An assessment of cyber security awareness and measures in the Norwegian maritime sector: A focus on shipping companies and equipment suppliers

Martin Nordrum Brattås

Buskerud and Vestfold University College

May 2015

Master of science
Maritime management technical specialization

Author notes

This master thesis is written within the Maritime Management master program at Vestfold and Buskerud University College spring semester 2015. The thesis comprises 30 ECTS credits. Supervisors of the thesis are Kjell Ivar Øvergård, Christian Hovden, and Thomas Nordli.

Abstract

This thesis sets out to assess cyber security awareness and measures in the Norwegian maritime sector. To be able to evaluate the conditions regarding cyber security in the Norwegian maritime sector, a self-evaluation questionnaire was sent out to shipping companies and ship`s equipment suppliers with connections to Norway. The respondents were asked to rate their attitude towards a range of different statements regarding cyber security. Cyber attacks were reported in the survey targeting both physical and information assets from external and internal sources. An exploratory factor analysis revealed three factors, of which one of them showed significant differences on cyber security awareness between shipping companies and equipment suppliers. A repeated measures general linear model analysis revealed differences between shipping companies and equipment suppliers on their measures taken towards external threats directed at physical assets, and that informational assets receive a higher focus than physical assets.

Some theory is provided to give the reader a basic knowledge about cyber security, the maritime sector, and its stakeholders.

Keywords: Cyber security, Cybersecurity, Information security, maritime sector, Norway

Acknowledgements

My personal motivation to write this thesis came after a walk around campus looking for ideas on a subject that could be formulated into an interesting assignment. Criteria's set for the assignment included that it had to be part of my scholar background as an electronics engineer, and that it was relevant for my current master program within maritime management. I got in contact with Christian Hovden at the electro automation department who presented to me a report by The European Network and Information Security Agency (ENISA). The report stated that cyber security awareness in the maritime sector in Europe was low to non-existent. As the possibility to write a thesis on the subject satisfied my criteria and appealed to me, Hovden introduced me to his coworker Thomas Nordli who has great knowledge about computer programming. I then formed my plan for the master thesis and got assigned Hovden and Nordli as supervisors, together with the bright professor Kjell Øvergård as main supervisor. Thank you very much for your ideas, discussions, corrections, and motivation.

I want to thank Maritime Dept. Federation of Norwegian Industries (Maritime Bransjeforening) and the director Lars Gørvell-Dahll for constructive conversations and cooperation with survey distribution to their members. I would also like to thank individuals in the Norwegian shipowners association for discussions and inputs. To every single respondent participating in the survey, tank you very much for your contribution!

I thank my mother Kirstin, father Bjørn Øyvind, and brother Øyvind for the unconditional love, support and encouragement throughout the years. I would also like to thank my fiancée Idunn for her positive look on life, and for giving me confidence in my work and myself. Finally, I want to thank my soon to be born son for giving me inspiration and joy to finish the thesis in time before his birth.

Table of contents

Introduction

The European Network and Information Security Agency (ENISA) did in November 2011 issue a report on cyber security in the EU maritime sector. The report with the title “Analysis of cyber security aspects in the maritime sector” highlighted that the maritime sector is lacking awareness on cyber security, and at the same time the maritime sector is getting more dependent on ICT to optimize operations. The report explains that maritime transportation for cargo and passengers is of crucial importance to the EU, and that the maritime sector is considered a part of the European critical infrastructure (ENISA, 2011).

The ENISA report illustrates the criticality of the maritime sector by referring to that of the goods traffic in Europe 2010, 52% was carried by water, an increase of about 7% over a period of 10 years. The report also states that more than 43% of internal trade within EU, and around 90% of external trade to and from EU is carried by water. Several major seaports are located at EU shores, and together they handle a large percentage of the container traffic to and from Europe. 3-5% of EU`s GDP is generated by industries and services related to the maritime sector (ENISA, 2011).

Norway has traditionally been, and is still considered a large shipping nation. The Norwegian fleet is one of the largest and most advanced in the world, and together with a global leading maritime industry, Norway has established a complete and world leading maritime cluster (Norwegian Shipowners’ Association, 2013). Of the 500 million tonnes of goods transported to, from, and within Norway in 2013, 83% were carried by sea. Of the inland transportation with a share of 300 million tonnes, 53% were transported by water. The Norwegian external trade is dominated by sea transport. It is also suggested by the Norwegian agencies that seaborne transport and related new technology should be prioritized in the future to ensure efficient and eco friendly transportation of goods (Transportetatene, Avinor, Jernbaneverket, Kystverket, & Statens vegvesen, 2015).

The Norwegian maritime industry employs about 100 000 people and creates value of about 150-160 billion NOK per annum. Of this, half of the value creation results from shipping activities alone (Jakobsen, Mellbye, & Holmen, 2014; Norwegian Shipowners' Association, 2013). The GDP generated by the Norwegian maritime industry accounts for almost 6% of Norway's total gross domestic product, and the Norwegian controlled merchant fleet constitutes about 5% of the world`s fleet total (Smart Comp, 2013).

The maritime sector`s importance to Norway. A look at the figures presented in the previous section indicates similarities between the criticality of the maritime sector to EU to the conditions of the Norwegian sector. As the Norwegian maritime sector constitutes a higher percentage of total GDP, and a similar percentage of goods transport carried by maritime transportation compared with EU figures, this dependency and hence the importance of the maritime sector can be argued to be at least as important to Norway as it is to EU. The maritime sector could therefore be considered critical to Norway's economy, as well as the supply of goods performed by maritime transportation is critical to the Norwegian society. Based on the Norwegian Ministries (2012a) definition of critical infrastructure that includes supply of goods, the maritime transportation could also be regarded as a critical infrastructure.

The importance of cyber security to the maritime sector. The information exchange in the maritime sector is frequent and often contains valuable and detailed information sent over the Internet. Ships are equipped with control systems and navigational systems that have known vulnerabilities to cyber attacks (CyberKeel, 2014). Norwegian ship`s equipment suppliers delivers automated equipment to Norwegian ships (Mellbye & Jakobsen, 2014). An attack on the maritime sector could potentially threaten the Norwegian economy, and hinder maritime transportation of goods and passengers as it could in EU (ENISA, 2011). Cyber security to protect information and physical assets is therefore important to the maritime sector.

Aim and research questions

This thesis sets out to assess the awareness of cyber security and measures in the Norwegian maritime sector. Since the maritime sector in Norway is spanning a wide area with many diverse actors, some limitations in the choice of the population of interest had to be taken. The ship`s equipment suppliers and shipping companies have therefore been given a special focus in this thesis.

Since knowledge about cyber security can help raise awareness about cyber security, there is a hope that this thesis can enlighten the reader and in that way create an interest and awareness of the topic. A desired goal is that the thesis could be beneficial for stakeholders in the maritime sector and to learning institutions.

Overall aim. The overall aim of this thesis is to assess cyber security awareness and measures in the maritime sector in Norway with a special focus on ship owners and equipment suppliers.

Research questions. The research questions for this thesis are:

- Have they been subjected to cyber attacks?
- Are the Norwegian maritime equipment suppliers and ship owners aware of cyber security related issues?
- Do they take precautions in order to deal with cyber threats?
- Are there any differences in how they relate to physical and information aspects of cyber security?

- Are there any differences between the cyber security measures between ship owners and equipment suppliers?

Theory

This part of the thesis sets out to provide the reader with knowledge about cyber security, the Norwegian maritime sector, cyber security concern, organizational and technical features, and influencing factors. The reason behind the provided theory is to provide the reader with an understanding of the different concepts in this thesis, which could be helpful in order to better understand the thesis research questions, discussion, and conclusion.

Definitions

Maritime sector. The terms *maritime sector and maritime industry/industries* are used ambiguously in literature and in this thesis. The definitions of the maritime industry, industries, and maritime sector are quite similar, although maritime industries seem to be the more preferred term used in economic and statistical literature. The maritime sector/industry can be divided into 4 main sectors or groups: Shipping companies including shortsea, deepsea, offshore, and drilling and production (rigs); Ship`s equipment including mechanical, electrical and electronic, design, trade, and other operating equipment; Yards including new builds, maintenance, repairs, and modifications; Maritime services including financial and juridical, technological (engineering, design, classification etc.), ports and logistics, and trade (wholesale, brokers etc.) (Mellbye & Jakobsen, 2014; Rederi-skatteutvalget, 2006; Reve & Sasson, 2012).

Use of the word “cyber security”. The spelling of the topic varies within news sources, books, and in scientific papers, where the words cybersecurity, cyber security, and cyber-security are used interchangeably. Search results in databases containing scientific publications, and from popular Internet search engines produce different results with similar content when using the different spellings. This is pointed out by Brumfield (2013), and the author of this thesis verifies these results. Despite that cybersecurity, cyber security, and cyber-security differ grammatically and provides different search results, they are the same word with different spellings, and are probably written differently based on geographical location, and other influences on the writer (Brumfield, 2013). For this paper, the phrase *cyber security* will be used consistently unless direct citations require the word spelled differently. The reason for the chosen way of spelling is the report made by ENISA (2011), and Norwegian Ministries (2012a), which use the phrase cyber security in their writings about the topic. Others, such as the ISO/IEC has grasped the word cybersecurity (ISO/IEC, 2012).

Safety vs. security. It can be useful to have in mind some general differences between safety and security when dealing with the concept of cyber security. The terms safety and security can be confusing at times, especially in a country as Norway, where the polysemous word “Sikkerhet” is referring to both safety and security and thus has to be interpreted from context (Albrechtsen, 2003). The following definitions of safety and security are taken from the Oxford online dictionaries.

- Safety is defined as a mass noun as “*The condition of being protected from or unlikely to cause danger, risk, or injury*” (Oxford Dictionaries, n.d.-d) , and as modifier “*Denoting something designed to prevent injury or damage*” (Oxford Dictionaries, n.d.-d).
- Security as a mass noun is defined as “*The state of being free from danger or threat*” (Oxford Dictionaries, n.d.-f), and as modifier “*The safety of a state or organization against criminal activity such as terrorism, theft, or espionage*”, “*Procedures followed or measures taken to ensure the security of a state or organization”, and “The state of feeling safe, stable, and free from fear or anxiety*” (Oxford Dictionaries, n.d.-f).

From the Oxford definitions, it can be hard to spot significant differences, I will therefore try to sort them out. Safety and security, although different, have similarities and they can be complimentary. It is implied that a safety breach can result in difficulties remaining a desirable level of security, while a breach in security can result in failure to ensure safety (Bartnes, Nordland, Rostad, & Tondel, 2006). The focus of security lies primarily on intentional, malicious acts or events with relations to threats and incidents, while safety concerns mostly those which are unintended with origin from hazards and failures (Bartnes et al., 2006). A threat can be seen as a "*potential cause of an unwanted incident, which may result in harm to a system, individual or organization*" (ISO/IEC, 2012, p. 7). Even though safety is mostly connected to unintentional events, a violation could pose a threat to both security and safety. Violations are considered intended, they are however not malicious or carried out to harm or destroy, but rather to reduce efforts, time spent, evaluating own solutions as better than existing procedures etc. (Reason, 1995).

The concept of security concerns threats that originate from a human source. Security threats can further be divided into those originating outside of, and those that originate inside an organization. Threats related to security are most often motivated by the will of an individual or a group, with a goal to profit or inflict harm (e.g. the acts are intended or willed). However, a security threat can also arise from human actions that has unintentionally has led to a vulnerability for an organization (Albrechtsen, 2003).

Albrechtsen (2003) also argues that intended malicious acts (*e.g.* threats) are more unpredictable than unintended errors (*e.g.* hazards originating from human or technical errors), as threats are not likely to be "… *observable, tangible, and proximate*" (Albrechtsen, 2003, p. 7). Another addition to security is that there has to be an adversary (*e.g.* Threat agent, a person with an intention of performing a malicious act) present in order for a malfunction to be a matter of security. Without an adversary, a deviation from expected behavior would then have to be caused by some form of error or accident (Singer & Friedman, 2014).

Cyber Security.

Definitions concerning cyber security and accompanying terms in this thesis are mostly retrieved from International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). More specifically the ISO/IEC 27000:2014 (ISO/IEC, 2014) is used for general definitions, while IOC/IEC 27032:2012 (ISO/IEC, 2012) is used for definitions directly related to cyber security. When more explanation of terms is deemed necessary, other definitions are included to clarify or discuss a topic.

To give an explanation of the concept of cyber security, it can be useful to start with the concept of information security. Information security is defined by ISO/IEC as the "*preservation of confidentiality, integrity and availability of information."* (ISO/IEC, 2014, p. 4). In a note to the definition, ISO/IEC also add "*authenticity, accountability, non-repudiation, and reliability…*" (ISO/IEC, 2014, p. 4) to the list of properties that may be involved with the concept. The way information is stored varies from digital storage, material writings, or in the form where people are in possession of knowledge. The way information is transmitted can for example be in a conversation, electronically, or by postal services (ISO/IEC, 2014). The CIA triad shown in figure 1 has previously been used to illustrate how to ensure the security of information. The message within the triad is also valid to many aspects of cyber security (Von Solms & Van Niekerk, 2013).

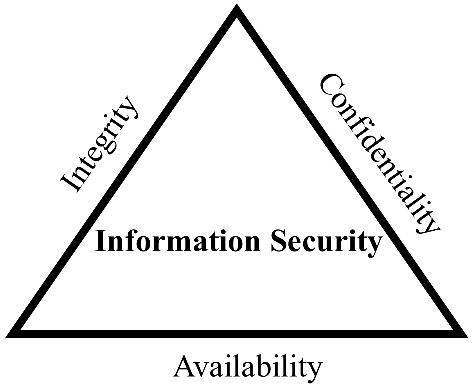


Figure 1. CIA triad/triangle, also known as the AIC triad. Adapted from (Harris, 2012, pp. 22-23)

The property of *confidentiality* is understood by that information is kept unavailable from unauthorized people, entities, or processes. *Integrity* is a property with relevance to the accuracy and completeness of something. *Availability* refers to how accessible and usable something is when an authorized entity tries to access and/or use it (ISO/IEC, 2014).

ISO/IEC defines cyber security in the same way as they define information security. The difference is that information within the concept of cyber security is with respect to information accessible through the cyberspace. It is therefore implied that information and the protection of information is a part of the concept cyber security. The standard lists a range of assets within the concept of cyber security, including information, software, physical, people, and even intangibles like reputation. In a note about the various types of assets in the cyberspace, ISO/IEC states that for simplicity, assets are often only seen as information or resources (ISO/IEC, 2012, p. 15). Cyberspace is a term originating from the short stories and novels written by the science fiction author William Gibson in the early 1980`s (Singer & Friedman, 2014). The cyberspace is defined by ISO as "*…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*" (ISO/IEC, 2012, p. 4). Despite that the cyberspace does not exist in any physical form, it is dependent on physical means to be able to store and transmit the digital data that the cyberspace is made out of. ICT encompasses the technology and equipment used for digital transfer and digital storage of data, and ICT security is thus the protection of these technologies (Von Solms & Van Niekerk, 2013).

According to Von Solms and Van Niekerk (2013), there is a variety of different information sources that interchangeably use the concepts of information security and cyber security. They argue that the concepts, although overlapping, have key distinctions that need to be taken into account. One difference lies in how the human role in a cyber security perspective have an additional dimension compared to information security, where in cyber security humans can be both targets of, and contributors to a cyber attack unaware of their participation (Von Solms & Van Niekerk, 2013). What also is worth noting is that Von Solms and Van Niekerk (2013) points out the possibility of a cyber security attack to cause direct harm or affect humans including their personal capacity and to society, while a breach in information security could only indirectly lead to the same. The term direct harm I believe would have to be seen from a different point of view compared to direct physical harm. A cyber attack would always be utilized with some form of digital means, and a cyber attack targeted at humans or society would therefore always be the result of an incident that initially took place in a digital context (Singer & Friedman, 2014).

The assets one wants to secure may also differ between information security and cyber security, as the assets within the concept of cyber security may include non-information assets in addition to information assets. They point out that their view of broader boundaries within the concept of cyber security compared to information security is in coherence with the ISO 27032 standard (Von Solms & Van Niekerk, 2013). Solms and Niekerk refers to those non-information assets with examples such as cyber bullying that can cause direct harm to a person, home automation appliances with applications connected to web based management systems, digital media piracy leading to a negative impact on the value system, and cyber terrorism that could set the wellbeing of society as a whole at risk (Von Solms & Van Niekerk, 2013). An illustration of the relationship between information-, ICT-, and cyber security is shown in figure 2.

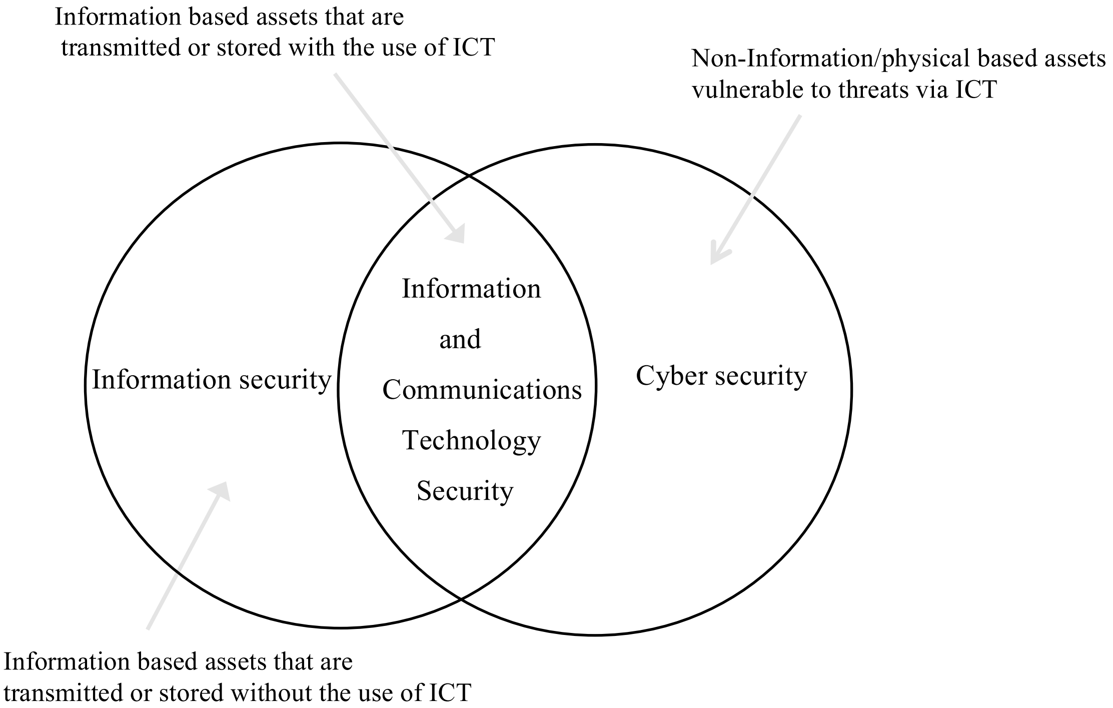

Information based assets that are transmitted or stored with the use of ICT
Non-Information/physical based assets vulnerable to threats via ICT
Information security
Information and Communications Technology Security
Cyber security
Information based assets that are transmitted or stored without the use of ICT

Figure 2. Relationship between information-, ICT-, and cyber security. Adapted from figure 4 (Von Solms & Van Niekerk, 2013, p. 101).

Threat agents. The objectives of a cyber attack is to cause loss of integrity, availability, confidentiality, or physical destruction. A cyber attack could then result in destruction, exposure, modification, disabling, theft, malfunctions, disclosure, physical harm, unauthorized access, or use of an asset (Gori, 2009; ISO/IEC, 2012).

Threat agents or *threat actors* are groups or individuals that take part of, performs, or that supports a cyber attack (ISO/IEC, 2012). Threat agents includes groups or individuals like "*…disgruntled employees, criminals, hackers, nation- states, and terrorists*." (U.S. Coast Guard, 2014, p. 46). In order to assess vulnerabilities and risks in an organization, understanding threat agent's motives, their capabilities, and intentions as shown in table 1 are considered important knowledge in order to identify vulnerabilities and to perform risk assessment (ISO/IEC, 2012).

Table 1

Threat agent`s motivation, capabilities, and intentions (ISO/IEC, 2012, p. 17).

Motivation	Capabilities	Intentions
Religious	Knowledge	Fun
Political	Funding	Crime
Economic	Size	Espionage

There are numerous ways of which a threat agent can perform a cyber attack directed against an organization`s information and physical assets. An attack can be initiated towards an organization`s assets from inside of (internal), or from outside (external) an organizations local networks. A combination of the two is also a possibility. If the attack is initiated from within the organizations network, the threat agent is likely an employee (insider), or someone who has gained unauthorized access to the company`s local networks. An attack from outside the local networks (e.g. through the internet) can be directed towards the organizations publicly facing systems, or assets located in the local network (ISO/IEC, 2012).

Ship cyber vulnerability

Industrial control systems. The vulnerability of a vessel to a cyber attack is amongst other things related to the many industrial control systems (ICS) located onboard a ship. These ICS are an important part of many commercial ships as they perform essential functions including "…manage propulsion, support navigation and communications, provide fire protection, operate safety systems, and manage cargo loading and discharge." (Wallischeck, 2013, p. 10). Actually there could be several hundred ICS found onboard a ship performing different processes as illustrated in figure 3.

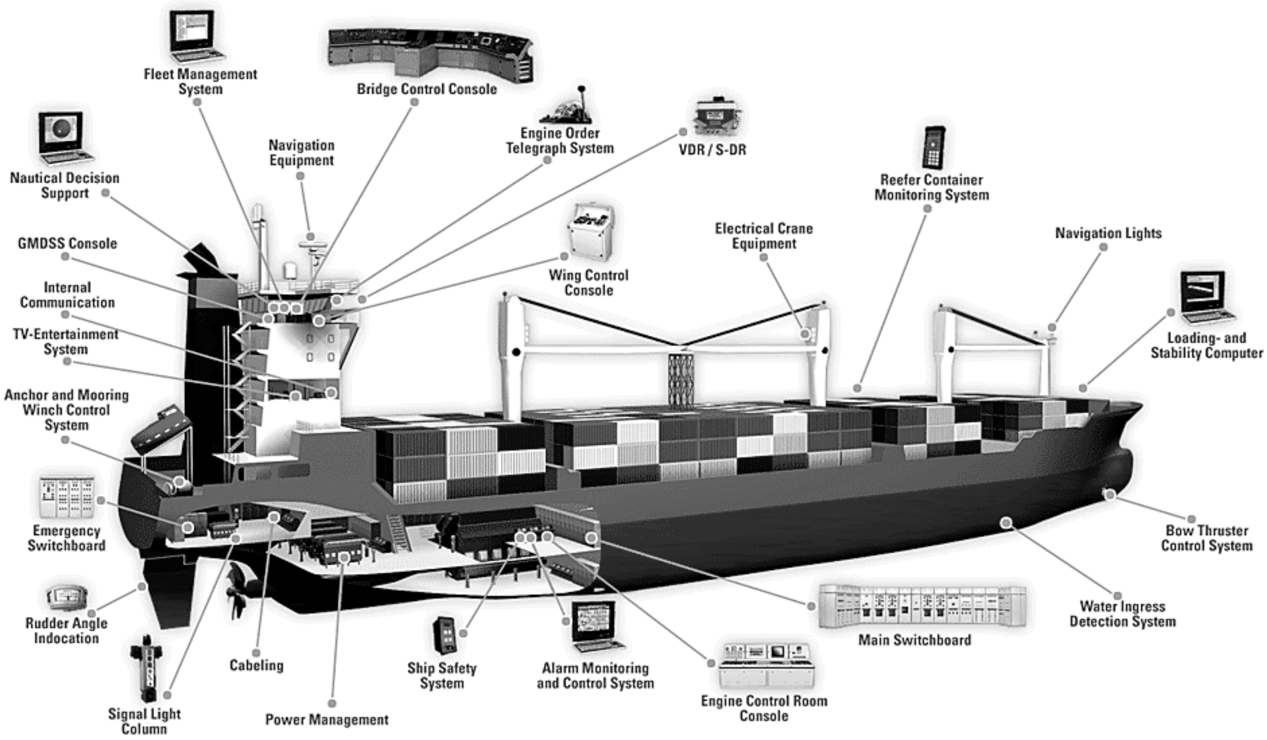

Fleet Management System
Bridge Control Console
Navigation Equipment
Engine Order Telegraph System
VDR / S-DR
Nautical Decision Support
Reefer Container Monitoring System
Electrical Crane Equipment
Navigation Lights
GMDSS Console
Wing Control Console
Internal Communication
TV-Entertainment System
Loading- and Stability Computer
Anchor and Mooring Winch Control System
Emergency Switchboard
Bow Thruster Control System
Water Ingress Detection System
Main Switchboard
Rudder Angle Indocation
Cabeling
Ship Safety System
Alarm Monitoring and Control System
Engine Control Room Console
Signal Light Column
Power Management

Figure 3. "*Typical Shipboard Industrial Control Systems*" (Wallischeck, 2013, p. 10). Credentials: www.interschalt.de/. Ownership of the U.S. Government. Reprinted with permission from Volpe, The National Transportation Systems Center. U.S. Department of Transportation.

The confidentiality, integrity, and availability of these ICS are an important part of ensuring a ship`s cyber security. In contrast to information security where confidentiality is seen as the most important part of security component, availability is regarded the most important security component in ICS. The reason for this is that ICS often are part of continuous and essential processes, and loss of availability of such a system could therefore be critical even for short periods of time (Stouffer, Falco, & Scarfone, 2011).

ICS are often designed with a belief that they are separated from other network systems and thereby inaccessible to threat agents. In reality, many control systems are connected to networks that can provide remote accessibility from within local (LAN), or remote network locations (internet) (Marine Cybernetics, n.d.). The belief that the ICS are separated from other systems may originate from a time when ICS mostly were custom based designs, often using specialized hardware and software. The ICS has changed as cheaper and more standardized systems have become widely available, and now the ICS mostly contains commercial off the shelf standardized hardware and software, Ethernet, and Internet Protocol (IP). More standardized ICS with remote connectivity provides great opportunities for different companies, as it is enable remotely access for diagnostics, maintenance, and monitoring. The downside is that the availability of the systems makes them vulnerable to cyber incidents as they are becoming more like IT systems. In addition to external cyber threats to the system as a result of remote accessibility, there is also a possibility of unauthorized access to an ICS via for example removable media devices, LAN, and local wireless connections. As the ICS are used to control physical assets, there is a risk in that they could have a direct damaging affect on the surroundings including humans, property, or the environment if exposed to a cyber attack (Stouffer et al., 2011; Wallischeck, 2013).

The term ICS encompasses *"…supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and…Programmable Logic Controllers (PLC)…*" (Stouffer et al., 2011, pp. 2-1).

The main goal of ICS is to manipulate a controlled process by the use of actuators (valves, breakers, switches, motors etc.) that receives commands from a controller (PLC etc.), which receives information from sensors that measure physical properties of the process. A set point is programmed in the controller and is used to calculate a new signal that is sent to an actuator. Information from the process can then be sent to human machine interface (HMI) that provides a graphical interface for an operator to receive information about-, and make adjustments to the process (Stouffer et al., 2011, pp. 2-3).

SCADA systems are typically used onboard ships (CyberKeel, 2014), and provides a way to gather information about, and to control dispersed assets from remote locations. Remote connections via satellite from ICS enables connections to shipping operators (Radan, n.d.), while equipment suppliers are using remote connections to "*monitor, service and upgrade software components on the vessels*."(CyberKeel, 2014, p. 14)

Navigational equipment. Many vessels today navigate with the help of technological aids including GPS (Global Positioning System), ECDIS (Electronic Chart Display and Information System), and AIS (Automatic Identification System). GPS receivers are identified to be vulnerable to attacks that could block or spoof the GPS and could result in a loss of availability in that the signals are lost, or a loss of integrity as data can be manipulated to show wrong time and location (Wallischeck, 2013). ECDIS systems have been proven to be penetrable from both internal and external sources, and access could give an attacker the ability to affect availability, integrity, and confidentiality of data on the system. ECDIS systems can be connected to the Internet for chart downloads, and as it also is connected to the internal network on the ship to receive data from sensors, an attacker could potentially get access to other onboard assets. AIS have been demonstrated to be vulnerable for a number of different threats involving integrity of the information. AIS signals can be manipulated to show false information about the ship to the vessels crew, as well as to stakeholders with a legitimate interest in details concerning the ship (CyberKeel, 2014).

Reported cyber incidents

This section tries to give an overview of different cyber incidents that potentially could be connected with risks in the Norwegian maritime sector regarding physical and information assets.

For general cyber incidents in Norway, the Norwegian National Security Authority (NSM) did in 2014 manually handle 5069 cyber incidents of which 88 were considered severe, in 2013 they manually handled 3400 with 51 severe incidents, and 2012 they handled 2332 with 46 severe incidents. The majority of these incidents relates to cyber espionage directed towards private and public organizations. The figures are indicating that there is an increase in the number of cyber incidents amongst Norwegian organizations (NSM, 2015).

The dark figures for cyber related incidents are probably many times higher than figures presented by NSM. A report looking at dark figures for unreported cyber incidents from Norwegian organizations discovered a large gap between actual and reported cyber incidents. By collecting data from various sources including automated reporting sensors, it is estimated that around 50% of large companies (>100 employees) was subjected to some form of cyber attack in 2013. Without data from other sources, a survey was conducted on the same population. Of the respondents in the survey only 5% reported that they had reported a cyber incident in relations to hacking. There are however a large uncertainty about the findings in the report (NSR, 2014).

To the authors knowledge there are not many reported cyber security incidents with relations to the Norwegian maritime sector available to the public. There are however one incident that has received the medias attention. The incident happened at Ulstein Group in spring of 2014. The Ulstein Group`s is a parent group of companies involved in amongst other things maritime design and solutions, shipbuilding, power and control, property, ship ownership and investments (Ulstein Group, 2013). The company is considered innovative with own development and large international activity. Unknown unauthorized actors gained access to their computer systems and managed to maintain access to their information assets over a period of at least one week. At the release of the cited article the company did not know what kind of information that was retrieved by the perpetrators (Ruset, 2014). The files were allegedly encrypted before they were retrieved from the company's systems, making them hard to identify (NSM, 2015). The attack on Ulstein group happened despite of what is described by a company representative as very good security systems (Ruset, 2014). The company chose to have an open dialogue about the incident based on the idea that communication with other companies is an important part of security work. The incident was identified due to abnormal network traffic and resolved with the help of governmental authorities (Ervik & Hansen, 2014).

Vulnerabilities in Norwegian water supply infrastructure were identified by NSM in 2014. An attack that exploited this vulnerability could potentially lead to a stop in water supply. The oil and energy sector was in 2014 prone to a cyber attack involving over 50 companies. The targeted and coordinated attack was conducted with emails containing malicious attachments, and is considered the largest cyber attack ever directed against Norwegian ICT infrastructure (NSM, 2015).

Equipment made by a company that has been infected with some form of malware could potentially create a risk for the customer of that product. An example of such an attack is found in a case where barcode scanners were delivered pre infected to a company. The malware was found in purchased bar code scanners that created a backdoor for criminals into their networks. This kinds of attacks point out the importance of evaluating hardware suppliers (CyberKeel, 2014).

Two incidents are infamous for causing physical damage. The Stuxnet worm caused the most famous incident where physical damage has been reported. Kaspersky Lab discovered Stuxnet in 2010. By examining the code, Kaspersky and other security firms discovered a highly sophisticated malicious code programmed to attack the Iranian nuclear power program. More precisely, Siemens Microsoft based software used to program industrial control systems that operated the Iranian centrifuges were targeted. The PLC`s used to monitor and control sensors and actuators were compromised, and the speed of the centrifuges could then be set to self-destruct. Stuxnet initially infects a system with malicious code placed on a USB stick. After a computer has been infected, the worm spreads undetected into the system while checking if other computers are part of the correct Siemens ICS. When finding a match it tries to update itself before it gathers information about system operations, before the information is subsequently applied to attack the centrifuges. If the worm does not find the correct ICS system it will not perform any malicious actions. The complexity of the code together with information leaks indicates that United States and Israeli governments developed Stuxnet. Since the discovery of Stuxnet it has spread outside its intended area of use, rediscovered in networks at private companies, and widely available for malicious actors to use parts of the code in developing their own (Kushner, 2013).

An unnamed German steel mill was subjected to an advanced persistent threat attack on their internal systems and industrial components. The date of the event is not revealed in the document. The attack infiltrated the steel mills systems through spear phishing emails disguised as from a trusted source that together with social engineering first stuck their office network, and then found its way into their production networks. The damages from the attack were massive as control components or entire installations broke down, resulting in the uncontrolled shut down of a blast furnace (Federal Office for Information Security, 2014).

Like the examples of Stuxnet, the German steel mill, and the vulnerability of the Norwegian water supply infrastructure, equipment and control systems installed on vessels may also have vulnerabilities that could lead to physical damage. The hypothetical scenarios including a cyber attack on a ship`s systems or equipment can result in disasters for people, organizations, and the environment.

Stakeholders in the Norwegian maritime sector.

To assess the awareness of the maritime sector, two groups were identified as vital to the maritime sector, and to cyber security. The groups were chosen because of the large and important maritime fleet owned by shipping companies that has a connection to Norway, and that the maritime equipment supplier industry in Norway is world leading. The author assess these two groups as important to ensure cyber security on a vessel, and their importance in the Norwegian maritime sector is high as they together account for about 76% of the total value creation in the maritime sector in 2012 (Jakobsen et al., 2014).

Shipping companies description. The ownership, operation, and management of ships can be organized in a variety of different arrangements. Shipowners are as the name indicates fully or partially owners of one or more ships/vessels and are making the final decisions concerning the ship. The term shipowners is also interchangeably used to describe a ship owning company, also known as a shipping company. The shipping companies range from single owners to large organizations, with different structures in both organization and in decision-making (Branch, 2007; Stopford, 2009)

Vessels can be registered independently from the ship owning company`s location or nationality. Often the vessels are registered in tax favorable states called flags of convenience, commonly by one–ship companies with a sole purpose of owning an individual vessel. A holding company can have the role as shareholder in the one-ship companies, with the previously mentioned ship owner or shipping company as the beneficial owner of the holding company. In this way, a ship owner or shipping company may have several ships registered in different nations around the world while the company has its headquarter in e.g. Norway. The jurisdiction of the flag under which the ship is registered applies, and the international maritime conventions, codes, and recommendations provided by International Maritime Organization (IMO) serve as general standards (Stopford, 2009).

A ship operator needs not to be the owner of his controlled fleet. Often vessels are chartered from a ship owner or investor to a charterer. Through different charter agreements (charter-parties) the charterer to varying degrees operates and provides management of the vessels. Charter agreements are normally accomplished with the help of shipbrokers and standardized charter-parties (Stopford, 2009). In a bare boat charter (demise charter), the charterer takes over the responsibilities associated with the vessel and can then be regarded as the disponent owner A shipping company may provide day-to-day management of ships in-house, or partially or fully outsource the task to dedicated management companies (Branch, 2007).

Equipment supplier’s description. In a report by Menon Business Economics made on the behalf of the Maritime Dept. Federation of Norwegian Industries, figures for the Norwegian equipment suppliers were presented. The figures were categorized by different main and subgroup, and as the maritime equipment suppliers often provides equipment to other sectors besides the maritime, figures were calculated by only including the maritime part of the companies operation (Mellbye & Jakobsen, 2014).

As the focus in this thesis lies primarily on equipment suppliers that deliver equipment to ships/vessels, the groups of companies that deliver equipment made for rigs (drilling equipment), and equipment for the fishing fleet and fish farming (marine equipment) is seen as less important. The third group of the maritime equipment suppliers are the ship`s equipment suppliers (i.e. the companies that deliver equipment to ships/vessels) and includes the subgroups: mechanical equipment, electrical and electronic equipment, ship equipment design, trade, and other operating equipment. The subgroups that are of interest in this thesis are *mechanical equipment*, *electrical and electronic equipment,* and *ship equipment design* companies. Together the three subgroups account for approximately 67% of the 63.3 billion NOK ship`s equipment suppliers total turnover, and employs 13750 out of the total 19284 that are employed in the Ship`s equipment suppliers group (Mellbye & Jakobsen, 2014).

The ship equipment suppliers have a large share of exports with about 90% of their total turnover (if trading companies are excluded to avoid duplicated figures), or around 8% of Norway's total Exports. The high export percentage includes equipment sold to Norwegian shipping companies that operate in foreign countries, equipment sold via Norwegian yards to foreign companies, and direct sales. If one only looks at the equipment that ends up at Norwegian shipping companies regardless of their operations location, almost 30% of the equipment ends up at Norwegian shipping companies (Mellbye & Jakobsen, 2014, p. 19).

Connected stakeholders. In addition to the shipping companies and equipment suppliers that are the main focus of this thesis, several other stakeholders may have a direct or indirect role to ensure a level of cyber security in the Norwegian maritime sector. Two of the stakeholders are described in the subsequent section.

Insurance. Insurance has been an important player for shipping companies for ages, and offers a way to transfer risk. Cyberinsurance is a field of great expansion and development, it is also getting noticed in the maritime sector.

There are several risks that could lead to substantial monetary loss, including damages to reputation, business interruption, and theft of valuable information assets. With growing cyber threats and increased reliance on ICT systems, cyberinsurance is one way an organization can deal with risks, by transferring financial risk to another party in exchange for an agreed insurance premium. Other ways to deal with cyber risks is through self-insurance, where funds is set aside to be used if an incident occurs, or through self protection by introducing policies, awareness, and technical measures. A combination of methods is probably the favored choice, and for each method there is a need to identify threats and vulnerabilities to be able to quantify the associated risk and find the best possible solution (Toregas & Zahn, 2014).

As premiums are often based on the risk level of a given company, cyber security measures that lower risk may benefit a company with a lower premium. In this way insurers can help to improve innovation and cyber security investments within organizations. There are however those that argue cyberinsurance as negative to organizational cyber security work in that cyber risks as to complex to quantify, and actual losses to hard to prove (Oğüt, Raghunathan, & Menon, 2011; Toregas & Zahn, 2014).

The financial losses related to these attack can be high, but a cyber attack may also result in physical damage to people and property. In these scenarios a more sophisticated and complex insurance philosophy would be required. The maritime insurance industry lags behind the technologic development but recently they have started to focus on bodily injury and property damage caused by incidents related to cyber incidents. The insurance coverage under development would then go beyond interruption of business, network security, and privacy, to also include physical damage caused by cyber events. There is however a possibility that coverage can be manuscripted for a specific risk if the underwriter is provided with enough information about it (Greenwald, 2014).

International Maritime organization. IMO conventions, codes, and recommendations cover many areas within shipping with emphasis on safety, security, and the environment. Requirements found in IMO conventions and codes are mandatory for member states (including Norway), whilst recommendations are not. Recommendations are by some states implemented into national legislation (Branch, 2007).

Conventions and codes are monitored by inspections and certifications performed by classification societies on the behalf of flag states or ship owners. Classification societies are also involved in legislative work as they often participate in the role as technical advisors for IMO delegations (Branch & Robarts, 2014).

In the maritime domain the concept of security had a boost after the 9/11 attacks on the World Trade Center in 2001 with the introduction of the International Ship and Port Facility Security (ISPS) code, implemented as chapter XI-2 in the Safety of Life at Sea (SOLAS) convention the following year. The code introduced security into the ship and port environment by adding a layer of mandatory security requirements and recommendation guidelines to SOLAS. The code includes one mandatory part (part A), and together with a part (Part B) with recommendations in order to provide a framework for risk assessment, identification and assessment of key operations and threats, cooperation and exchange of information, identify and delegate roles and responsibility in order to ensure a certain level of security. The recommended part of the ISPS code explains good practices to fulfill the requirements of the mandatory part (Branch & Robarts, 2014; International Maritime Organization, 2003).

Unfortunately it may be the case that the ISPS code has major deficiencies in today's more technologically advanced world, as according to ENISA (2011) the code does not address cyber security but focus on physical security threats and safety.

Currently no rules or regulations concerning cyber security have been recognized by the author to be released by IMO. It seems however that things are starting to happen as IMO has been advised to address maritime cyber security on several occasions, and now the topic is up for discussion. On the Maritime Safety Committee (MSC) ninety-fourth session in 2014, cyber security was discussed based on a proposal of cyber security guidelines submitted by Canada and the United States. The proposed guidelines aims to enhance the cyber resilience of systems amongst other found in ships, ports, and marine facilities. The guidelines were proposed to be voluntary and are seen as a necessity for maritime stakeholders because of the increasing use and reliance on cyber systems. It is interpreted by the author that the proposed guidelines is intended to be implemented in the ISPS code in order to help achieve the code`s goals, also to now include cyber security measures. (IMO, 2014c).

IEC is currently working on the IEC 61162-460 standard that is intended to enable safe and secure interconnections to external sources, by setting higher requirements to systems operation and components. The external sources “include other ship networks, off-ship data sources and removable external data sources”(IMO, 2014a, p. 2).

IMO have also set criteria on navigational and vessel identification equipment that can be associated with cyber security risks. ECDIS is today an accepted method for chart carriage, but if used fully or partially, backup arrangements are required, Automatic identification system (AIS) is required to be installed on all passenger vessels, vessels larger than 300 gross tonnage on international voyages, and on vessels larger that 500 gross tonnage if they are not sailing internationally (IMO, n.d.-a, n.d.-c). This means that most ships are equipped with navigational systems related to cyber security issues.

Cyber security awareness

Awareness is defined as “*Knowledge or perception of a situation or fact*”(Oxford Dictionaries, n.d.-a), or “*Concern about and well-informed interest in a particular situation or development*” (Oxford Dictionaries, n.d.-a). Cyber security awareness can then be linked by the authors interpretation of the definition to an organization`s knowledge, perception, concern, and well-informedness of cyber security.

The Danish cyber security company CyberKeel did in a whitepaper regarding maritime cyber security point out some awareness issues in the maritime sector. They pointed out that cyber security often is considered a technical issue that is delegated to the IT department or Chief Information Officer (CIO) of companies, that there often is doubt about whether cyber threats actually are real, and if they are relevant to own company. Together with little awareness on cyber incidents from comparable industries, these elements are part of a general unawareness of cyber risks found amongst senior decision makers in the maritime sector (CyberKeel, 2014).

Low Cyber security awareness may be connected to the low number of reported incidents within the maritime sector, as well as a lack of reporting mechanisms with a specific focus on the maritime sector. As incidents are not gaining the attention of stakeholders, the awareness is kept at a low level, leading to "…*a low sense-of-urgency combined with an inadequate preparedness regarding cyber risks*." (ENISA, 2011, p. 8). Due to these factors there is a probability that a cyber attack directed towards maritime ICT systems could have a greater impact than it would if directed against sectors with higher cyber security awareness. To deal with the low awareness in the maritime sector ENISA recommends that in the short term national awareness campaigns should be developed specifically for cyber security in the maritime domain (ENISA, 2011). The Norwegian government has not yet released any awareness campaigns specific to the maritime sector recognized by the author. The Norwegian government did however in 2012 issue a strategy for cyber security with an accompanying action plan that is aimed among other things to aid and raise the awareness among decision makers in the Norwegian private sector (Norwegian Ministries, 2012a). The action plan describes that a lack of cyber security awareness constitutes a high and increasing risk, and that owners of critical infrastructure often are unaware of or lacks knowledge about vulnerabilities, and precautionary measures (Norwegian Ministries, 2012d, p. 8).

Management and measures

As no specific maritime guidelines or requirements yet are available to the authors knowledge, more general cyber security management and precautions are discussed in this section.

On a general basis there are issued several guidelines for cyber security from different standardization organizations including ISO/IEC (ISO/IEC, 2012) on general organizational cyber security, and the National Institute of Standards and Technology (NIST) concerning industrial control systems (Stouffer et al., 2011). As these guidelines and recommendations covers a very large field, reaching into complicated risk assessment and management, only a collection of some general cyber security recommendations as seen important by the author is presented below.

An organization should focus on understanding the surrounding situation of cyber security in relations to own business. Acknowledge if the company are aware of risks, if risks are dealt with, and if risk assessment is carried out. Understand vulnerabilities and consider whether the company has done enough to reduce them (NSM, 2015).

Organization should consider the possibility of their own organizations impact on others by its presence in cyberspace. The organization should consider sharing relevant information with other stakeholders (ISO/IEC, 2012).

Critical assets should be identified and evaluated according to its importance for the company, its vulnerabilities, and how they could be protected (ISO/IEC, 2012).

Assess whether the company has necessary security competence and whether employees are aware of how to contribute to the company’s security. Cyber security training should be carried out to raise the awareness amongst employees (ISO/IEC, 2012; NSM, 2015).

Cyber attacks conducted through third parties, suppliers and other partners have already been identified used against Norwegian companies. Such attacks might exploit the potentially weaker defense mechanisms present at a third party company in order to reach its target company. Assessing the state of cyber security amongst partner companies should therefor be considered (NSR, 2014).

Summary of theory

The theory provided in this thesis has shown that the maritime sector consist of vital organizations in relations to Norway`s economy and transportation of necessary goods. The shipping companies and Ship`s equipment suppliers are of special interest to this thesis because of their vital role in the Norwegian maritime sector. Cyber security is a matter of information security, ICT security, as well as security of physical assets that are connected to a network or the Internet. Cyber security should be of concern not just for the IT department of an organization, but should be part of a managerial action plan in order to deal with it properly. The maritime sector is not only vulnerable of threats to their informational assets, but also their ships with its equipment may be targeted in a cyber attack. This has been proven possible through incidents striking the maritime, as well as other sectors with similar assets. A cyber attack can be performed from inside or from outside an organization`s network, be perpetrated by different actors and can take many different forms. To deal with the threats it is important that companies are aware of threats, and knows how to deal with them.

Method

Sampling

Because of the complex composition of the maritime sector, as well as the intricately maritime company structures, necessary information required to create a randomized sample relevant to the survey was deemed unrealistic. A sample based on a non-probability sampling approach was seen as more feasible. The chosen sampling technique was used in order to give the author the ability to choose a sample based on specific criteria that by a qualitative subjective interpretation by the author would provide the best possible representative sample with relations to cyber security. The sampling technique was also utilized in order to reach potential participants because of the low profile, diverse activities, and equipment belonging to the companies in the maritime sector. The sample can be regarded as a non-probability sample chosen by the use of a purposive sampling approach (Bryman & Bell, 2011).

Cyber security includes physical elements such as industrial control systems and equipment, and it was seen as a necessity by the author to have a sample with some connection to this. As the survey also targets the Norwegian maritime sector, some criteria's were also set in order to reach respondents with a certain connection to Norway. Table 2 shows the selection criteria for the sample.

Table 2

Criteria for the sample

Group1: Shipping companies	Group 2: Ship`s equipment suppliers
Connection to Norway.	Connection to Norway.
Owns, operate, and/or manages vessels/ships.	Has equipment with some degree of automation. Delivers equipment used onboard vessels (excluding rigs).

In order to obtain a sample fulfilling this criteria`s the respondents were selected from the member lists of Maritime Dept. Federation of Norwegian Industries (Maritim Bransjeforening) (Norsk Industri, n.d.), and the Norwegian Shipowners` Association (Norges rederiforbund, 2014). The members list of the two maritime interest groups served as a good starting point as they have membership requirements that include, to varying degree, a connection to Norway (Personal communication with interest group organizations, 2015). Because these requirements are not widely available to the public, I have not been able to specify the degree of Norwegian affiliation of the survey participants. Relevant ship owning companies that were members of the Norwegian Shipowners` Association were narrowed to fulfill the criteria by conducting a review of the possible respondents websites. Following the criteria`s set excluded companies solely engaged in for example rig operation, crew management or catering companies. In addition, Norwegian Shipowners` Association employees provided some guidance in what companies to exclude from the list. Companies complying with criteria were then contacted by phone to retrieve best possible contact information for submission of the questionnaire. The original list was eventually narrowed down from about 150 to *73 companies*.

The equipment suppliers was selected from the members list of Maritime Dept. Federation of Norwegian Industries (Maritime Bransjeforening), followed by a website review to identify whether some of their products (equipment or systems) contained some degree of automation. Those that did not supply equipment containing some degree of automation, for example vessel furnishing companies were excluded from the list. Contact information was obtained via Maritime Dept. Federation of Norwegian Industries members list that consists of 188 companies. *39 companies* in total within the ship`s equipment suppliers category were selected to be a part of the sample.

Survey

As a part of this thesis a survey was issued to relevant participants in order to answer the thesis research questions. The information given at the start of the survey can bee seen in the appendix. The survey aims to gather quantitative data on cyber security awareness and measures found in the maritime sector.

The survey questions were mostly created with information from (ISO/IEC, 2012), (Office of Compliance Inspections and Examinations, 2014), (Von Solms & Van Niekerk, 2013), and (ENISA, 2011). Some answer choices for multiple answer questions was identified through Internet searches to find reasonable figures and possible answer to the questions. Questions were also generated as a result of input and discussions with secondary supervisors.

The survey was constructed with the help of the online survey platform SurveyMonkey (SurveyMonkey, n.d.). A paid subscription was signed with the service provider in order to create the desired survey outline and functions. The survey has not received any sponsorship or funding, an exception to this would be if Buskerud and Vestfold University College grant survey expenditures refund.

The survey was distributed to the two defined groups within the Norwegian maritime sector; Ship`s equipment suppliers, and shipping companies. Because of a possible risks involved with identifying individual companies participating in this survey, a choice was made to only provide limited explanatory information about the participants. However, in order to give some degree of applicability to the results of the survey, some general information about survey participants was seen as necessary.

Survey design

The survey was designed as a self-completion questionnaire with no intervention from the researcher except from the information provided at the start of the survey (Bryman & Bell, 2011).

About 85% of the questions were formed as statements followed by a response scale using a closed verbal format referred to as the Likert scale. The scale was used in order to examine the attitude of participants against the different statements, and because of the closed question format (answers are predefined by me), both time used to answer the survey and the data analysis process was made easier compared to if respondents themselves were to insert own formulated answers (Bryman & Bell, 2011). The Likert scale was arranged in order from Strongly Disagree, disagree, neither agree nor disagree, agree, and strongly agree. The scale was then coded from their string ordinal values to numeric values ranging from 1-5, in order for the resulting dataset to be applicable for further analysis in IBM SPSS statistics software. The used scale and corresponding coded values are shown in table 3.

Table 3

Coding from Likert to numeric scale

Likert scale	Coded value
Strongly disagree	1
Disagree	2
Neither agree nor disagree	3
Agree	4
Strongly agree	5

The remaining questions contained multiple choices or interval ranking scales. The multiple-choice questions had predefined text alternatives with an option to choose "other (please specify)" in case other responses than the suggested by the author could be of importance. On questions based on answer rankings, the ranking scales consisted of predefined text or numeric interval alternatives.

The respondents were informed on the first page of the survey with the following information about terms used in the questionnaire "*assets are categorized as either Information assets or physical/non-information assets. Information assets include information that has value to your company, stored or transmitted with the use of ICT technology. Physical/non-information assets include physical assets accessible through ICT technology. For the equipment suppliers physical/non-information assets are limited to equipment/systems that is or will be installed on ships/vessels. For ship owners/operators/management, the actual ships/vessels with its equipment/systems that is accessible through ICT are considered physical/non-information assets. Physical/non-information assets can include but is not limited to; remote management systems, control systems, SCADA, telecom equipment, navigation equipment, information equipment, AIS, propulsion technology, safety systems, cargo handling equipment, mooring equipment, power management, ballast water treatment etc. Threats are in this survey classified* *as either internal or external. Internal refers to whether a cyber security incident originates from within the organization's network. External refers to if the cyber security incident is conducted from outside the organization's network (ie. from internet).”*

Procedure

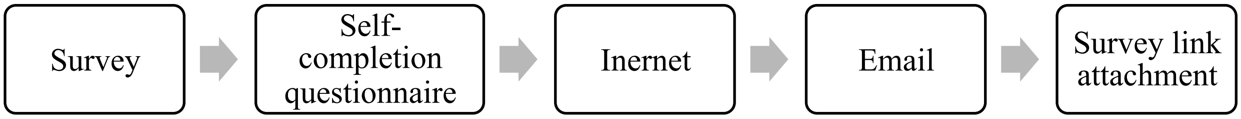
Reaching people within companies with skills to answer questions regarding cyber security were attempted by phone calls to every shipping company in the sample. During the phone calls, some notes were taken on a general reception of my enquiry. With an explanation of my thesis and the survey I got an impression that the topic was shown interest, but that it appeared to evoke some skepticism, and possibly a lack of knowledge on the subject. Some companies said that they were not answering surveys as a general policy.

It was encouraged in a cover letter mail regarding the survey to both the equipment suppliers and the shipping companies that recipients should forward the survey to suitable persons within the organization. The job position of those answering the survey is thus unknown.

The survey was sent to a total of 112 companies. 1 recipient replied survey email with that the survey was erroneously sent to him/her, and that mails in connection with the survey consequently was deleted. In a few other instances the mail address was wrongly spelled or obtained, and the survey had to be resent to a corrected address. Others replied for various reasons that they were not suitable for the survey as they were part of an international organization and thus had little influence on cyber security matters. Two reminder emails were sent to all respondents who had not yet answered the questionnaire. The mode of distribution is shown in figure 4.

Figure 4

Survey mode of administration. Adapted from figure 7.2 (Bryman & Bell, 2011, p. 175)



Responses. A total of 20 recipients carried out the survey, of those, 19 were considered usable and 1 was considered unusable. The usable responses include those who completed the survey. With completed is meant that respondents answered the question identifying respondent groups in addition to pressing the done button on the final survey page to submit their reply. Those partially finishing the survey, i.e. those not pressing the done button on the final page was considered unusable.

The total response rate ”$\frac{Number\ of\ usable\ respondents}{total\ sample - unsuitable\ or\ uncontactable\ members\ of\ the\ sample} * 100$ “ (Bryman & Bell, 2011, p. 189) would for this survey be $\frac{19}{112-1} * 100 = 17.1\%$.

Of the respondents who completed the survey, the percentage of questions answered was high.

The respondents were divided into two groups depending on their answer to Q22*“My organization/business division is considered a: a) Ship owning/operating company (with or without own ship management team), b) Dedicated ship management company, c) Maritime equipment supplier.”*. As explained in the sampling section, ship owners, operators, and ship management companies were sorted into *Group 1* (e.g. those who responded alternative a, or alternative b), while *Group 2* consists of the equipment suppliers (e.g. those who ticked off alternative c.). The number of usable responses per group is shown in table 4.

Table 4

Usable responses per group category

	Group	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	12	63.2	63.2	63.2
	2.00	7	36.8	36.8	100.0
	Total	19	100.0	100.0	

Results

Cyber attack incidents. Table 5 shows the number of cyber security incidents for shipping companies and equipment suppliers categorized by group, internal or external attack source of the attack, and the type of asset that the incident targeted.

Table 5

Q7. In the last 2 years my organization has been subjected to one or more cyber incidents; theft, destruction, alternation, hijacking, unauthorized access, exploits, or denial of availability of

	Group			
	Shipping companies		Equipment suppliers	
	Count	Column Responses %	Count	Column Responses %
Information assets, perpetrated by an internal source (Employee or trusted third party with access to internal network).	0	0.0%	1	9.1%
Information assets, perpetrated by an external source (Malware, hackers...)	2	15.4%	4	36.4%
Physical/non-information executed by internal source (Employee or trusted third party with access to internal network).	0	0.0%	1	9.1%
Physical/non-information executed by external source (Malware, hackers...)	1	7.7%	2	18.2%
To our knowledge we have not been subjected to a any form of cyber incident	10	76.9%	3	27.3%
N Total	12	100.0%	7	100.0%

Cyber security awareness and precautions towards cyber threats. In order to get a meaningful interpretation of the data set, an exploratory factor analysis, more specifically a principal components analysis was in collaboration with my main supervisor identified as an appropriate analysis.

An explanatory factor analysis is a tool used in order to find inter-correlations between variables and sort them into hypothetical factors (clusters of variables) so that the data set can be more easily understood and more manageable. There is no consensus on the minimum number of respondents in a factor analysis, however there is an underlying agreement is that there should be more respondents than variables (Bryman & Cramer, 2005; Robson, 2011).

The method used for extraction of factor analysis was principal components. The Principal components analysis was conducted on variables Q1, Q2, Q3, Q4, Q8, Q12, Q13, Q14, Q15, Q16, Q17, and Q18. To decide on the number of resulting factors (components) in the analysis, an extraction criterion known as the Kaiser`s criteria limited the number of factors to include only those with an eigenvalue > 1. The rotation used in the factor analysis was an orthogonal method named Varimax. Because of the orthogonal method the resulting components are unrelated to each other (Bryman & Cramer, 2005). The principal component factor analysis revealed three components that together could be used to explain 71.1% of the variance. The components with their eigenvalues and variance are shown in table 6.

Table 6

Total Variance Explained

	Initial Eigenvalues			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	**4.563**	**38.024**	**38.024**	3.353	27.942	27.942
2	**2.376**	**19.797**	**57.820**	2.602	21.687	49.630
3	**1.595**	**13.290**	**71.110**	2.578	21.481	71.110
4	.967	8.061	79.172			
5	.751	6.261	85.433			
6	.606	5.050	90.482			
7	.381	3.172	93.654			
8	.286	2.385	96.039			
9	.266	2.213	98.252			
10	.134	1.114	99.366			
11	.062	.513	99.879			
12	.015	.121	100.000			

Extraction Method: Principal Component Analysis.

The resulting rotated component matrix from the principal components analysis are shown in table 7. Variables that correlates with lower values than 0.3 or -0.3 with a factor were set to be excluded as they are considered unimportant (Bryman & Cramer, 2005).

Table 7

Rotated Component Matrix[a]

	Component		
	1	2	3
Q1. The concept of cyber security is well known within our organization.			**.897**
Q2. My organization evaluates cyber security as an important topic in relation to our business.		**.762**	
Q3. My organization assess cyber security as an increasing concern.	.322	**.715**	
Q4. My organization has taken precautionary measures to deal with cyber security threats.		**.656**	.304
Q8. It is likely that my organization could be subjected to an attack in the next two years.		**.839**	
Q12. My organization has established good information sharing and coordinating procedures for cyber security events.			**.870**
Q13. My organization knows where and how to report a cyber security event.	.430		**.784**
Q14. My organization has established partnership with a CERT/CIRT/CSIRT team.	**.842**		
Q15. My organization has good communication and information sharing with other companies in our business segment regarding cyber security.	**.705**	.490	
Q16. My organization has good communication with our third party suppliers regarding cyber security.	**.865**		
Q17. Our third party suppliers have established procedures to deal with cyber security issues.	**.608**		
Q18. My organization sets cyber security requirements for new IT/ICT equipment purchases.	**.762**		

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 5 iterations.

The three components that are outlined in bold in table 7 was named based on a subjective qualitative interpretation of the variables constituting the different components:

- Component 1: *Collaboration (externally oriented)* (Q14, Q15, Q16, Q17, Q18).
- Component 2: *Organizational concern.* (Q2, Q3, Q4, Q8).
- Component 3: *Organizational procedures (internally oriented).* (Q1, Q12, Q13).

An independent sample t-test (unpaired two-group t-test) was used to check if there were any statistical differences between shipping companies and equipment suppliers on the components. With confidence interval was set to 95%, the test showed a significant difference between the Shipping companies and equipment suppliers regarding the component *organizational concern* ($\rho < 0.05$.). No significant differences were found between the groups on either *Collaboration (externally oriented),* or *Organizational procedures (internally oriented)* components. Mean values of the variables constituting the factors are shown in table 8

Table 8

Mean scores of components variables

	Group	N	Mean	Std. Deviation	Std. Error Mean
Organizational concern.	1.00	10	3.7750	.38097	.12047
	2.00	7	4.1429	.65918	.24915
Collaboration (externally oriented).	1.00	12	3.4167	.50061	.14451
	2.00	7	3.2000	1.08321	.40941
Organizational procedures (internally oriented).	1.00	11	3.4848	.65597	.19778
	2.00	6	3.3889	1.04172	.42528

Differences between measures towards cyber security. Four variables were created on the basis of the questionnaire that asked questions regarding the shipping companies and equipment suppliers measures on cyber security in relations to *Internal threats information assets* (Q36-41), *External threats information assets* (Q42-45*)*, *Internal threats physical/non-*

information assets (Q46-49), and *External threats physical/non-information assets* (Q50-53). Mean values were created for the variables by adding each item within the variable and then dividing it by the number of items ($\overline{X} = \frac{\sum x}{n}$). The mean values of the variables sorted by group are shown in table 9.

Table 9

Mean scores variables

Variables	N	Mean	Std. Deviation
External threats information assets.	19	3.4342	.60577
Internal threats information assets	18	3.5667	.58712
External threats physical/non-information assets	18	3.2361	.61520
Internal threats physical/non-information assets	18	3.2500	.52859
Valid N (listwise)	17		

A repeated measures general linear model (GLM) analysis was performed in order to test the mean variables against each other on several levels, and between groups. The variables were defined to a two level factor named Physical vs. Information, and a two level factor named *external vs. internal.* Together with the two level factor *groups,* they constituted a (2x2x2) matrix (Physical vs. Information x External vs. Internal x Group1vs. Group2). *Physical vs. Information* and *External vs. Internal* was used *within* subjects, and *Group1 (Shipping companies) vs. Group2 (Equipment suppliers) between* subjects (Bryman & Cramer, 2005). Resulting relevant figures for *Physical vs. Information* is shown in figure 5, internal vs. external x physical vs. information for shipping companies are shown in figure 6, and internal vs. external x physical vs. information for equipment suppliers are shown in figure 7.

The analysis revealed a statistical significant difference between Physical vs. Information indicated by ($p < 0.05$).

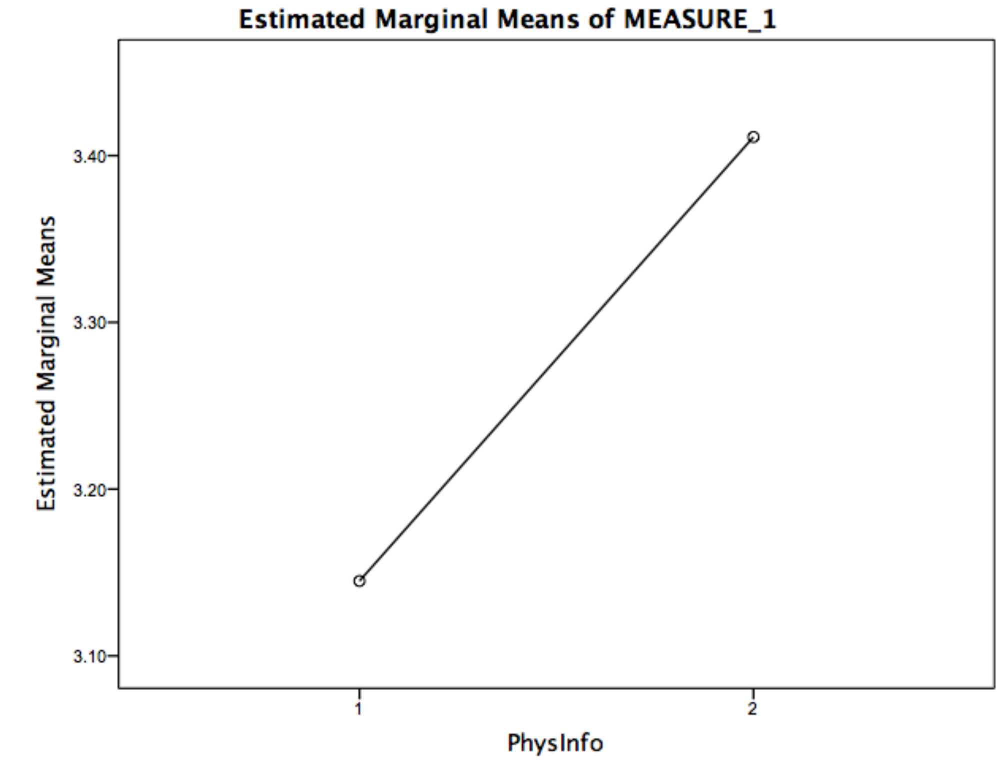


Figure 5. Physical vs. information cyber security measures. Y-axis represents the mean score, while Physical is connected with 1 and information with 2 on the x-axis.

A statistical significant difference was also revealed between Physical vs. Information vs group, indicated by ($p < 0.01.$). No other significant differences were found by the GLM analysis. A t-test verified the findings ($p < 0.05.$), and pointed out measures towards external physical was significantly different between the groups.

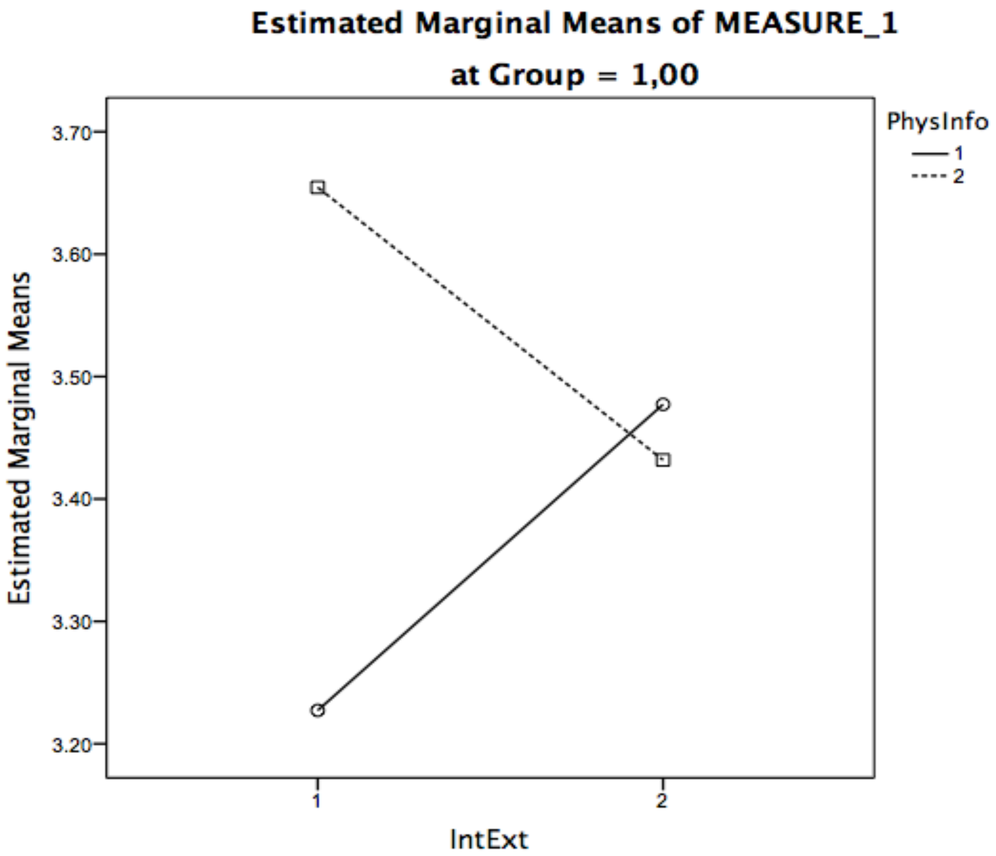


Figure 6. Figures for group 1 (Shipping companies). Comparing internal vs. external security measures against physical vs. information cyber security efforts. Y-axis represents the mean score, while internal is connected with 1 and external with 2 on the x-axis. A solid line represents physical, while information is represented by a dotted line.

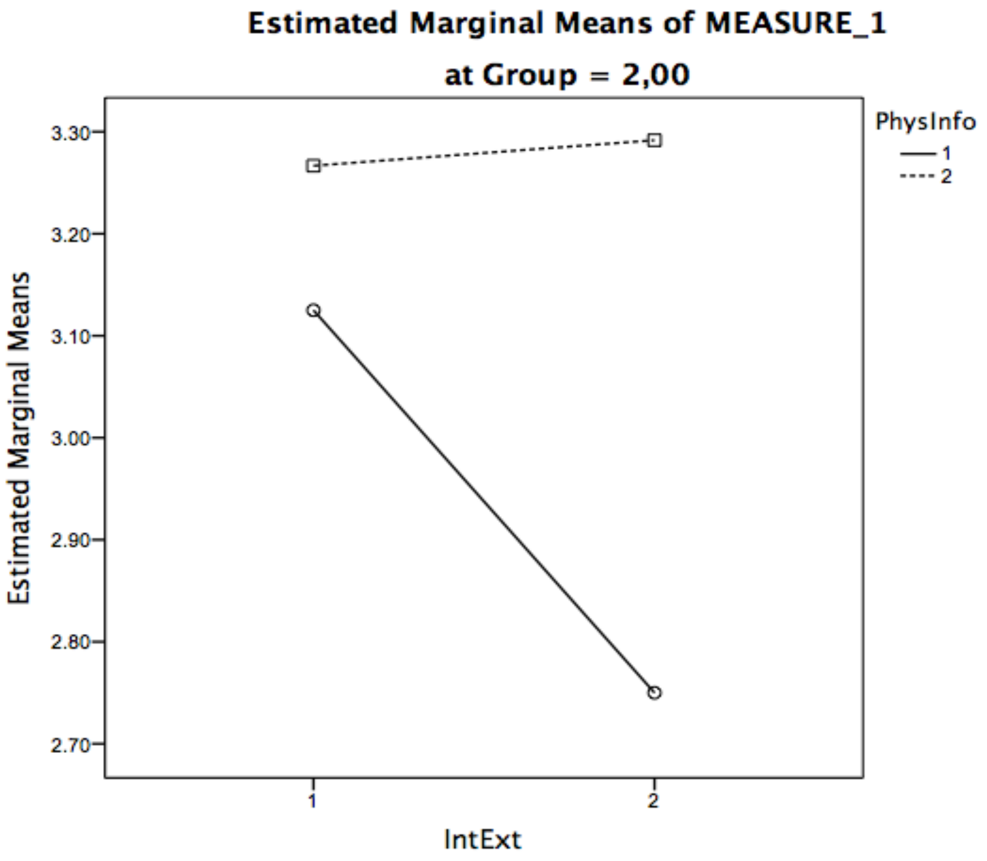


Figure 7. Figures for group 2 (Equipment suppliers). Comparing internal and external efforts against each other and physical information cyber security efforts. Y-axis represents the mean score, while internal is connected with 1 and external with 2 on the x-axis. A solid line represents physical, while information is represented by a dotted line.

Limitations

The sample in this thesis is based on the members lists from the dominating interest groups for maritime equipment suppliers and shipping companies Norwegian. This could be a strength as their members represent by the authors evaluation of the members lists, most of the major actors within Ship`s equipment suppliers and Shipping companies. It can however not be assumed that all companies in Norway that fulfilled the sampling criteria in this thesis are members of these interest groups.

The chosen sampling technique may be argued to have a low degree of generalizability because of the purposive selection of respondents. Purposive sampling in the form of non-probability sampling technique that is known to have limitations in generalization to larger populations (Bryman & Bell, 2011).

The response rate of the questionnaire can be argued to be low, and thereby limited in its ability to be generalized. The response rate of 17.1% can possibly be explained by factors identified in other research on information security. A survey that was part of a Ph.D. thesis by Albrechtsen in 2008 was carried out amongst Norwegian persons responsible for information security in different organization. The survey yielded a response rate of 16%. Using the response rate formula applied in my thesis, the response rate would have been approximately 13% because their calculations included unusable responses. The possible explanations discussed included results from another study of information security performed by Kotulic and Clark in 2004 that had an even lower response rate. The study by Kotulic and Clark was followed up by a survey in an effort to explain the low response rate. Possible explanations included that there existed policies within companies not share their information security performance, and unwillingness to spend valuable managing time on surveys (Albrechtsen, 2008).

A certain level of skewness was detected in the data set slightly biased towards a positive attitude on questions regarding self-assessment of own security awareness and measures. That respondents typically want to show themselves from their best side is a common disadvantage of surveys that is dependent on answers from respondents (Robson, 2011). However, as this survey is about cyber security, an even greater bias might be present. This skewness was also present in the survey conducted by Albrechtsen (2008). Albrechtsen argues that because of the skewness, respondents consider themselves "…the best of the class…" (Albrechtsen, 2008, p. 49). The skewness together with the low response of the survey could indicate that "*only those who have knowledge and interest in information security responded to the survey."* (Albrechtsen, 2008, p. 49). Since information security is a part of cyber security, this reasoning should also be valid for my survey.

To ask only one respondent from each organization to represent the whole company means that a high number of companies can more easily be included in the survey, saving both time and resources. It may however be unwise to expect one person to know the answer to all the questions asked in the questionnaire, and the respondent may also try to favor his/her role in the company, especially if the respondent has a managing role (Bryman & Bell, 2011). In an effort to avoid this in my research it is specified in the cover letter that it was possible to forward the questionnaire to be fully or partially completed by other persons in the organization.

Discussion

In this section, each research questions is discussed on the basis of the results obtained from the questionnaire. Some theory is used in order to discuss aspects that are seen as important by the author. The author introduces some thoughts and opinions about the results in an effort to explain and discuss them. It could be important to acknowledge that these are the author's subjective opinions.

Have they been subjected to cyber attacks? The number of replies on cyber incidents shows that of the 12 shipping companies, 10 did not know or had not been subjected to a cyber attack. The 2 shipping companies that responded that they had been subjected to a cyber attack was attacked by an external threat actor that targeted either their physical or their information assets. Of the equipment suppliers, 3 companies reported that they had not been subjected to any cyber attack to their knowledge. 4 companies reported that they had been subjected to one or more attacks, and 1 company within this group responded that they had been subjected to an attack on both physical and information assets from an internal and external source. Another company had been subjected to an attack on both information and physical assets perpetrated by an external perpetrator, and an external actor attacked the 2 last companies' information assets. This shows that actors in the maritime sector are vulnerable to, and have ben subjected to cyber attacks. The attacks was perpetrated from internal and external sources directed at both informational and physical assets.

6 out of 19 companies or 31% of the participants reported that they had been prone to at least one cyber attack in the last two years. As cyber attacks against large Norwegian companies were estimated at around 50% in 2013 (NSR, 2014), and that there is a chance that companies are reluctant to share security information (Albrechtsen, 2008), there is a possibility that the

actual incidents are higher than the 31% reported to the survey of this thesis. Comparing the results from this thesis with estimated cyber attacks against large Norwegian companies (NSR, 2014) does not seem to indicate that the actors in the maritime sector are more frequently attacked that other Norwegian organization unless there exists unreported attacks. Sharing information about incidents may help to raise the awareness about cyber security in the sector (ENISA, 2011).

Are the Norwegian maritime equipment suppliers and ship owners aware of cyber security related issues? A principal components factor analysis revealed three unrelated components. *Component 2* was interpreted by the author to have a relation to *organizational concern,* based on it`s contained variables that includes *my organization evaluates cyber security as an important topic in relation to our business*, *my organization assess cyber security as an increasing concern*, and *it is likely that my organization could be subjected to an attack in the next two years*. By looking at a definition for awareness "*Concern about and well-informed interest in a particular situation or development*" (Oxford Dictionaries, n.d.-a) it can be seen a likely connection between the component contents and awareness. The last variable in the component *"My organization has taken precautionary measures to deal with cyber security threats*" may be less coupled with awareness, but could possibly relate to the other variables as precautions taken potentially could be a response of the awareness A significant difference was found between the shipping companies and equipment suppliers on the component *organizational concern. Th*e ship`s equipment suppliers had a higher mean value score of 4.14 on the Likert scale compared to 3.77 for the shipping companies. This might be an indication that the ship`s equipment suppliers are slightly more aware of cyber security related issues than the shipping companies. As to the author's knowledge, no recommended baseline exists in order for me to decide with certainty if the mean values of organizational concern and awareness are good or bad. The following interpretation of the mean values is thus based on a subjective interpretation by the author. The mean score for the ship`s equipment suppliers could indicate that their attitude towards the asked questions are positive as 4 on the Likert scale indicated that they agree to the statements and thereby showing a positive attitude towards cyber security awareness. A mean value score above 4 is to the authors opinion an indication of that the Ship`s equipment suppliers are aware of cyber security related issues on a level that is higher than the awareness found by ENISA in 2011 where cyber security awareness in the European maritime sector was identified as either very low or even non-existent (ENISA, 2011). Because the shipping companies mean values are closer to agree than to the neutral statement on the Likert scale, it is by the authors opinion also awareness present amongst the shipping companies that is higher that the findings of ENISA. The comparison against ENISA`s findings may however be far fetched, as ENISA does not give any information about scale rankings of their findings. As by the author's opinion the awareness is indicated to be higher than the findings in Europe in 2011, it could potentially mean that Norwegian organizations in the maritime sector are more aware than in the rest of Europe, or that the cyber security awareness in the maritime sector has increased on a general basis during the last four years. These assumptions have however not taken into account the limitations in that respondents typically want to show themselves from their best side in a self-assessment survey.

Do they take precautions in order to deal with cyber threats? The content in *component 1 Collaboration (externally oriented)* may be described with that precautions are taken when collaborating with third party suppliers by ensuring that their partners have procedures to deal with cyber security, and for ensuring cyber security for purchases of new equipment. Partnership with a CERT/CIRT/CSIRT team, and good information sharing with other companies may indicate that they take precautions by staying updated on cyber security issues. *Component 3 Organizational procedures (internally oriented)* content may be explained by precautions taken by ensuring that the concept of cyber security is well known within the organization, and by preparation in case of a cyber incident. No significant differences were found between the groups on either of the components. Their mean value scores as seen in table 8 is leaning towards *nether agree nor disagree* on the Likert scale for both components and groups with 3.41 (component 1) and 3.48 (component 3) for the shipping companies, and 3.2 (component 1) and 3.38 (component 3) for the equipment suppliers. By a subjective understanding of the mean values and related components, there is likely that some precautions taken in order to deal with cyber security threats. The attitude towards precautions might however not be sufficient to avoid cyber threats that from partner companies and their equipment, or to communicate relevant information about a cyber attack with other stakeholders if an attack should occur.

Are there any differences in how they relate to physical and information aspects of cyber security? A repeated measures GLM analysis was performed in order to find differences between Physical vs. Information x External vs. Internal x Group1vs. Group2. A significant difference was found between cyber security measures taken towards physical and information assets. The difference can be seen in figure 5 where it can bee seen that security measures towards information assets has a higher mean value score of 3.41 compared with the measures towards the physical assets that has a mean value score of 3.14. This indicates that there is a higher focus on measures taken towards information assets than the physical assets.

Are there any differences between the cyber security measures between ship owners and equipment suppliers? The repeated measures GLM analysis showed a significant difference on Physical vs. Information x External vs. Internal x Group1vs. Group2

Figure 7 shows that the ship`s equipment suppliers measures towards physical assets against threats from external sources have a mean score of 2.75, while the shipping companies (figure 6) have a mean value score of 3.47. A mean score of 2.75 indicates that the mean score is below neither agree nor disagree on the Likert scale, and may on a subjective evaluation indicate that their cyber security measures are inadequate towards their equipment that is installed on ships. A possible explanation based on a subjective interpretation may be if the responsibility of securing equipment is transferred to the shipping companies after delivery. The author does however not know which one of the two who groups that has the fully or partially responsibility of equipment after delivery.

Conclusions

The conclusion of this thesis try to answer to the five research questions regarding the assessment of cyber security awareness and measures in the Norwegian maritime sector.

Have they been subjected to cyber attacks? Yes, actors in the maritime sector are found to be vulnerable to cyber attacks on both physical and informational assets. In the results of this thesis it is shown that both shipping companies and Ship`s equipment suppliers have been subjected to cyber attacks in the last two years. A majority of these attacks was targeting informational assets from external threat actors, but both physical and information assets have been attacked from external and internal sources.

Are the Norwegian maritime equipment suppliers and ship owners aware of cyber security related issues? The Shipping companies and equipment suppliers both scored high on the mean scores on a component regarding cyber security awareness. A significant difference between the shipping companies and equipment suppliers was found. With a higher mean value score the equipment suppliers were found to have higher cyber security awareness than the shipping companies.

Do they take precautions in order to deal with cyber threats? No significant results were obtained to answer this question. The answer to this question is thus left open if deemed interesting for further research.

Are there any differences in how they relate to physical and information aspects of cyber security? Yes, a significant difference was found between cyber security measures taken towards physical and information assets. The mean values ranked highest with relations to information assets. This shows that there is a higher focus on measures taken towards information assets than towards the physical assets.

Are there any differences between the cyber security measures between ship owners and equipment suppliers? Yes, the ship`s equipment suppliers measures towards physical assets against threats from external sources had a mean score of 2.75, while the shipping companies mean value scored 3.47. The difference was found to be significant, and hence the shipping companies can be said to have a higher focus on measures towards external physical assets.

References

Albrechtsen, E. (2003). *Security vs safety* Retrieved from http://www.iot.ntnu.no/users/albrecht/rapporter/notat safety v security.pdf

Albrechtsen, E. (2008). *Friend or foe? : information security management of employees.* (Ph.D. thesis), Norwegian University of Science and Technology, Faculty of Social Sciences and Technology Management, Department of Industrial Economy and Technology Management, Trondheim.

Bartnes, L. M., Nordland, O., Rostad, L., & Tondel, I. A. (2006). *Safety vs security?* , New Orleans, USA. http://sfweb2.sintef.no/Publikasjoner-SINTEF/Publikasjon/?pubid=SINTEF+S827

Branch, A. E. (2007). *Elements of shipping* (8 ed.). London: Routledge.

Branch, A. E., & Robarts, M. (2014). *Branch's elements of shipping* (9th ed. ed.). London: Routledge.

Brumfield, C. (2013). Is it “Cybersecurity,” “Cyber Security” or (Please No) “Cyber-Security?" I Asked the Experts. Retrieved 05.01, 2015, from http://www.digitalcrazytown.com/2013/08/is-it-cybersecurity-cyber-security-or.html

Bryman, A., & Bell, E. (2011). *Business Research Methods* (3 ed.). Oxford: University Press.

Bryman, A., & Cramer, D. (2005). Quantitative data analysis with SPSS 12 and 13 : a guide for social scientists. London: Routledge.

CyberKeel. (2014). *Maritime cyber-risks Virtual pirates at large on the cyber seas* Retrieved from http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf

ENISA. (2011). *Analysis of cyber security aspects in the maritime sector.* Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport

Ervik, C., & Hansen, E. T. (2014, 28.08). Vil vere opne om data-angrep. *NRK Møre og Romsdal*. Retrieved from http://www.nrk.no/mr/vil-vere-opne-om-data-angrep-1.11902610

Federal Office for Information Security. (2014). *The State of IT Security in Germany 2014.* Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf.pdf?__blob=publicationFile

Gori, U. (2009). Modelling cyber security: approaches, methodology, strategiesNATO science for peace and security series. Amsterdam: Ios Press.

Greenwald, J. (2014). Insurers develop cyber cover for maritime industry.(Brief article). *Business Insurance, 48*(10), 0030.

Harris, S. (2012). CISSP exam guideAll-in-one (Series) (6th ed. ed.). Berkeley, Calif.: Osborne McGraw-Hill distributor.

IMO. (2014a). *Any other business* IMO Document NCSR 2/22/4, Submitted by the International Electrotechnical Commission, 2 January, *Progress on standards development by the International Electrotechnical Commission (IEC)* Retrieved from https://docs.imo.org

IMO. (2014c). *Measures to enhance maritime security* IMO Document MSC 94/4/1, Submitted by Canada and the United States, 12 September *Measures toward enhancing maritime cyber security* Retrieved from https://docs.imo.org

IMO. (n.d.-a). AIS transponders. Retrieved 13.03, 2015, from http://www.imo.org/OurWork/Safety/Navigation/Pages/AIS.aspx

IMO. (n.d.-c). Charts. Retrieved 13.02, 2015, from http://www.imo.org/OurWork/Safety/Navigation/Pages/Charts.aspx

International Maritime Organization. (2003). *ISPS code: International Ship and Port Facility Security Code and SOLAS amendments adopted on 12 December 2002* (2003 ed. ed.). London: International Maritime Organization.

ISO/IEC. (2012). *ISO/IEC 27032:2012: Information technology – Security techniques – Guidelines for cybersecurity* (1st ed.). Genève: ISO/IEC.

ISO/IEC. (2014). *ISO/IEC 27000:2014: Information technology - security techniques - information security management systems - overview and vocabulary* (3rd ed.). Genève: ISO/IEC.

Jakobsen, E. W., Mellbye, C. S., & Holmen, R. B. (2014). *Maritim verdiskapingsbok* Menon Business Economics (Ed.) Retrieved from http://menon.no/upload/2014/02/17/maritimt-forum-verdiskapingsbok-2014.pdf

Kushner, D. (2013). The real story of stuxnet. *IEEE Spectrum, 50*(3), 48-53. doi: 10.1109/MSPEC.2013.6471059

Marine Cybernetics. (n.d.). *Cybersecurity and network resilience* Retrieved from http://www.marinecybernetics.com/images/CyberFlyer.pdf

Mellbye, C. S., & Jakobsen, E. W. (2014). *Norwegian Maritime Equipment Suppliers 2014.* M. B. Economics (Ed.) Retrieved from http://www.norskindustri.no/siteassets/dokumenter/maritime_equipment_suppliers_eng_web.pdf

Norges rederiforbund. (2014). Medlemmer. Retrieved 11.01, 2015, from https://www.rederi.no/om-oss/medlemmer/

Norsk Industri. (n.d.). Våre medlemmer. Retrieved 15.11, 2015, from http://www.norskindustri.no/medlem/vare-medlemmer/?branch=Maritim+bransjeforening

Norwegian Ministries. (2012a). *Cyber Security Strategy for Norway.*: The Ministry of Government Administration, Reform and Church Affairs Retrieved from http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Cyber_Security_Strategy_Norway.pdf.

Norwegian Ministries. (2012d). *Nasjonal strategi for informasjonssikkerhet: Handlingsplan*. Oslo: Retrieved from https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf.

Norwegian Shipowners' Association. (2013). *Great maritime opportunities Maritime outlook report 2013* Retrieved from http://93.124.224.90/nrweb/mm.nsf/lupgraphics/Final_6242-Konjunkturrapport-eng-5k.pdf/$file/Final_6242-Konjunkturrapport-eng-5k.pdf

NSM. (2015). *Risiko 2015* Retrieved from https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2015-web.pdf

NSR. (2014). *Mørketallsundersøkelsen - Informasjonssikkerhet, personvern og datakriminalitet* Retrieved from http://www.nsr-org.no/getfile.php/Dokumenter/NSR publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall_2014.pdf

Office of Compliance Inspections and Examinations. (2014). *National exam program: Risk alert* Vol. 4. Retrieved from http://www.eci.com/pdf/SEC-Cybersecurity-Sample-Questions.pdf

Oğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk analysis : an official publication of the Society for Risk Analysis, 31*(3), 497. doi: 10.1111/j.1539-6924.2010.01478.x

Oxford Dictionaries. (n.d.-a). Awareness. Retrieved 20.03, 2015, from http://www.oxforddictionaries.com/definition/english/awareness

Oxford Dictionaries. (n.d.-d). safety. Retrieved 01.02, 2015, from http://www.oxforddictionaries.com/definition/english/safety

Oxford Dictionaries. (n.d.-f). security. Retrieved 01.02, 2015, from http://www.oxforddictionaries.com/definition/english/security

Radan, D. (n.d.). MARINE POWER PLANT CONTROL SYSTEM, POWER / ENERGY MANAGEMENT OF MARINE POWER SYSTEMS. Trondheim, Norway: Norwegian University of Science and Technology - NTNU.

Reason, J. (1995). Understanding adverse events: human factors. *Quality in health care : QHC, 4*(2), 80-89.

Rederi-skatteutvalget. (2006). Forslag til endringer i beskatningen av norsk utenriks sjøfart : utredning fra et utvalg oppnevnt ved kongelig resolusjon 17. desember 2004 : avgitt til Finansdepartementet 7. mars 2006 Norges offentlige utredninger (Journal : online) (Vol. NOU 2006:4). Oslo: Departementenes servicesenter, Informasjonsforvaltning. Retrieved from https://www.regjeringen.no/contentassets/88c6dec7cea548a4bfae051fb9559308/no/pdfs/nou200620060004000dddpdfs.pdf.

Reve, T., & Sasson, A. (2012). *Et kunnskapsbasert Norge*. Oslo: Universitetsforl.

Robson, C. (2011). *Real world research : a resource for users of social research methods in applied settings* (3rd ed. ed.). Chichester: Wiley.

Ruset, I. J. (2014, 30.05). Ulstein Group vart utsett for dataangrep. *NRK Møre og Romsdal*. Retrieved from http://www.nrk.no/mr/ulstein-group-utsett-for-dataangrep-1.11747769

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press.

Smart Comp. (2013). *Martime sector developments in the global markets.* Vol. 3. *SmartComp Research Report.* Retrieved from http://www.utu.fi/en/units/tse/units/PEI/research/Documents/SmartComp Research Report October 2013 final.pdf

Stopford, M. (2009). *Maritime Economics* (3 ed.). 2 Park square, Milton park, Abingdon, Oxon: Routledge.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST Special Publication 800-82*: NIST.

SurveyMonkey. (n.d.). Home. Retrieved 06.1, 2015, from https://www.surveymonkey.com

Toregas, C., & Zahn, N. (2014). *Insurance for Cyber Attacks: The Issue of Setting Premiums in Context* Retrieved from http://www.cspri.seas.gwu.edu/s/cyberinsurance_paper_pdf.pdf

Transportetatene, Avinor, Jernbaneverket, Kystverket, & Statens vegvesen. (2015). *Utfordringer for framtidens transportsystem - Hovedrapport fra analyse- og strategifasen Nasjonal transportplan 2018-2027* Retrieved from http://www.ntp.dep.no/Nasjonale+transportplaner/2018-2027/Utredninger+og+grunnlagsmateriale

U.S. Coast Guard. (2014). *Cybersecurity: Vulnerabilities Threats Risk management* Coast Guard Journal of Safety & Security at Sea: Proceedings of the Marine Safety & Security Council Vol. 71. Retrieved from http://www.uscg.mil/proceedings/archive/2014/Vol71_No4_Wint2014.pdf

Ulstein Group. (2013). About. Retrieved 02.04, 2015, from http://www.ulstein.com/Kunder/ulstein/cms66.nsf/$all/DF4E1FA5AD94658BC125715C0066B68A?open&ql=AboutLayout&qm=wcm_2,4,1,0

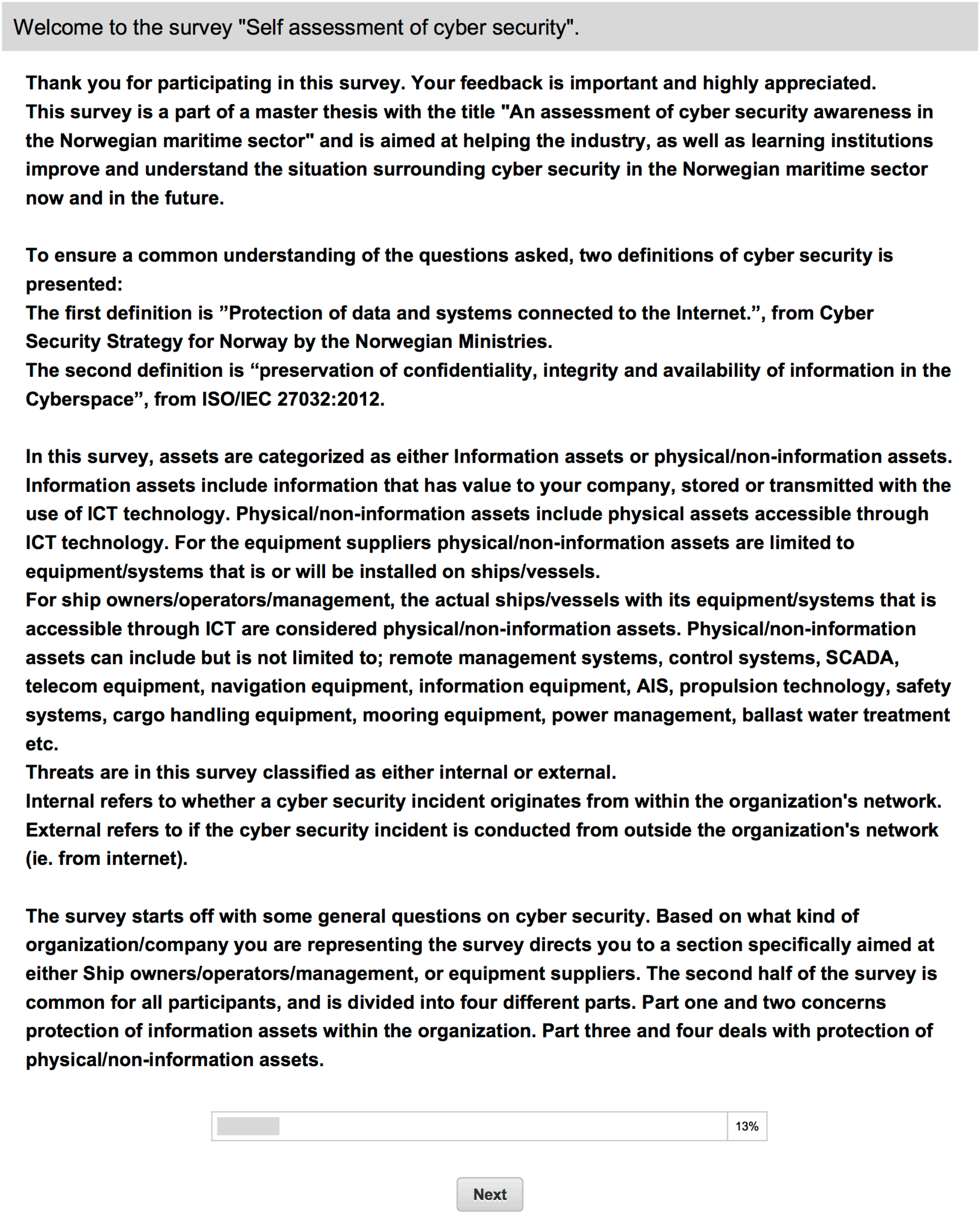
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security, 38*, 97-102. doi: 10.1016/j.cose.2013.04.004

Wallischeck, E. Y. (2013). *ICS Security in Maritime Transportation: A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure* Retrieved from http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf

Appendix

Survey

The appendix in this thesis contains the survey issued to both shipping companies and equipment suppliers in the maritime sector. The attached survey was extracted from the SurveyMonkey platform to PDF format; the PDF was further converted to the PNG picture format. The survey was issued to respondents in a graphical manner as shown below, with exceptions; text that originally was found in the dropdown menus were excluded due to the non compatible format of SurveyMonkey application and image file; any colors present in the original survey have been removed; Question number was added to more easily refer to different questions.



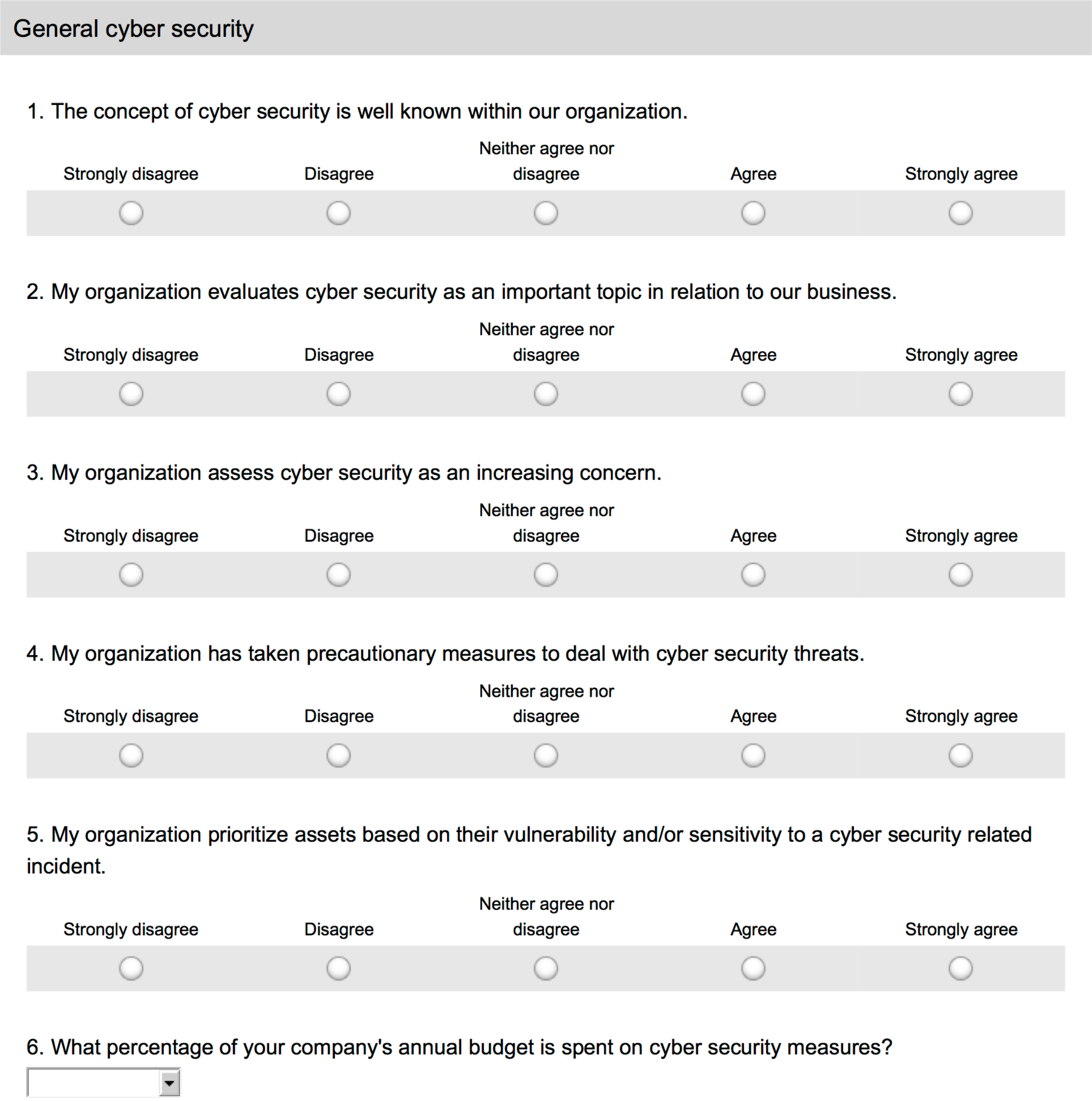
Welcome to the survey "Self assessment of cyber security".

Thank you for participating in this survey. Your feedback is important and highly appreciated.
This survey is a part of a master thesis with the title "An assessment of cyber security awareness in the Norwegian maritime sector" and is aimed at helping the industry, as well as learning institutions improve and understand the situation surrounding cyber security in the Norwegian maritime sector now and in the future.

To ensure a common understanding of the questions asked, two definitions of cyber security is presented:
The first definition is ”Protection of data and systems connected to the Internet.”, from Cyber Security Strategy for Norway by the Norwegian Ministries.
The second definition is “preservation of confidentiality, integrity and availability of information in the Cyberspace”, from ISO/IEC 27032:2012.

In this survey, assets are categorized as either Information assets or physical/non-information assets. Information assets include information that has value to your company, stored or transmitted with the use of ICT technology. Physical/non-information assets include physical assets accessible through ICT technology. For the equipment suppliers physical/non-information assets are limited to equipment/systems that is or will be installed on ships/vessels.
For ship owners/operators/management, the actual ships/vessels with its equipment/systems that is accessible through ICT are considered physical/non-information assets. Physical/non-information assets can include but is not limited to; remote management systems, control systems, SCADA, telecom equipment, navigation equipment, information equipment, AIS, propulsion technology, safety systems, cargo handling equipment, mooring equipment, power management, ballast water treatment etc.
Threats are in this survey classified as either internal or external.
Internal refers to whether a cyber security incident originates from within the organization's network.
External refers to if the cyber security incident is conducted from outside the organization's network (ie. from internet).

The survey starts off with some general questions on cyber security. Based on what kind of organization/company you are representing the survey directs you to a section specifically aimed at either Ship owners/operators/management, or equipment suppliers. The second half of the survey is common for all participants, and is divided into four different parts. Part one and two concerns protection of information assets within the organization. Part three and four deals with protection of physical/non-information assets.



General cyber security

1. The concept of cyber security is well known within our organization.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

2. My organization evaluates cyber security as an important topic in relation to our business.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

3. My organization assess cyber security as an increasing concern.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

4. My organization has taken precautionary measures to deal with cyber security threats.

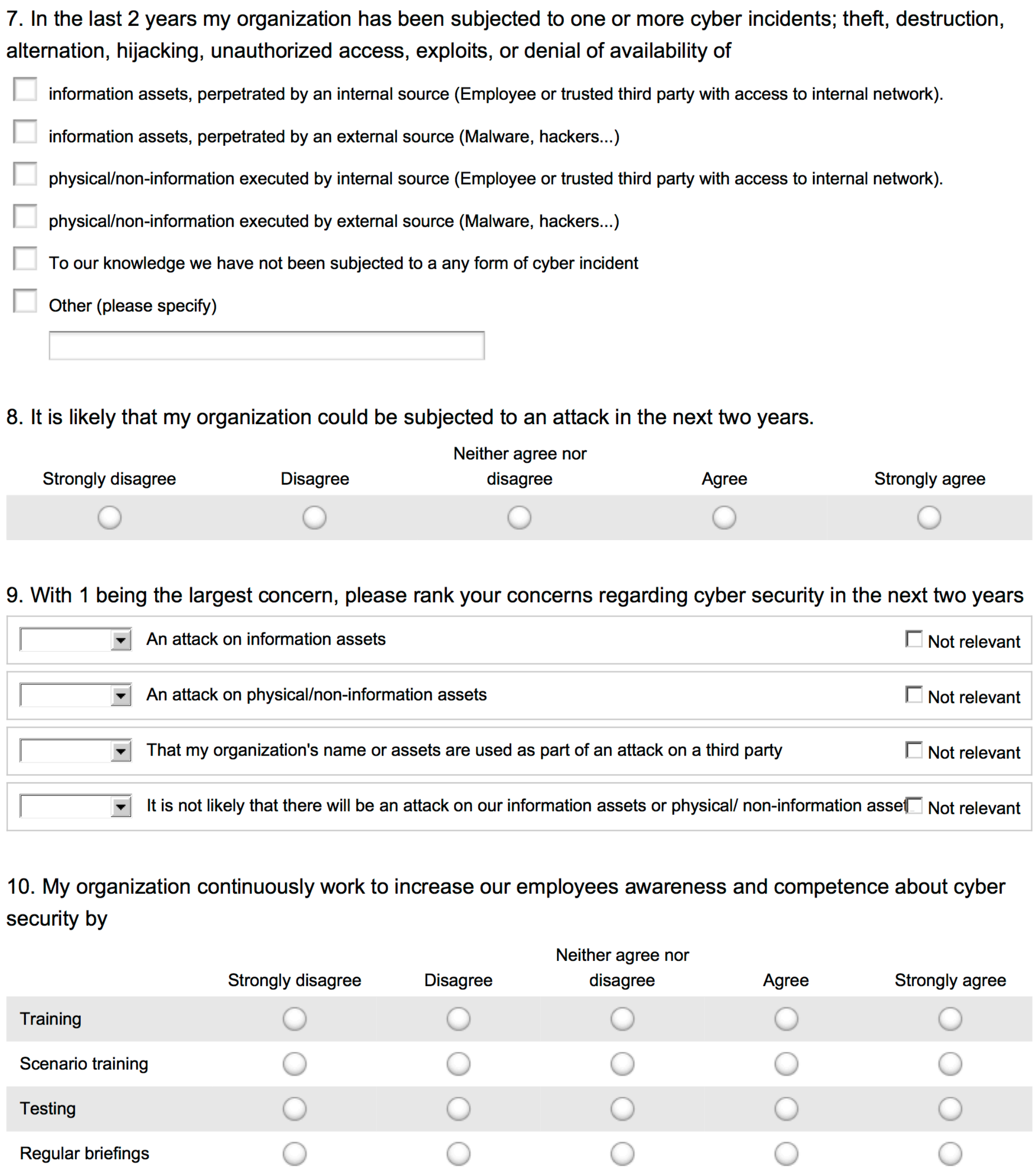
Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

5. My organization prioritize assets based on their vulnerability and/or sensitivity to a cyber security related incident.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

6. What percentage of your company's annual budget is spent on cyber security measures?

▼



7. In the last 2 years my organization has been subjected to one or more cyber incidents; theft, destruction, alternation, hijacking, unauthorized access, exploits, or denial of availability of

- □ information assets, perpetrated by an internal source (Employee or trusted third party with access to internal network).
- □ information assets, perpetrated by an external source (Malware, hackers...)
- □ physical/non-information executed by internal source (Employee or trusted third party with access to internal network).
- □ physical/non-information executed by external source (Malware, hackers...)
- □ To our knowledge we have not been subjected to a any form of cyber incident
- □ Other (please specify)

8. It is likely that my organization could be subjected to an attack in the next two years.

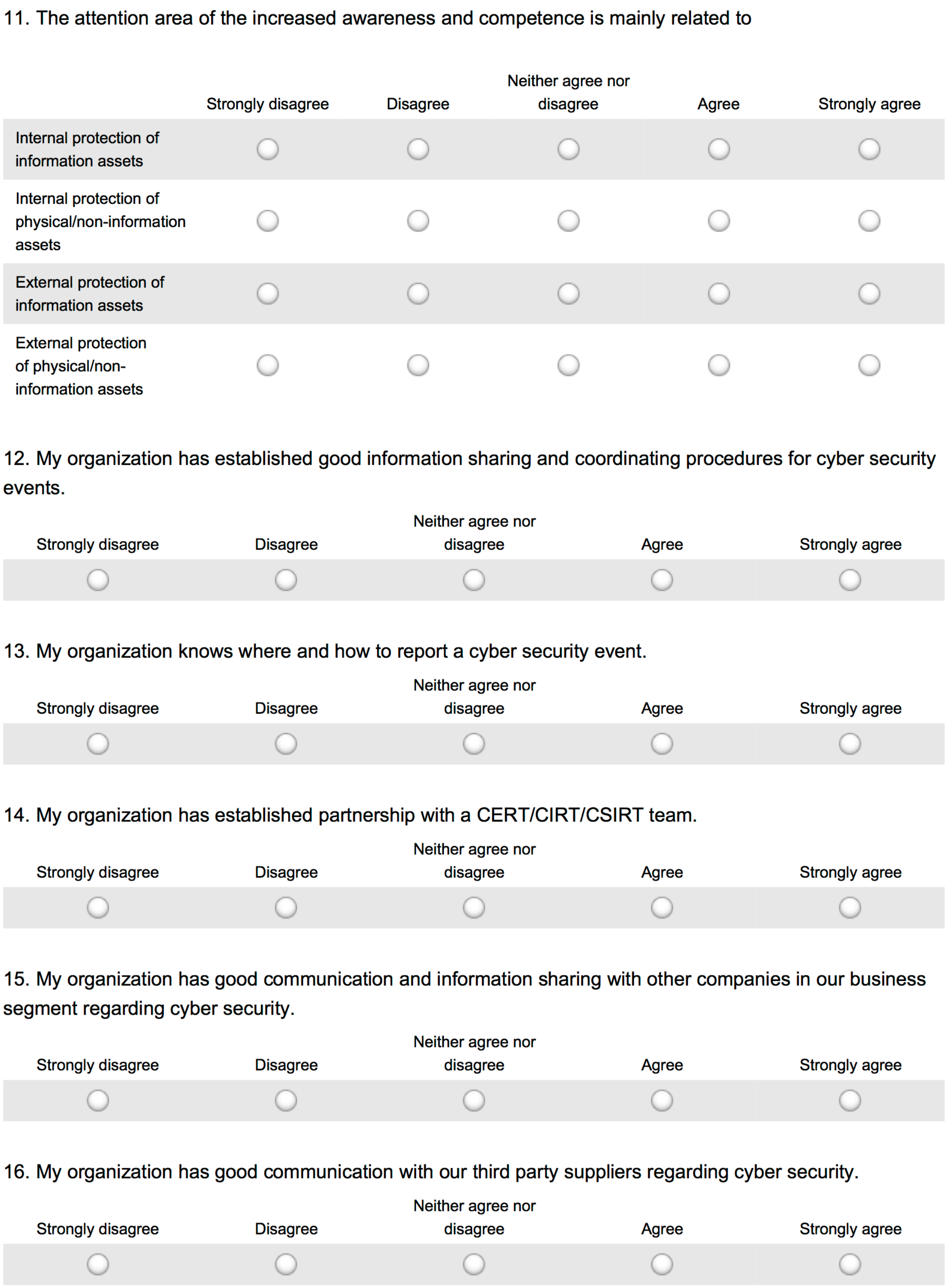
Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

9. With 1 being the largest concern, please rank your concerns regarding cyber security in the next two years

▾	An attack on information assets	□ Not relevant
▾	An attack on physical/non-information assets	□ Not relevant
▾	That my organization's name or assets are used as part of an attack on a third party	□ Not relevant
▾	It is not likely that there will be an attack on our information assets or physical/ non-information asse	□ Not relevant

10. My organization continuously work to increase our employees awareness and competence about cyber security by

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Training	○	○	○	○	○
Scenario training	○	○	○	○	○
Testing	○	○	○	○	○
Regular briefings	○	○	○	○	○



11. The attention area of the increased awareness and competence is mainly related to

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Internal protection of information assets	○	○	○	○	○
Internal protection of physical/non-information assets	○	○	○	○	○
External protection of information assets	○	○	○	○	○
External protection of physical/non-information assets	○	○	○	○	○

12. My organization has established good information sharing and coordinating procedures for cyber security events.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

13. My organization knows where and how to report a cyber security event.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

14. My organization has established partnership with a CERT/CIRT/CSIRT team.

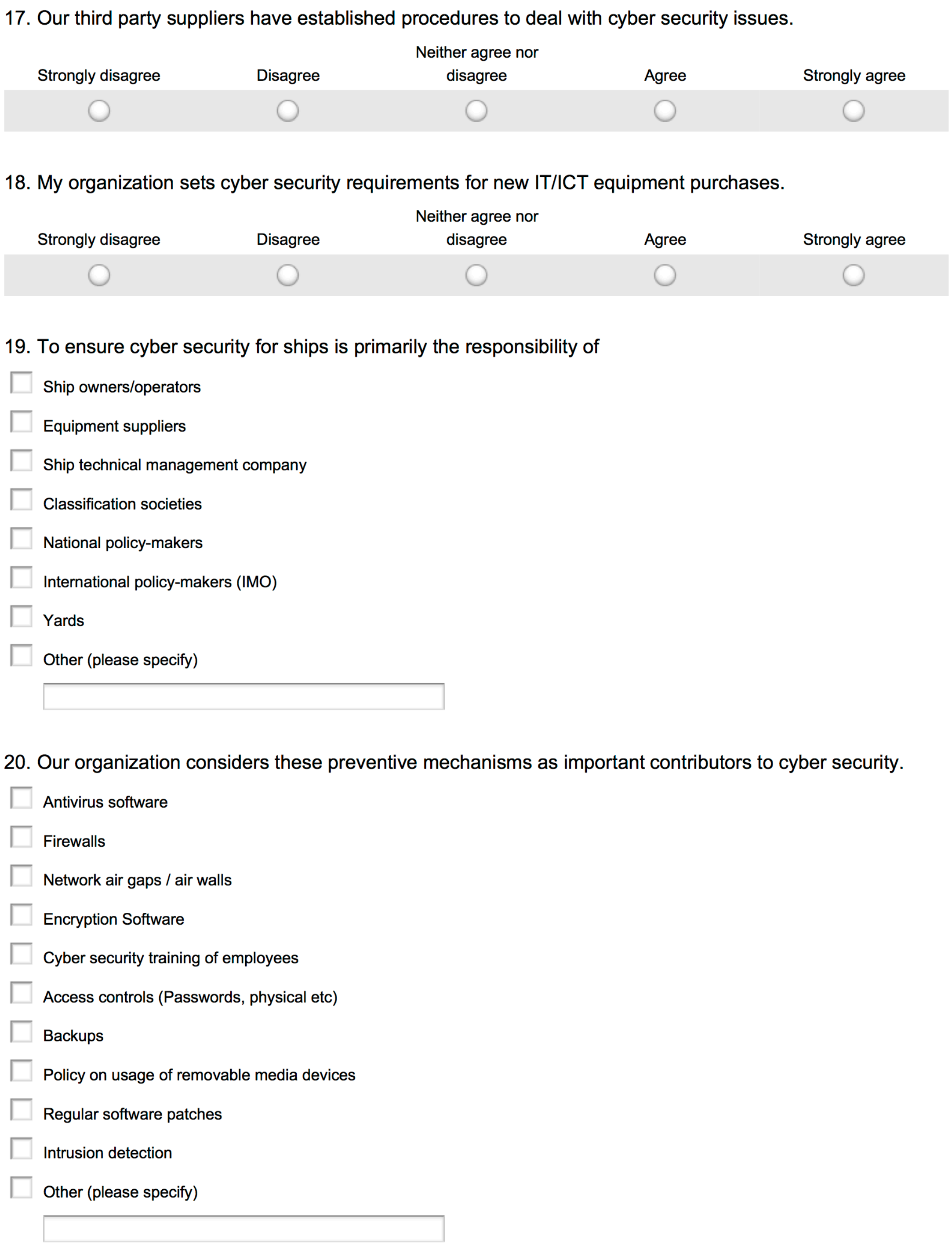
Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

15. My organization has good communication and information sharing with other companies in our business segment regarding cyber security.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

16. My organization has good communication with our third party suppliers regarding cyber security.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○



17. Our third party suppliers have established procedures to deal with cyber security issues.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

18. My organization sets cyber security requirements for new IT/ICT equipment purchases.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

19. To ensure cyber security for ships is primarily the responsibility of

□ Ship owners/operators

□ Equipment suppliers

□ Ship technical management company

□ Classification societies

□ National policy-makers

□ International policy-makers (IMO)

□ Yards

□ Other (please specify)

20. Our organization considers these preventive mechanisms as important contributors to cyber security.

□ Antivirus software

□ Firewalls

□ Network air gaps / air walls

□ Encryption Software

□ Cyber security training of employees

□ Access controls (Passwords, physical etc)

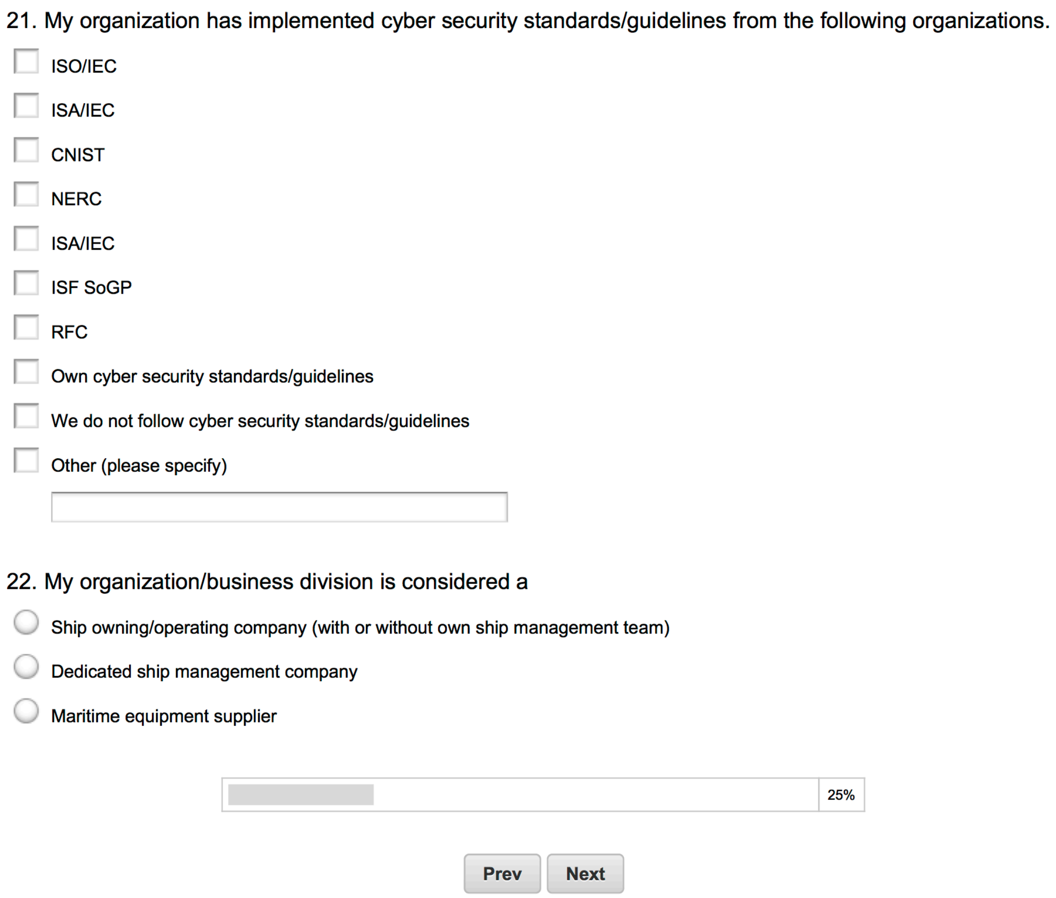
□ Backups

□ Policy on usage of removable media devices

□ Regular software patches

□ Intrusion detection

□ Other (please specify)



21. My organization has implemented cyber security standards/guidelines from the following organizations.

□ ISO/IEC

□ ISA/IEC

□ CNIST

□ NERC

□ ISA/IEC

□ ISF SoGP

□ RFC

□ Own cyber security standards/guidelines

□ We do not follow cyber security standards/guidelines

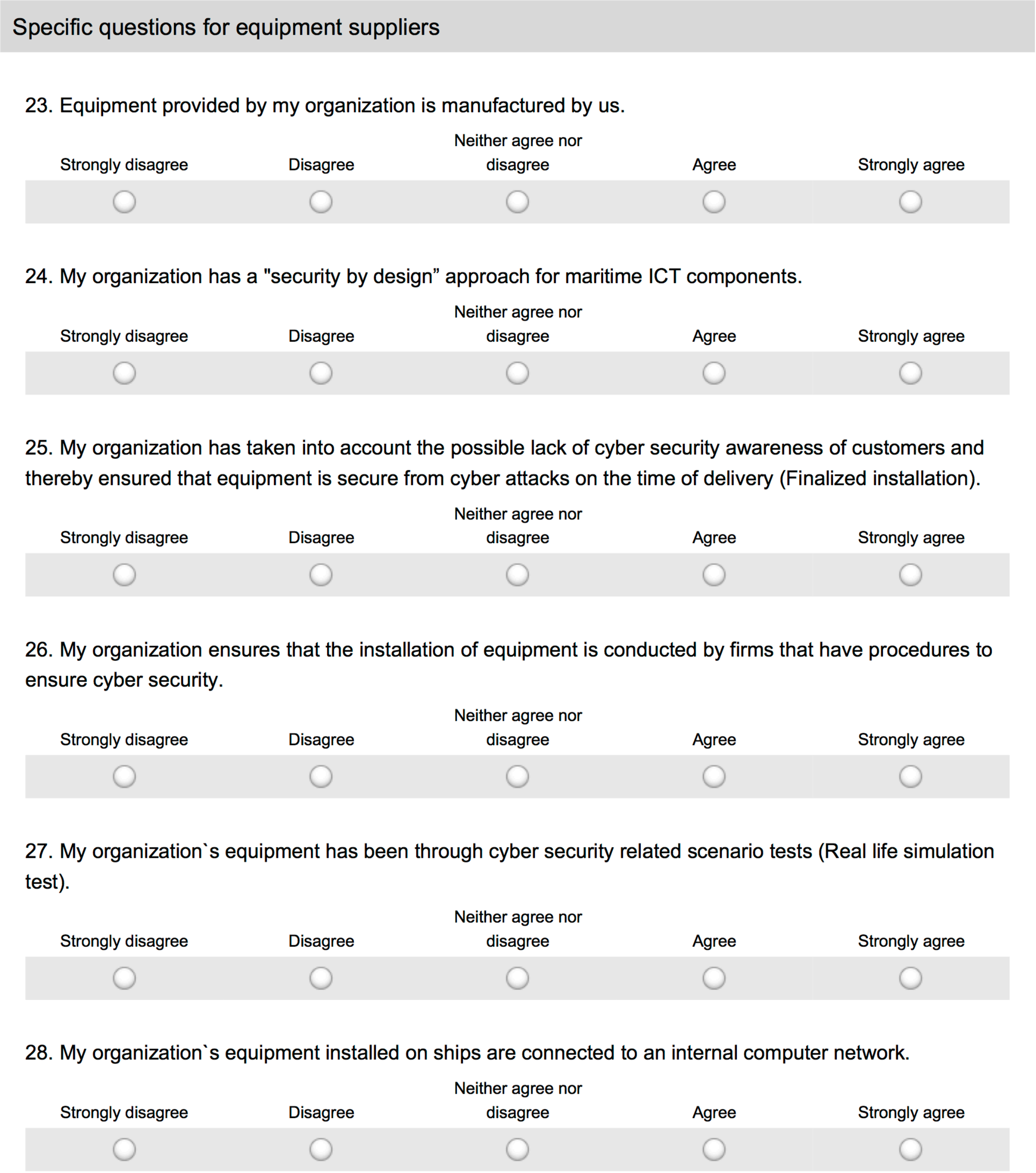
□ Other (please specify)

22. My organization/business division is considered a

○ Ship owning/operating company (with or without own ship management team)

○ Dedicated ship management company

○ Maritime equipment supplier



Specific questions for equipment suppliers

23. Equipment provided by my organization is manufactured by us.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

24. My organization has a "security by design” approach for maritime ICT components.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

25. My organization has taken into account the possible lack of cyber security awareness of customers and thereby ensured that equipment is secure from cyber attacks on the time of delivery (Finalized installation).

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

26. My organization ensures that the installation of equipment is conducted by firms that have procedures to ensure cyber security.

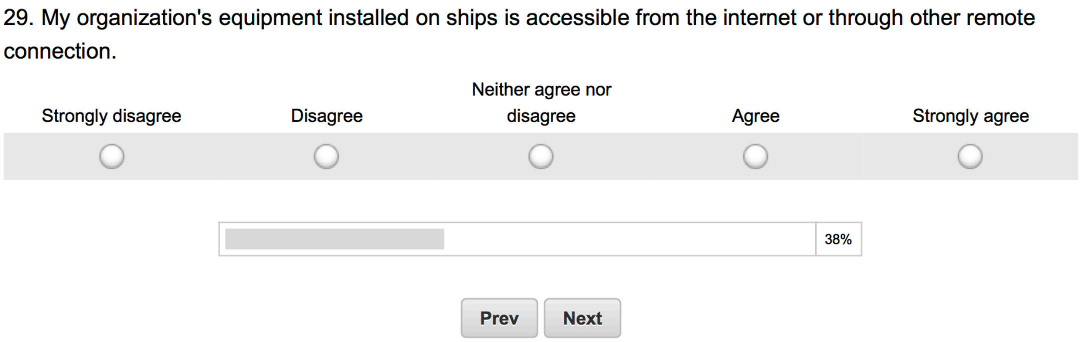
Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

27. My organization`s equipment has been through cyber security related scenario tests (Real life simulation test).

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

28. My organization`s equipment installed on ships are connected to an internal computer network.

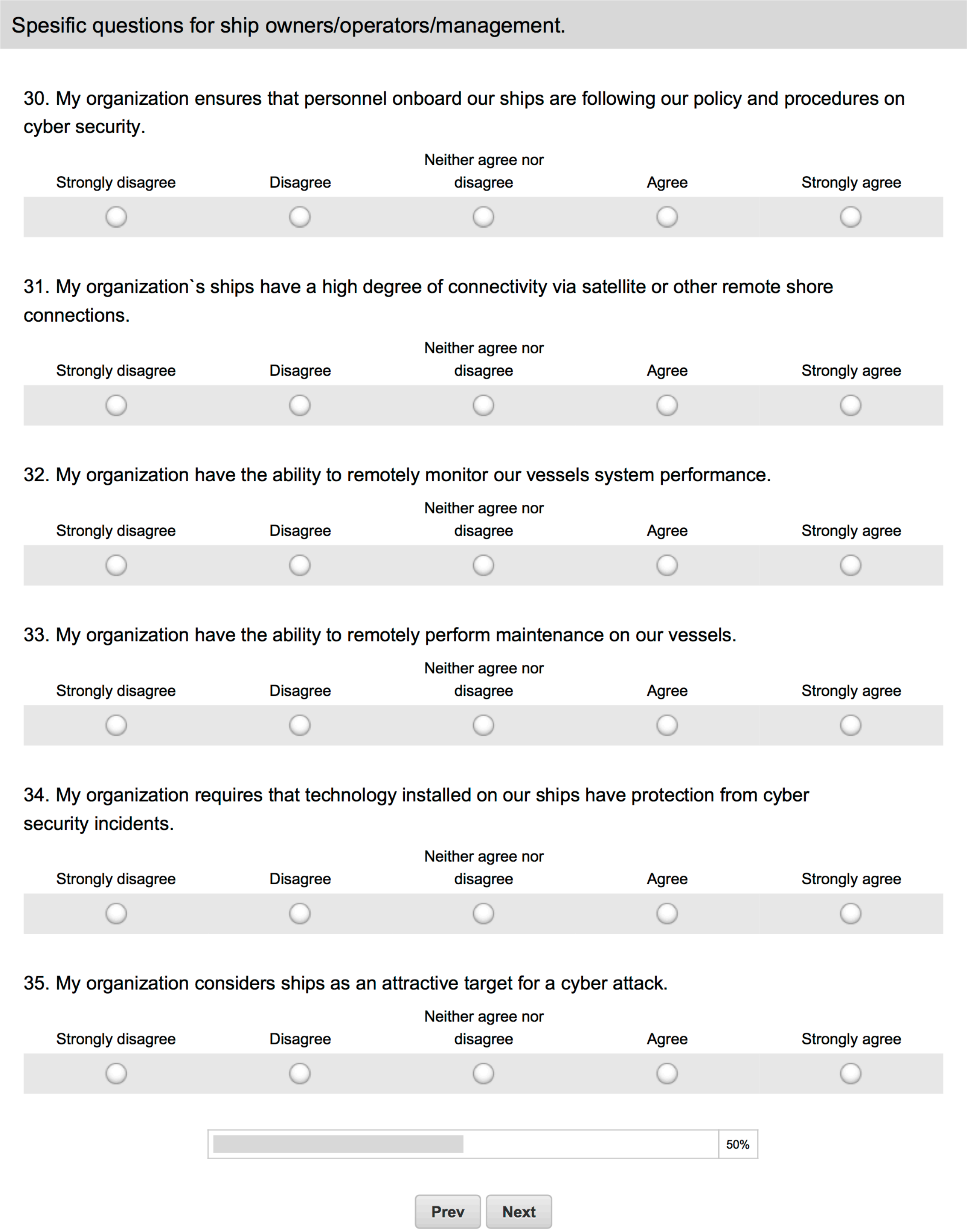
Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○



29. My organization's equipment installed on ships is accessible from the internet or through other remote connection.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

38%



Spesific questions for ship owners/operators/management.

30. My organization ensures that personnel onboard our ships are following our policy and procedures on cyber security.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

31. My organization`s ships have a high degree of connectivity via satellite or other remote shore connections.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

32. My organization have the ability to remotely monitor our vessels system performance.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

33. My organization have the ability to remotely perform maintenance on our vessels.

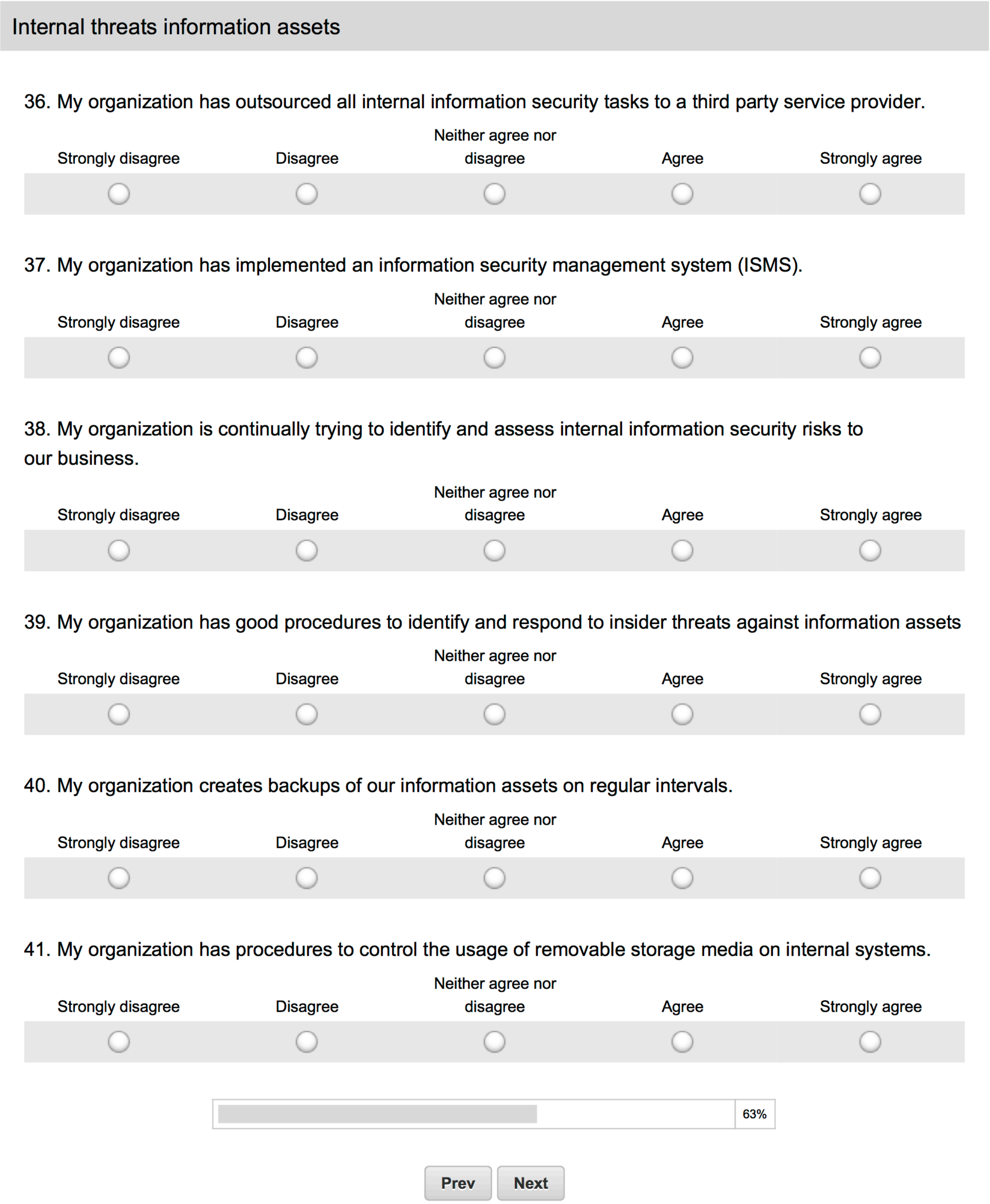
Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

34. My organization requires that technology installed on our ships have protection from cyber security incidents.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

35. My organization considers ships as an attractive target for a cyber attack.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○



Internal threats information assets

36. My organization has outsourced all internal information security tasks to a third party service provider.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

37. My organization has implemented an information security management system (ISMS).

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

38. My organization is continually trying to identify and assess internal information security risks to our business.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

39. My organization has good procedures to identify and respond to insider threats against information assets

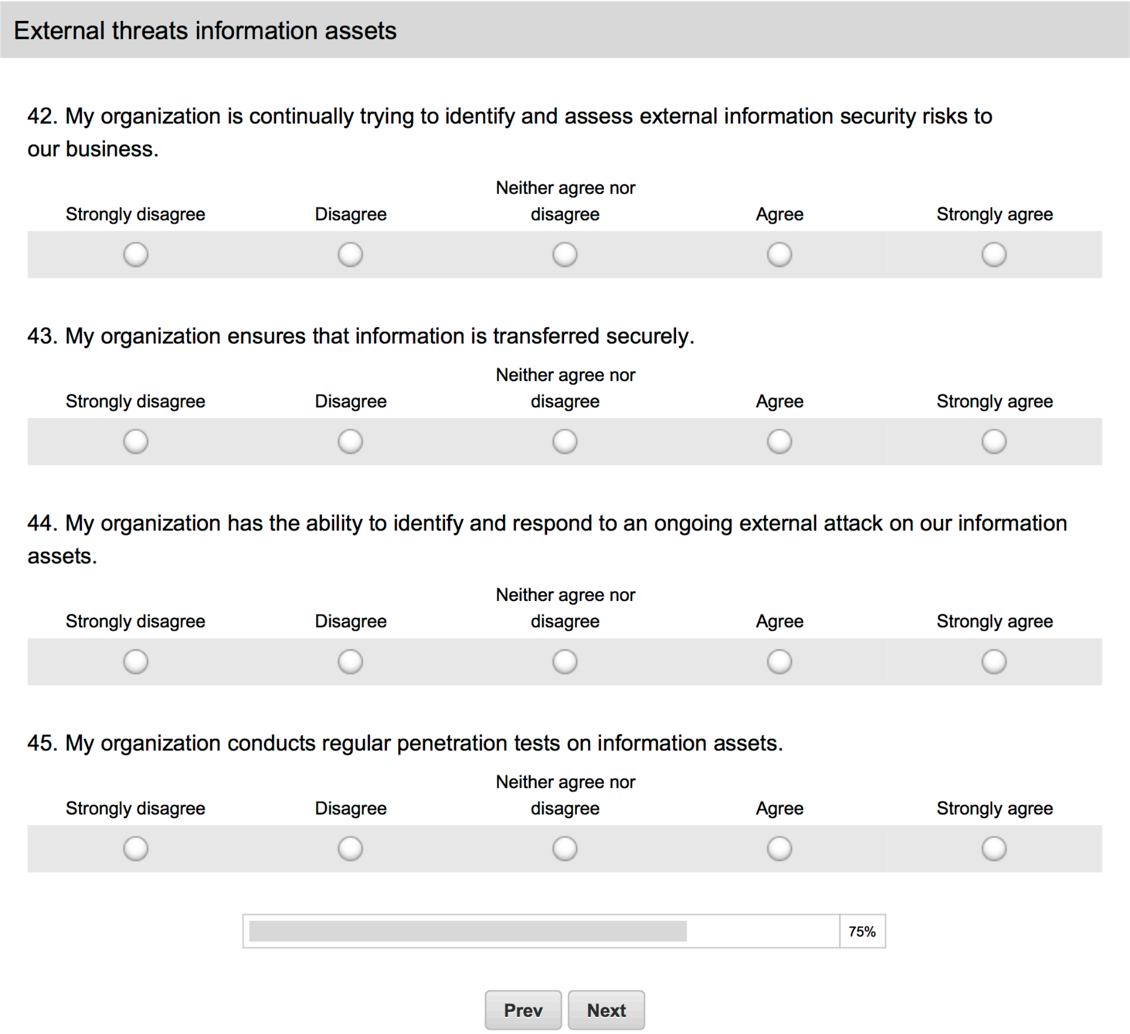
Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

40. My organization creates backups of our information assets on regular intervals.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

41. My organization has procedures to control the usage of removable storage media on internal systems.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○



External threats information assets

42. My organization is continually trying to identify and assess external information security risks to our business.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

43. My organization ensures that information is transferred securely.

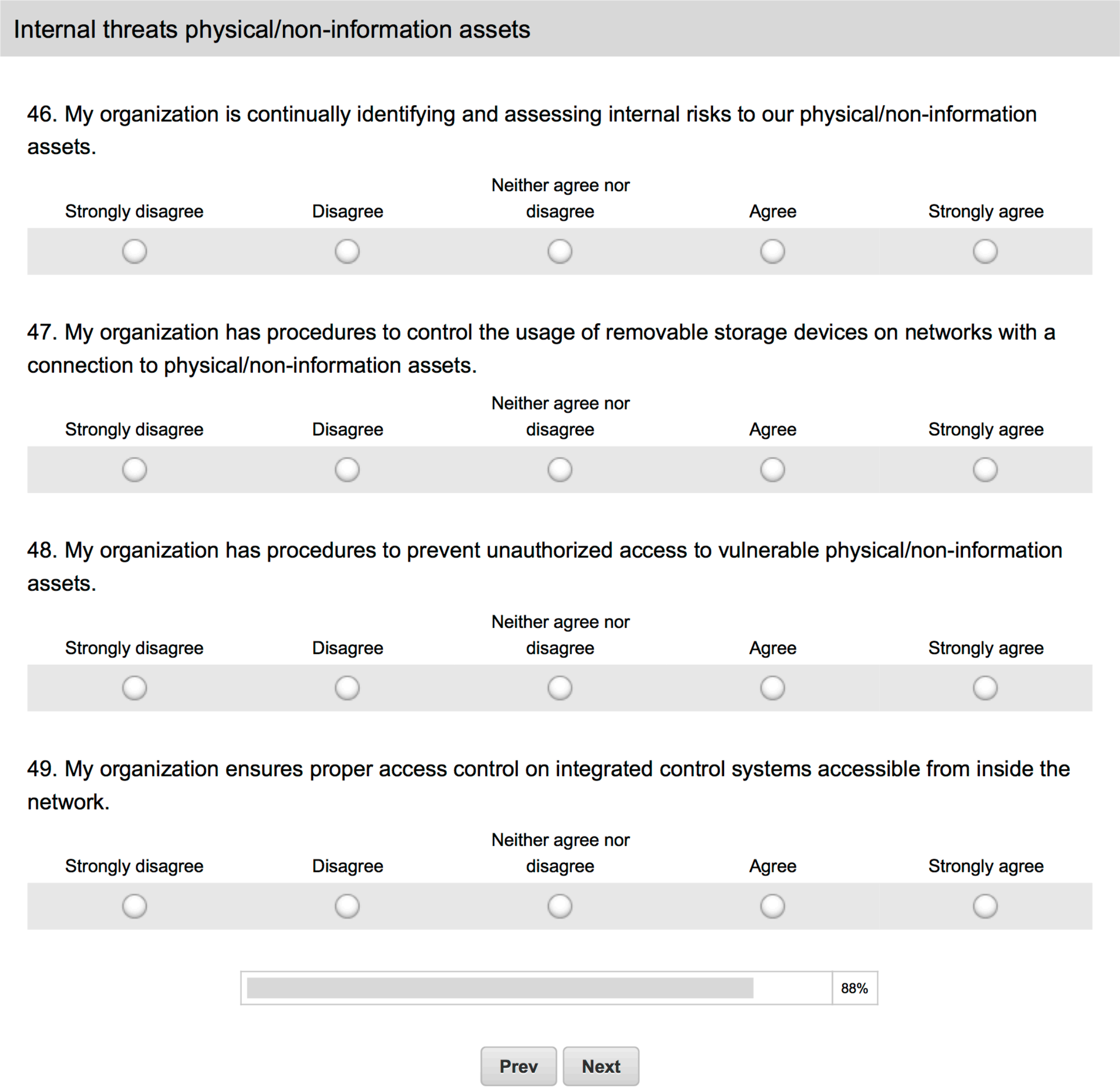
Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

44. My organization has the ability to identify and respond to an ongoing external attack on our information assets.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

45. My organization conducts regular penetration tests on information assets.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○



Internal threats physical/non-information assets

46. My organization is continually identifying and assessing internal risks to our physical/non-information assets.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

47. My organization has procedures to control the usage of removable storage devices on networks with a connection to physical/non-information assets.

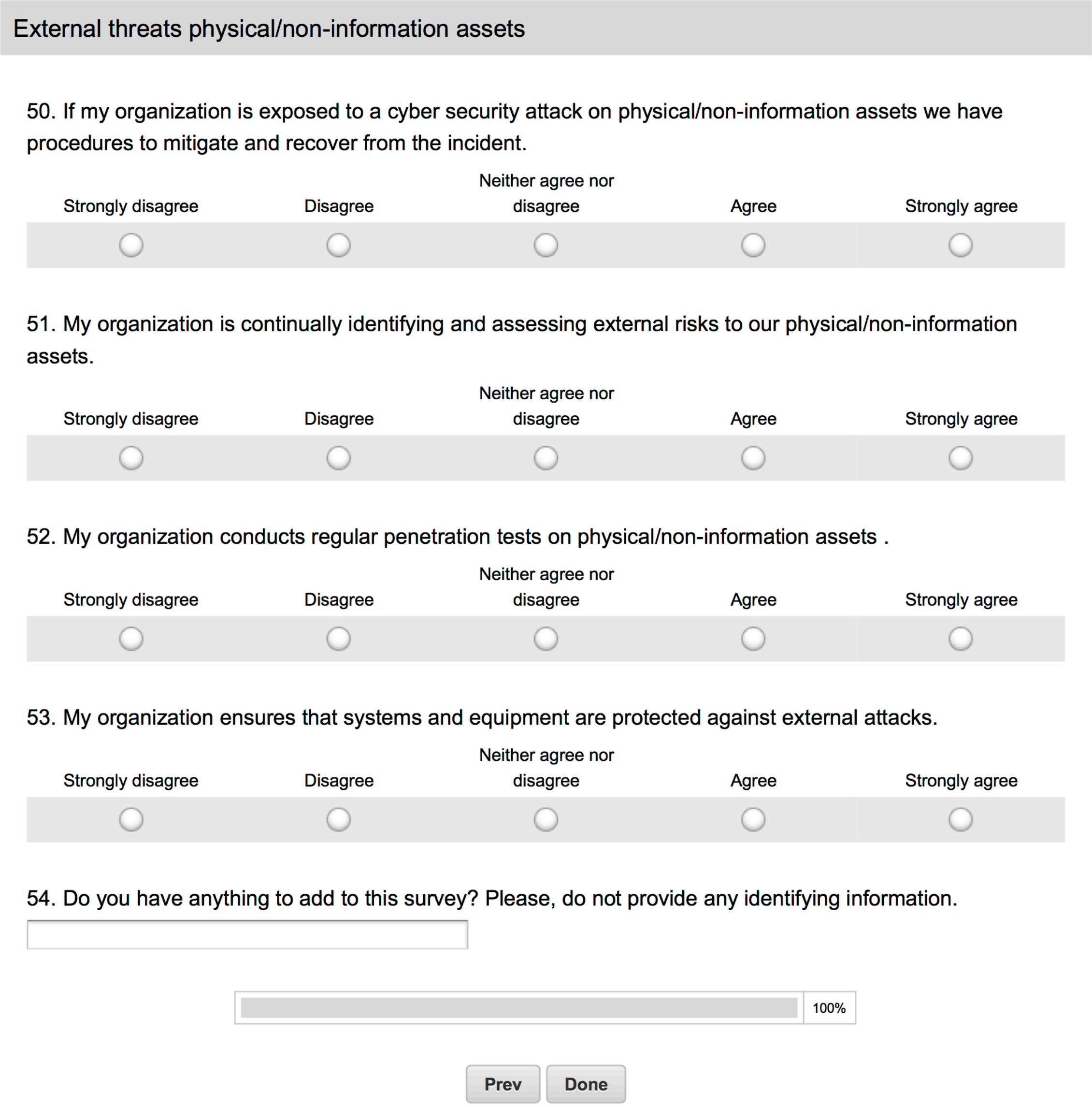
Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

48. My organization has procedures to prevent unauthorized access to vulnerable physical/non-information assets.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

49. My organization ensures proper access control on integrated control systems accessible from inside the network.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○



External threats physical/non-information assets

50. If my organization is exposed to a cyber security attack on physical/non-information assets we have procedures to mitigate and recover from the incident.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

51. My organization is continually identifying and assessing external risks to our physical/non-information assets.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

52. My organization conducts regular penetration tests on physical/non-information assets .

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

53. My organization ensures that systems and equipment are protected against external attacks.

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
○	○	○	○	○

54. Do you have anything to add to this survey? Please, do not provide any identifying information.