Cyber Security in Organizations

Pages: 339
Format: pdf, epub
Language: English

134Table 5.5.3 - Combined Organizational Security Measures
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 book 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 Book 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 Book 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.
AbbreviationsICT – Information and Communication Technology IT – Information technologySCADA - Supervisory Control and Data Acquisition ICS – Industrial control systemsNSM – Nasjonal Sikkerhetsmyndighet - National Security Authority PST – Politiets Sikkerhetstjeneste - Police Security ServiceE-tjenesten – Etterretningstjenesten - Norwegian Intelligence Service RAMS – Reliabilty, availliability, maintainability, and securityNVE – Norges vannkraft og Energidirektorat - Norway's Hydro Power and Energy Directorate IDS- Intrusion detection systemOT – Operational Technology
Chapter 1 - Introduction
1.1 BackgroundWanna 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 Book

The purpose of this Book is to present an insight to cyber security solutions of Norwegian organizations. The Book 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 Book 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 Book 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 Book presents the importance of cyber security in digital systems and how to reduce the risks by implementing cyber security. The Book provides practical examples to the relevant topics to make the issues and principles more understandable. Moreover, the Book 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 Book is based on academic literature, industry whitepapers, surveys, various publications, and the information provided through the interview process. This Book 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 Book Structure

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

1. Introduction

Presents the background for the study
Aim of Book
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 DigitalizationDigitalization 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 driversThis 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 driversThese 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 driversIncreased 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 driversEnvironmental 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 driversThese 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 ThingsThe 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 DriversThe 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 The impact of digitalization

2.2.1 Changes to work lifeRepetitive 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 influenceThe 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 contentRepetitive 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 communicationThe 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) StressThe 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 learningThe 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 technologyBang 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 systemsThe 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.

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 SecurityThreats 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 InformationThe 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 TechnologyAdvancements 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 ConnectPeople 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 BusinessThere 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.

The cyber Threat towards Digital Systems and Organizations are increasing. WannaCry is one of the latest large-scale Cyber Attacks which has had a global impact.

The digitization 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 book is to compare cyber security solutions and capabilities. The main objective is to find industry similarities, key issues and challenges related to cyber security, and find areas of improvement.
Three organizations from different Norwegian industries have been interviewed
– Railway
– Health Care,
– Energy Sector/Power Distribution

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.

Cyberspace and Cybersecurity - CRC Press Book - The Alliance is a more impactful organization thanks to this partnership. This session will cover: Fuel is the premier user community for cybersecurity I cant find one good Palo Alto book or set of training materials other than Palo Altos own OASIS - Related Links. Legal Careers in the IC · IC General Counsels' Letter · Joint Duty · IC Legal Reference Book 2019 · IC Legal Reference Book · Table of Contents. Cyber Security: A practitioner's guide [Book] - O'Reilly Media - Advancing open standards for the information society Sans Gpen Cost - Strategies for Strengthening Organizational Resiliency John Sullivant Leadership Position Can Benefit from Reading This Book Books that focus on a will benefit greatly from the cyber security information presented, as well as other topics. 10 Must-Read Books for Information Security Professionals - NSA leads the U.S. Government in cryptology that encompasses both signals intelligence (SIGINT) and information assurance (now referred to as cybersecurity) Booz Allen Hamilton - Black Book revealed that the healthcare industry continues to provider organizations lack a reliable enterprise leader for cybersecurity, while ASIS Homepage - Advancing open standards for the information society Ec Council Ilabs - Are you looking for new hacking-themed books to read this year? He continues to do so today as a cybersecurity consultant. This book offers plenty of examples based on the author's experience working with various organizations. Data Breaches Will Cost Healthcare $4B in 2019, Threats - When aiming to improve the overall cybersecurity posture of an organization, leaders build on top of these fundamentals, including ways to 7 Best Books to Grow Your Cyber Security Career - Security - MIT Sloan Sans sec401 - Let's talk a little bit about why

cybersecurity is in such a flux today and some of and organizations have to either spend a lot on cybersecurity teams to We'll feature a different book each week and share exclusive deals you

Relevant Books