The CERTs, along with security partners and authorities, play an important role in giving the organization updated information about the threat picture. The information which is shared works as an important active and preventive barrier. The updated patches from the security partners makes sure that the organizations are equipped to handle the latest threats. Also, the CERTs can communicate if there are any specific threats that abound in the sectors. Anonymity works as an enable for sharing experiences. The three organizations agree that transparency and communication is a key factor in improving securing and learning from others. However, there are certain elements that should not be discussed because it poses a security threat.

There is a focus on continuing to develop and implement innovative solutions, despite the concern for failure or potential risk. This does not mean that they are mindless in their concern for digital risk, but it does not act as a barrier. Innovation can occur in separate “sand-box” environments where security is not an issue. The overall focus is more toward making security the enabler and baseline for innovative solutions.

A Systematic Approach to Management Decisions

Management decisions are contributing to exposure and vulnerabilities in digital systems, mainly the when managing sensitive information and ICT systems. These are decisions that exposes the organization to unwanted events, typically decision related to outsourcing of ICT operation or cloud services. These are services that manage sensitive data, has potential access to production network, or similar. A systematic approach considers the risks and potential exposures of introducing third parties and compares it to other alternatives in the initial decision process. Cost is the main driver for any project, but there is a need to value other factors, such as assurance, governance, and financial stability. As stated in chapter 3, there are risk associated with long fragmented supply chains and the difficulty in ensuring control and compliance. These intangible factors need to be given a value or a scale to be compared with the cost of labor or other easily defined factors. Knowledge, expertise and experience plays a part in this process. Therefore, management needs a technical understanding of the ICT systems and its vulnerabilities. If a company decides to go for a third-party alternative, there must be transparency between the involved parties. Considerable efforts must be made in ensuring that the customer has ownership of the operation or service and that the service provider can assure quality and met the information and cyber security obligations and compliances. This must also be taken into consideration in the decision process.

Outsourcing without fully understanding the risk in contains, can cause more harm than a cyberattack (ref. Statoil, Helse Sør-Øst chapter 3.5.1 and 3.5.2). Understanding the technical vulnerabilities and having a system overview is an important challenge in digitalization. Visualization techniques can improve system overview and a renewed systematic approach to decision making can reduce the risk of poor management decisions.

Corporate Social Responsibility

Management must care for information and cyber security and be aware of vulnerabilities in digital systems, in the same way that they are concerned by traditional health, safety, and environmental issues. It should be a shareholder and top-management concern and a part of the corporate social responsibility to ensure security, making sure that the stakeholders are unaffected security issues in their operation, products, or services. It is profitable to remain protected against data-loss, production stop, industrial espionage, etc. caused by cyber-related events. Technology allows efficient digital solution, smart and optimized operation and maintenance. As more information stored and made available, the need for security becomes a premise for a sustainable operation.

Clear Legislation Definitions and Industry Alignment

To assure a common future direction in information and cyber security, there must be agreement, alignment between authorities and organization, and clear definitions in legislations. This means that the different industries and its supervisory authority should make regulations which have a basis in practical and effective security measures. The industries have tested what security measures are the most effective and this knowledge can be taken into consideration. An alignment of the involved parties can ensure a coherent industry vision, objectives and supervisory control.

ICT and cyber security in Education

As ICT and traditional engineering converge, there becomes a need for ICT knowledge in engineering. Schools, universities, and colleges can incorporate ICT and cyber security in the same way that traditional HSE has been a part of the curriculum for years. This will benefit both disciplines in that they have a common language and understanding of ICT risk.

Chapter 7 – Reflections on Scope of Work

7.1 Reflections on Scope of Work and Objectives

The thesis presents the connection between of digitalization, digital risk and cyber security. It is supposed to present the challenges and how they relate to each other. The main objective is to perform an analysis to find the organization's cyber security capabilities identify the areas of improvement. The relationship between the various topics has been presented throughout three chapters. A quick introduction of the drivers, impact and challenges of digitalization. The thesis continues to address the risks related to digitalization, connectivity, technology, organization, and human factors, along with practical examples. Further, the topic of cyber security presents threat agents, key points from previous studies, best practices, and an introduction to incident response. These topics creates the baseline for understanding cyber security from the different aspects, such as organization, technological, and human factors. Two models are provided as a foundation for the analysis, and has been based on the literature study. The analysis compares the industry solutions, key issues and challenges, and their cyber security capabilities. The analysis concludes with identifying areas of improvement. Further, a discussion of the results is performed in chapter 6. This conclude the fulfillment of the scope of work and objectives.

7.2 Challenges encountered

The way that digitalization, risk and cyber security affects the modern organization is interesting. It has been an ambitions task to start with little to no knowledge about the subject and learn more as the thesis progressed. Initially, a lot of time was spent acquiring knowledge about the subject and identifying the scope and objectives. It has been difficult to limit the range of the scope and still cover the subjects, while retaining depth. The analysis is limited by the current level of understanding of the area. Some of the topics are difficult to gather sufficient data to present a representative answer.

The most interesting part of the thesis has been the interviews. This allowed the author to see the practical impact of information and cyber security, and gain insight to how the organizations approach the challenges. However, it has been difficult to understand how their operation and organization works, beyond a conceptual understanding. The three organizations have large operations that includes many disciplines. The interviews were quite long (averaged at around 110 minutes) and required a lot of time finishing to making it presentable. There is secrecy involved in this topic. Therefore, it may be difficult to get actual practical examples of security related issues and solutions of critical core functions, nor was it aimed at specific systems other than the general operation. However, the quality or objectives of the thesis did not suffer because of this. Further studies can, if possible, address the issues of vulnerability to one specific hybrid system (ICT and engineering).

7.3 Areas for Further Studies

This thesis describes the lack of performance indicators and measurable security targets as one of the general improvement areas. This is an area where future studies can develop indicators based on the models in this thesis, and approach organizations with a quantitative questionnaire. It can be used as a benchmark tool for cyber security capabilities with a list of measurable HOT requirements and indicators. This thesis looks at cyber security from a general organizational perspective. Future studies specialize to one hybrid (ICT and engineering) system, and perform value, threat, and vulnerability assessment to enable potential risk reducing measures. Additionally, a study of measuring performance and quality of security in future data-driven digital technologies and organizational network structures. The decision-making aspect of risk related to outsourcing of ICT functions and ICT service providers can be an interesting topic. How do organizations establish measurable contractual requirements for security, and how do they enforce those requirements?

Chapter 8 - Conclusion

The security situation has changed significantly throughout a couple of years. The three organizations in this study has increased their focus on cyber security and are aware of vulnerabilities and risk associated with technology. Cyber security has become a common topic. Cyberattacks and digital vulnerabilities are frequently in the news. Organizations change with technology, and they should embrace the security aspect that comes with innovation and new technologies.

Security is a collaborative effort and is not possible to successfully achieve singlehandedly. The CERT communities are growing and act as a forum for cyber security. The CERTs and the security technology companies has an active role and are most vital for security in organizations. They provide updated threat intelligence and patches to fix current exploits. This information and expertise would be difficult for organizations to obtain themselves. As threats evolve over time and become more frequent and sophisticated, the role of these organizations become more important. Organizations should be competitors in business, but embrace the synergy effect in sharing and collaborating in security.

The most common exploit and vulnerability in digital systems is still related to human factors. Threat agents target employees in reconnaissance missions to find weaknesses in systems. Social manipulation, unaware users, and information from social networking sites are large information sources. One of the most important challenges is to increase user awareness and behavior, as well as managerial understanding. Modern security technology and basic security principles reduces most risk associated with vulnerabilities in digital systems. However, they will never be able to defend against all threats. This is where detect and response contributes as an active barrier. The threat agents will find ways to bypass the passive security barriers and enter the system. The detect and response mechanisms will greatly reduce the consequences of a cyberattack, along with the system recovery functions. Further, the information gained from the attack can be distributed to other organizations, so that they can prepare or adjust to the threat.

Authorities and industry organizations should discuss a future direction for security regulations. As technology and threats evolve, the security regulations may not be coherent with the modern ways of securing an organization. Supervisory authorities can increase their visibility in professional forums and communicate with the industry to gain knowledge of functional security technology, measures and procedures. Technology and modern operations makes ICT and traditional engineering converge. This creates an opportunity for schools, universities and colleges to decrease the gap between the two disciplines. This can increase systems overview and, in turn, increase security in systems.

The threat towards digital systems and organizations continues to evolve. The organizations must evolve with the growing threat and the new innovative solutions. Security measures should not be implemented out of compliance, but out of self-interest. Security is a premise for a successful and sustainable future.

Bibliography

1. Altinn, 2016. *Om Altinn*. [online] Available at: https://www.altinn.no/no/Toppmeny/Om-Altinn/ [Accessed 17.05.2017]
2. ATOS, 2012, *The convergence of IT and Operational Technology*, [pdf] Avaliable at: https://atos.net/content/dam/global/ascent-whitepapers/ascent-whitepaper-the-convergence-of-it-and-operational-technology.pdf [Accessed 06.02.2017]
3. Aven, T., 2015. *Risk analysis*, 2nd edition, John Wiley & Sons.
4. Aven, T., Krohn, B.S. 2014. *A New Perspective on how to Understand, Assess and Manage Risk and The Unforeseen* from *Reliability Engineering and System Safety volume 121*. Elsevier.
5. Avinor, 2017. *Fjernstyrte tårn.* [online] Available at: https://avinor.no/flysikring/vare-tjenester/remote-towers/ [Accessed 17.05.2017]
6. Bang, K. E. and Markeset, T. 2011a. *Identifying the Drivers of Economic Globalization and the Effects on Companies' Competitive Situation*, In: The Proceedings of the International Conference on Advances in Production Management Systems. Stavanger, Norway, September 26-28th (2011)
7. Bang, K. E. and Markeset, T., 2011b. *Impact of Globalization on Model of Competition and Companies' Competitive Situation.* In: The Proceedings of the International Conference on Advances in Production Management Systems, Stavanger, Norway, September 26-28th (2011)
8. Baur, C., Wee, D., 2017. *Manufacturing's next act*. McKinsey & Company. [online] Available at: http://www.mckinsey.com/business-functions/operations/our-insights/manufacturings-next-act. [Accessed 15 May 2017].
9. Bawane, M. S., Shelke, C. J., 2014, Analysis of increasing hacking and cracking techniques, International Journal of Application or Innovation in Engineering & Management (IJAIEM), ISSN 2319 - 4847
10. Bratbergsengen, K., 2016. *Digitalisering*. [online] Available at: https://snl.no/digitalisering [Accessed 25.06.2017]
11. Brown, A., 2016. *Watch These Self-Driving Drone Tractors Redefine Farming*. [online] Available at: https://www.yahoo.com/news/watch-self-driving-drone-tractors-154658185.html. [Accessed 15 May 2017].
12. Chaffey, P., 2017. *Det skal lønne seg å digitalisere.* [online] Available at: https://www.regjeringen.no/no/aktuelt/skal-lonne-seg-a-digitalisere/id2527613/ [Accessed 26.07.2017]
13. Cyber Threat Intelligence Network, 2016. *ISAOS & ISACS*. [online] Available at: http://ctin.us/site/isaos/ [Accessed 15.02.2017]
14. Datatilsynet, 2017. *Hva er skytjenester?*. Datatilsynet. [online] Available at: https://www.datatilsynet.no/Teknologi/Skytjenester---Cloud-Computing/Hva-er-nettskytjenester/. [Accessed 15 May 2017].
15. Direktoratet for e-helse, 2016a. *Én innbygger – én journal*. [online] Available at: https://ehelse.no/strategi/n-innbygger-n-journal. [Accessed 02.03.2017].
16. Direktoratet for e-helse, 2016b. *m-Helse*. [online] Available at: https://ehelse.no/m-helse [Accessed 02.03.2017].
17. DNV GL, 2015. *Digitale Sårbarheter Olje & Gass.* Lysneutvalget. [pdf] Available at: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/5.pdf [Accessed 05.01.2017]
18. Dvergsdal, H., 2015. *Stordata*, Store norske leksikon, [online] Available at: https://snl.no/Stordata. [Accessed 04.02.17]

19. Eason, K., 1992, Information technology and organizational change, Taylor & Francis. *Chapter-4: Towards the socio-technical design of information technology systems.*
20. EOS services, 2010, *Cybersikkerhet – Bakgrunnsnotat*, Koordineringsgruppen for IKT-risikobildet; Etterretningstjenesten, PST og NSM, [pdf] Available at: https://www.regjeringen.no/contentassets/252f869fdfac46648e41e6ca5fb0600a/cybersikkerhet_svar-med-merknader_nsm-pst-etterretningstjenesten.pdf [Accessed 27.01.17]
21. European Commission, 2017, The importance of the digital economy [online] Available at: https://ec.europa.eu/growth/sectors/digital-economy/importance_en [Accessed 06.02.2017]
22. EY, 2014, *Cyber program management*. [pdf] Available at: http://www.ey.com/Publication/vwLUAssets/EY-cyber-program-management/$FILE/EY-cyber-program-management.pdf [Accessed 08.02.2017]
23. Falliere, N., Murchu, L., Chien, E., 2011, *W32.Stuxnet Dossier*, Symantec, [pdf] Avaliable at: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf [Accessed 01.02.17]
24. Feide, 2017. Om Feide [online] Available at: https://www.feide.no/om-feide [Accessed 19.03.2017].
25. Gaarder, A., 2016. *Vil Robotic Process Automation (RPA) ta over jobbene våre?* [online] Available at: https://utbrudd.bouvet.no/2016/03/30/vil-robotic-process-automation-rpa-ta-over-jobbene-vare/
26. Gartner IT glossary, 201?, *Operational Technology (OT)*, [online] Available at: http://www.gartner.com/it-glossary/operational-technology-ot/
27. Goetz, E., Shenoi, S., 2008, Critical Infrastructure Protection. *Chapter 7: Reducing risk in oil and gas production operations* by *Johnsen, S., Ask, R., and Roisli, R*. First conference of IFIP International Federation for Information Processing. [pdf] Available at https://www.researchgate.net/profile/S_Johnsen/publication/221654737_Reducing_Risk_in_Oil_and_Gas_Production_Operations/links/565dbe8c08aefe619b26a695.pdf?origin=publication_list [Accessed 14.03.2017]
28. Hammarberg, D., 2014. The Best Defenses Against Zero-day Exploits for Various-sized Organizations [pdf] Available at: https://www.sans.org/reading-room/whitepapers/bestprac/defenses-zero-day-exploits-various-sized-organizations-35562 [Accessed 22.03.2017]
29. Harding, L., 2017, What we know about Russia's interference in the US election, [online] Available at: https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election [Accessed 19.02.2017]
30. Heimsvik, O., 2017. Alvorlig sikkerhetsbrudd i It’s Learning - sensitiv informasjon kan være på avveie - Aftenbladet.no. [online] Available at: http://www.aftenbladet.no/lokalt/Alvorlig-sikkerhetsbrudd-i-Its-Learning---sensitiv-informasjon-kan-vare-pa-avveie-540642b.html [Accessed 19.03.2017].
31. Hendrick, H.W., Kleiner, B., (ed.) 2002, Macroergonomics: Theory, methods, and applications, Human factors & Ergonomics. *Information and Communication technology (ICT) and changes in work life: Macroergonomic considerations by Bradley, G.*
32. Hoske, M., T., 2014, *Industry 4.0 and Internet of Things tools help streamline factory automation*, CFE Media [online] Available at: http://www.controleng.com/single-article/industry-40-and-internet-of-things-tools-help-streamline-factory-automation/9c8b622a9da7931dc821b20fccdc41a6.html [Accessed 06.02.2017]

33. IBM, 2016. *Robotic Process Automation*. [pdf] Available at: https://www-935.ibm.com/services/multimedia/dl_17119_rpa_flyer_04.pdf [Accessed 16.05.2017]
34. Imperva, 2013, *Web Application Attack Report*, [pdf] Available at: https://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed4.pdf [Accessed 26.01.2011]
35. Intel Corporation, 2016. Intel Brings Robust Data Analytics to Vehicles, Faster. [pdf] Available at: https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/telematics-fleet-management-solution-brief.pdf [Accessed 01.06.2017]
36. Inverstorpedia, n.d., Peer-to-Peer (P2P) Service, [online] Available at: http://www.investopedia.com/terms/p/peertopeer-p2p-service.asp [accessed 03.02.17]
37. Investment Industry Regulatory Organization of Canada (IIROC), 2016, *Cybersecurity Best Practices Guide*, [pdf] Available at: http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf [Accessed 01.03.2017]
38. IRPA (Institute for Robotic Process Automation), 2014. *What is Robotic Process Automation?*. Available at: http://irpaai.com/what-is-robotic-process-automation/ [Accessed 16.05.2017]
39. ISACA, 2016, *The Merging of Cybersecurity and Operational Technology*, [pdf] Avaliable at: http://www.isaca.org/Knowledge-Center/Research/Documents/IT-OT_wp_eng_0716.pdf?regnum=356037 [Accessed 06.02.2017]
40. Jaatun, M. G., Johnsen, S. O., Bartnes, M., Longva, O. H., Tøndel, I. A., Albrechtsen, E., Wærø, I., 2007, *Incident Response Management in the oil and gas industry*, Sintef [pdf] Available at: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2375186/SINTEF%2bA%2b4086%2bIncident%2bResponse%2bManagement%2bin%2bthe%2boil%2band%2bgas%2bindustry.pdf?sequence=3&isAllowed=y [Accessed 06.03.2017]
41. Jørgenrud, M., 2017. *Kobler hackerangrep mot Norge til mulig produksjon av masseødeleggelsesvåpen* [online] digi.no. Avaliable at: https://www.digi.no/artikler/kobler-hackerangrep-mot-norge-til-mulig-produksjon-av-masseodeleggelsesvapen/378355 [Accessed 22.03.2017]
42. Justis- og beredskapsdepartementet, 2013. *Ett politi – rustet til å møte fremtidens utfordringer*. NOU 2013:9 [pdf] Available at: https://www.regjeringen.no/contentassets/5e2a1012dbc7449e8f57813e7822252b/no/pdfs/nou201320130009000dddpdfs.pdf [Accessed 07.06.2017]
43. Kambic, K., Aurthor, K,. Ellis, W., Jensen, T., Johansen, K., Lee, B., Liles, S, 2013, *Crude Faux: An analysis of cyber conflict within the oil & gas industries*, Purdue University [pdf] Available at: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2013-9.pdf [Accessed 07.03.2017]
44. Klima- og miljødepartementet, 2014. *Klimaforliket*. [online] Available at: https://www.regjeringen.no/no/tema/klima-og-miljo/klima/innsiktsartikler-klima/klimaforliket/id2076645/ [Accessed 26.05.2017]
45. Knapskog, S., J., 2016. *Informasjonssikkerhet.* [online] Avaliable at: https://snl.no/informasjonssikkerhet [Accessed 11.03.2017]
46. KraftCERT, 2017. *Tjenester vi tilbyr*. [online] Available at: https://www.kraftcert.no/tjenester.html. [Accessed 14.05.2017].
47. Kunnskapsdepartementet (KD), 2017. *Informasjon om hackerangrepet mot norske institusjoner*. [letter] Available at: https://www.oep.no/search/resultSingle.html?journalPostId=21345854 (request access) [Accessed 24.03.2017]

48. Lloyd’s, 2010. *Digital Risk Report – Managing Digital Risk.* [pdf] Available at: https://www.lloyds.com/~/media/lloyds/reports/360/360-digital/lloyds_360_digital_risk_report-(2).pdf [Accessed 27.02.2017]
49. Lysneutvalget, 2016, Digitalt grenseforsvar, Avaliable at: https://www.regjeringen.no/contentassets/ca1f705dbebd48cb9a61889d4cfee6bf/digitalt-grenseforsvar-lysne-ii-utvalget.pdf [Accessed 19.02.2017]
50. MacRae, M., 2016. The RoboDoctor Will See You Now. *The American Society of Mechanical Engineers*. [ONLINE] Available at: https://www.asme.org/engineeringtopics/articles/robotics/robo-doctor-will-see-you-now. [Accessed 05.03.2017].
51. Marinos, L., 2014. *ENISA Threat Landscape 2014.* [pdf] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2014 [Accessed 18.05.2017]
52. Marinos, L., Belmonte, A., Rekleitis, E., 2016. *ENISA Threat Landscape 2015*. [pdf] Available at: https://www.enisa.europa.eu/publications/etl2015 [Accessed 03.04.2017]
53. McAfee, 2011, Global Energy Cyberattacks: “Night Dragon”, McAfee Foundstone Professional Services and McAfee Labs. Avalialbe at: https://www.mcafee.com/hk/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf [Accessed 02.02.2017]
54. Mueller, P., Yadegari, B., 2012, *The Stuxnet Worm,* [pdf] Available at: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf [Accessed 01.02.17]
55. Nilsen, J., 2014. *Kraftbransjen etablerer eget sikkerhetsselskap*. Teknisk Ukeblad. [online] Available at: https://www.tu.no/artikler/kraftbransjen-etablerer-eget-sikkerhetsselskap/231792. [Accessed 14.05.2017].
56. Norton, n.d., *Spear Phishing: Scam, Not Sport*, [online] Available at: https://us.norton.com/spear-phishing-scam-not-sport/article [Accessed 26.01.2011]
57. Norwegian Intelligence Service, 2017, *Fokus 2017*, [pdf] Available at: https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2017-utskriftvennlig.pdf [Accessed 08.02.2017]
58. NSM, 2009, Nasjonal strategi for cybersikkerhet - Forebygging og håndtering av IKT-hendelser med store samfunnsmessige skadefølger, [pdf] Avaliable at: https://www.regjeringen.no/globalassets/upload/fd/horingsdokumenter/cybersikkerhet-strategi-forslag_hoeringsnotat.pdf [Accessed 27.01.17]
59. NSM, 2015. *Helhetlig IKT-risikobilde 2015*. [pdf] Available at: https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2015_lr.pdf [Accessed 05.03.2017]
60. NSM, 2016a, *Helhetlig IKT-risikobilde 2016*, Available at: https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2016_web_enkel.pdf [Accessed 08.02.2017]
61. NSM, 2016b?. *Risikovurdering for sikring.* [online] Available at: https://www.nsm.stat.no/globalassets/dokumenter/handboker/risikovurdering_nsm_handbok_mars2016.pdf [Accessed 26.05.2017]
62. NSM, 2017. *Varslingssystem for digital infrastruktur (VDI)*. [online] Available at: https://nsm.stat.no/norcert/varslingssystem-for-digital-infrastruktur-vdi/. [Accessed 14.05.2017].
63. Omland, E., Wernersen, C., 2017. *Største dataangrepet verden har sett*. NRK [online] Available at: https://www.nrk.no/norge/nsm_-_-storste-dataangrepet-verden-har-sett-1.13515221 [Accessed 25.07.2017]

64. Omland, E., Wernersen, C., 2017. *Største dataangrepet verden har sett*. NRK [online] Available at: https://www.nrk.no/norge/nsm_-_-storste-dataangrepet-verden-har-sett-1.13515221 [Accessed 25.07.2017]
65. Østbø, H., M., 2017. It's Learning-problemet er løst - Aftenbladet.no. [online] Available at: http://www.aftenbladet.no/lokalt/Its-Learning-problemet-er-lost-540665b.html [Accessed 19.03.2017].
66. Ovide, S., 2017, Facebook Risks Breaking Its Perfect Business Model, Bloomberg L.P., [online] Avaliable at: https://www.bloomberg.com/gadfly/articles/2017-01-09/facebook-learns-to-share-but-may-break-its-perfect-business-model [Accessed 03.02.2017]
67. PWC, 2015, The Sharing Economy, [pdf] Available at: https://www.pwc.com/us/en/technology/publications/assets/pwc-consumer-intelligence-series-the-sharing-economy.pdf [Accessed 03.02.2017]
68. PWC, 2017a, The Global State of Information Security Survey 2017, [pdf] Available at: https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf [Accessed 15.02.2017]
69. PWC, 2017b, Cyber Crime Survey 2017, [pdf] Available at: http://www.pwc.no/no/tjenester/consulting/business-technology/cybercrime-survey.pdf [Accessed 15.02.2017]
70. Remen, A. C., Tomter, L., 2016, *Tastefeilen som stoppet Statoil*, [online] Available at: https://www.nrk.no/norge/xl/tastefeilen-som-stoppet-statoil-1.13174013 [Accessed 06.03.2017]
71. Restad, H., 2015. *WikiLeaks*. [online] Available at: https://snl.no/WikiLeaks [Accessed 02.05.2017]
72. Rick, T., 2016. *The real challenges of digitization is not technology*. [online] Available at: https://www.torbenrick.eu/blog/technology/the-real-challenges-of-digitization-is-not-technology/. [Accessed 15 May 2017].
73. Robertson, J., Riley, M., 2014. *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar.* [online] Bloomberg Technology. Available at: https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar [Accessed 27.03.2017]
74. Rockwell Automation, 2016a, *Smart Manufacturing*, [pdf] Available at: http://literature.rockwellautomation.com/idc/groups/literature/documents/wp/cie-wp007_-en-p.pdf [Accessed 06.02.2017]
75. Rockwell Automation, 2016b, *You can't achieve Smart Manufacturing without embracing modern technology*, [pdf] Avaliable at: http://literature.rockwellautomation.com/idc/groups/literature/documents/sp/cie-sp005_-en-p.pdf [Accessed 06.02.2017]
76. Rouse, M. 2014. What is customer relationship management (CRM)? *Techtarget*. [online] Available at: http://searchcrm.techtarget.com/definition/CRM. [Accessed 02.03.2017].
77. Rouse, M., 2016, *Internet of things*, Techtarget, [online] Available at: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT [Accessed 04.02.2017]
78. Salesforce, 2016. Healthcare CRM: Improve Relationships Between Patients and Staff. *Salesforce* [online] Available at: https://www.salesforce.com/solutions/industries/healthcare/overview/. [Accessed 05.03.2017].
79. Sanner, J., T., 2015. *Planlegging for framtiden*. [online] Available at: https://www.regjeringen.no/no/aktuelt/plankonferansen-2015/id2395505/ [Accessed 26.05.2017]
80. Sivertsen, E., Sommer, P., 2017. *Google: – Bli digital eller dø*. NRK [ONLINE] Available at: https://www.nrk.no/kultur/google_-_-bli-digital-eller-do-1.13451727. [Accessed 15.05.2017].

81. Skjeggestad, S. R., Stolt-Nielsen, H., Tomter, L., Omland, E., Strønen, A., 2017, *Norge utsatt for et omfattende hackerangrep*, NRK.no [online] Available at: https://www.nrk.no/norge/norge-utsatt-for-et-omfattende-hackerangrep-1.13358988 [Accessed 19.02.2017]
82. Skjetne, O., L., 2017. PST: *Ni norske epostkontoer utsatt for målrettet russisk hackerangrep, også PST selv* [online] vg.no. Avaliable at: http://www.vg.no/nyheter/innenriks/politiets-sikkerhetstjeneste-pst/pst-ni-norske-epostkontoer-utsatt-for-maalrettet-russisk-hackerangrep-ogsaa-pst-selv/a/23915390/ [Accessed 22.03.2017]
83. SMMT (The society of motor manufacturers and traders limited), 2017. *Connected and autonomous vehicles.* [pdf] Avaliable at: https://www.smmt.co.uk/wp-content/uploads/sites/2/Connected-and-Autonomous-Vehicles-Revolutionising-Mobility-in-Society.pdf [Accessed 26.05.2017]
84. Solberg, P., Bjerkeseth, A., Brønseth, N., 2015. *Slik blir framtidens flyplasser.* [online] Available at: https://www.nrk.no/buskerud/slik-blir-framtidens-flyplasser-1.12575787 [Accessed 17.05.2017]
85. Sunde, K., E., 2017. *Konjunkter, Digitalisering og Politikk.* Norsk Industri. [online] Available at: https://www.norskindustri.no/contentassets/1eacb745bb0e4179b7b5afcf8592f682/konjunkturer-digitalisering-og-politikk-ved-knut-e.-sunde.pdf [Accessed 26.05.2017]
86. Sykehusbygg, 2016. *Teknologinotat - konsekvenser for langtidsplanlegging sykehusbygg.* [pdf] Available at: https://sway.com/nxeIzUdtuNCQzLCR [Accessed 05.03.2017].
87. Taleb, N. N., 2007. *The Black Swan – the impact of the highly improbable*. United States: Random House.
88. Telenor, 2017. *Stordata-samfunnet*. [online] Available at: https://www.telenor.no/om/teknologi-norge/stordata-samfunnet.jsp. [Accessed 15 May 2017].
89. The Royal Academy of Engineering, 2012, *Smart infrastructure: the future*, [pdf] Avaliable at: http://www.raeng.org.uk/publications/reports/smart-infrastructure-the-future [Accessed 06.02.2017]
90. Threatalytics, 2016. *Modelling Cyber Security Risk Across the Organization Hierarchy.* [pdf] Available at: http://www.track-assets.com/files/Modelling%20Cyber%20Security%20Risks%20across%20the%20organization%20Mar16.pdf [Accessed 27.05.2017]
91. Tomter, L., Remen, A., C., 2017a. Helse Sør-Øst: Innrømmer at utenlandske IT-arbeidere har hatt tilgang til pasientjournaler - NRK Norge - Oversikt over nyheter fra ulike deler av landet. [ONLINE] Available at: https://www.nrk.no/norge/helse-sor-ost_-innrommer-at-utenlandske-it-arbeidere-har-hatt-tilgang-til-pasientjournaler-1.13478443. [Accessed 12.05.2017].
92. Tomter, L., Remen, A., C., 2017b. *Helseministeren må forklare seg bedre om journalskandalen* [Online] Available at: https://www.nrk.no/norge/helseministeren-ma-forklare-seg-bedre-om-journalskandalen-1.13510305. [Accessed 12.05.2017].
93. Upstream Intelligence, 2017, *Offshore Digital Services Report: IT Challenges and Opportunities for Digital Vendors*¸ [pdf] Available at: http://img03.en25.com/Web/FCBusinessIntelligenceLtd/%7Be061106d-51a9-4144-ba27-65c5a0c96bf6%7D_4788_White_Paper_1.pdf?elqTrackId=56B5119823EBC4C509E374914376CA34&elqaid=15966&elqat=2 [Accessed 08.02.2017]
94. Valmot, O. R., 2016. Nå kommer det femte våpenet mot kreft til Norge. *Teknisk ukeblad* [online] Available at: http://www.tu.no/artikler/na-kommer-det-femte-vapenet-mot-kreft-til-norge/348748. [Accessed 05.03.2017].
95. Veum, E., 2017, *Etterretningssjefen: Landet ligger åpent for cyberangrep*, NRK.no, [online] Avaliable at: https://www.nrk.no/norge/etterretningssjefen_-landet-ligger-apent-for-cyberangrep-1.13360031 [Accessed 19.02.2017]

96. WebWise team, 2012, What are cookies, BBC, [online] Available at: http://www.bbc.co.uk/webwise/guides/about-cookies [Accessed 03.02.17]
97. Zachariassen, E., 2012. Ingen vet når en elektronisk pasientjournal kan være klar. Teknisk Ukeblad. [online] Avaliable at: http://www.tu.no/artikler/ingen-vet-nar-en-elektroniskpasientjournal-kan-vaere-klar/236260 [Accessed 04.03.2017].
98. Zetter, K., Poulsen, K., 2010. *U.S. Intelligence Analyst Arrested in Wikileaks Video Probe* [online] Available at: https://www.wired.com/2010/06/leak/ [Accessed 02.05.2017]

Appendix A – Interview Guide

På Norsk:

Bedriften
Spørsmål
1. Hvilken stilling har du?
2. I hvilken sektor opererer dere i?
3. Hva er forventet omsetning i år?
4. Hvor mange ansatte har dere?
Digitalisering
5. Hvilke typer digital teknologi eller system tar dere i bruk?
6. Hvor avhengige er dere av digitale system i deres drift, og hvor viktig er digitaliseringen i utviklingen av organisasjonens konkurransefordel?
7. Hvilke fordeler drar dere nytte av ved bruk av ny digital teknologi?
Nylige dataangrep
8. Hvor mange cyberangrep har dere vært utsatt for i løpet av de siste 12 månedene, og hvor mange av disse angrepene har medført alvorlige konsekvenser? Er det en økning eller reduksjon i antall sammenlignet med året før?
9. Hvilke typer og metoder er brukt i disse angrepene? Har dere analysert angrepene (root cause analysis)?
10. Hvilke konsekvenser har disse angrepene hatt for organisasjonen? F.eks. økonomiske eller driftsrelatert.
11. Er det en økning i ressursbruk relatert til sikkerhetstiltak (cyber security) etter disse angrepene?
12. Rapporterer dere disse hendelsene til myndighetene og andre bedrifter, hvis så, hvilke fordeler har det for organisasjonen?
Ledelse og Cyber Security
13. Bruker dere standarder (f.eks ISO/IEC 27005: Information Security risk management) som retningslinjer for kvalitet og planlegging i sikkerhetsarbeidet? Hvis så, hvilke?
14. Er ledelsen engasjert i sikkerhetsarbeidet? Hvis så, på hvilken måte er det synlig?
15. Hvilke kortsiktige og langsiktige mål har dere relatert til digital risiko og sikkerhet, og hvordan knytter dere dette opp mot organisasjonens overordnede strategi?
16. Hvordan sikrer at relevant informasjon om trusselbildet og sikkerhetstiltak blir distribuert til og mellom alle nivåer i organisasjonen?
Risikostyring
17. Beskriv hvor ofte og hvor omfattende dere utfører risikoanalyser og vurderinger knyttet til eksterne og interne faktorer, relater til digital risiko og cyber security?
18. På hvilken måte sikrer dere at alle de involverte partene i risiko- og sikkerhetsarbeid har samme oppfatning av risiko og et felles språk?
Bevisstgjøring
19. Hvilke tiltak har dere for å øke bevisstheten om dataangrep og digital risiko i bedriften og med andre bedrifter? Har bevisstheten endres seg de siste fem årene?

20. Hvor stor åpenhet er det i organisasjonen rundt dataangrep og digitale sårbarheter med kunder, leverandører, og evt. presse?

Trusselbildet

21. Hvordan tilegner organisasjonen seg kunnskap om det nåværende data- og cybertrusselbildet?
22. Hvordan har trusselbildet endret seg de siste 3 årene?

Eksponering og sårbarheter

Organisasjon

23. Hvordan påvirker verdikjeden eksponering for digital risiko?
24. I hvilken grad tar organisasjonen høyde for trusler fra insidere, sabotasje og spionasje i risikovurderinger og utvikling av nye systemer? Hvis mulig, hvilke konkrete tiltak er satt i gang?

Menneske

25. Hvordan tar dere hensyn til menneskelige faktorer knyttet til sårbarheter i teknologi og digitaliseringen?

Teknologi

26. Hvordan sikrer dere at bruken av avansert IKT samsvarer med kompetansenivået i organisasjonen?
27. Hvordan kontrollerer dere hvem som får tilgang til systemer, digital infrastruktur (databaser, servere og nettverk) og hvordan sikrer dere at uvedkommende ikke har tilgang?

Beredskap

28. Hvilke forberedende aktiviteter gjennomfører dere med tanke på beredskapsplan og risikoreduserende tiltak?
29. Hvordan sikrer dere kvalitet i sikkerhetsarbeidet?
30. Dersom en uønsket hendelse (dataangrep) er oppdaget i en av deres systemer (tilstandsovervåkning, nettverk, servere, etc.), hvordan foregår varsling, behandling- og gjennomrettingsprosessen?
31. I hvilken grad lærer dere av tidligere hendelser, og hvilken effekt har dette på arbeidet med IKT sikkerhet?

Innovasjon, ytelse og sikkerhet

32. Hvordan går dere frem for å sikre balanse mellom fordelene av digitaliseringen og digital sikkerhet?

Fremtiden

33. Hvilke endringer er det forventet at digitaliseringen kommer med i de neste fem årene, og hvordan påvirker dette trusselbildet og cyber risk management?
34. Hvordan kan en åpen diskusjon om cybersikkerhet og dataangrep i bransjen og på tvers av sektorer virke positivt for deres bedrift og andre norske bedrifter?

In English:

Organization

Questions

1. What position do you have?
2. In which industrial sector do you operate?
3. What is the expected turnover this year?
4. How many employees do you have?

Digitalization

5. What types of digital technology or systems do you use?
6. How dependent are you of digital systems in your operations, and how important is digitization in the development of the organization's competitive advantage?
7. What benefits do you get from using new digital technology?

Recent Cyberattacks

8. How many cyberattacks have you been exposed to in the last 12 months, and how many of these attacks have caused serious consequences? Is there an increase or decrease in number compared with the previous year?
9. What types and methods are used in these attacks? Have you analyzed the root causes?
10. What consequences have these attacks been for the organization? For example, economic or operational consequences.
11. Is there an increase in resource allocation to cyber security after these attacks?
12. Do you report these events to the authorities and other companies, if so, what benefits does it have for the organization?

Management and Cyber Security

13. Do you use standards (for example, ISO / IEC 27005: Information Security Risk Management) as guidelines for quality and planning in the safety work? If so, which?
14. Is the management involved in the security activities? If so, how is it visible?
15. What short-term and long-term goals do you have related to digital risk and security, and how do you link this to the overall strategy of the organization?
16. How does relevant information about cyber threats and security measures distribute to and between all levels of the organization?

Risk Management

17. Describe how often and how comprehensive you conduct risk analyzes and risk assessments related to external and internal factors related to digital risk and cyber security?
18. In what way do you ensure that all involved parties in risk and security activities have the same perception of risk and a common language?

Awareness

19. What measures do you have to raise awareness about cyberattacks and digital risks in the company and with other businesses? Has the organizational awareness changed over the last five years?
20. How much transparency is there in the organization around cyberattacks and digital vulnerabilities with customers, suppliers, and possibly press?

Threat picture

1. How does the organization acquire knowledge about the current cyber threat picture?
2. How has the threat picture changed over the last 3 years?

Exposure and vulnerabilities

Organization

3. How does the value chain affect exposure to digital risk?

4. To what extent does the organization face threats from insiders, sabotage and espionage in risk assessments and the development of new systems? If possible, what specific risk reducing measures have been implemented?

Human

21. How do you consider human factors related to vulnerabilities in technology and digitization?

Technology

22. How do you ensure that the use of advanced ICT matches the level of competence in the organization?

23. How do you control who can access systems, digital infrastructure (databases, servers and networks) and how do you ensure that unauthorized users do not have access?

Emergency Preparedness

24. What preparatory activities do you take in terms of contingency plan and risk mitigation measures?

25. How do you ensure quality in the security activities?

26. If an unwanted event (cyberattack) is detected in one of your systems, how is the notification, incident and response process?

27. To what extent do you learn from past events and what effect does this have on ICT security?

Innovation, performance and security

28. How are you going to ensure a balance between the benefits of digitization and digital security?

Future

29. What changes are expected by digitalization the next five years, and how does this affect the cyber risk picture?

30. How can an open discussion about cyber security and cyberattacks in the industry and across industrial sectors be beneficial to your business and other Norwegian businesses?