TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Even Langfeldt Friberg 165636IVCM

The Cyber-Insurance Market in Norway: An Empirical Study of the Supply-side and a Small Sample of the Maritime Demand-side

Master's thesis

Supervisor: Hayretdin Bahşi
PhD
Co-Supervisor: Ulrik Franke
PhD

Tallinn 2018

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Even Langfeldt Friberg 165636IVCM

Norra küberkindlustusturg: Empiiriline uurimusnõudlustest ja pakkumistest merenduse näitel

Magistritöö

Juhendaja: Hayretdin Bahşi
PhD
Abijuhendaja: Ulrik Franke
PhD

Tallinn 2018

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Even Langfeldt Friberg

23.05.2018

Abstract

This master thesis is an empirical study of the current cyber-insurance market in Norway, based on semi-structured interviews with supply- and demand-side actors. On the supply-side 6 non-marine insurance companies, 1 marine insurance company and 2 insurance intermediaries have been interviewed. On the demand-side, 3 shipping companies, 1 passenger transport company and 1 municipal agency have been interviewed, in addition to one executive manager with a background from both shipping and technology.

Findings include that the Norwegian cyber-insurance market is still the least mature of the four Nordic markets, even though the supply-side has grown significantly during the last two years. The GDPR is found to have had a modest effect on the market so far, but have been used by the supply-side as an icebreaker to discuss cyber-insurance with customers. The NIS Directive has had little or no impact on the Norwegian cyber-insurance market until now.

One should be careful not to generalize from the demand-side sample to the wider maritime industry. The findings include that the interviewees are largely lacking knowledge of cyber-insurance and that the awareness of cyber-risk to onshore IT systems has increased especially because of ransomware attacks in 2017. It is assessed that many vessel-owners are more eager to remove cyber-exclusions from traditional marine insurance policies than to pursue dedicated cyber-insurance.

Based on the findings, low adoption, ambiguity of coverage, motivations for (not) buying insurance, information-sharing, regulations and a rough characterization of the market is discussed.

This thesis is written in English and is 88 pages long, including 6 chapters, 3 figures and 2 tables.

Annotatsioon
Norra küberkindlustusturg: Empiiriline uurimus nõudlustest ja pakkumistest merenduse näitel

See magistritöö on Norra praeguse küberkindlustusturu empiiriline uurimus, mis põhineb osalise struktuuriga intervjuudel pakkumise ja nõudluse pooltega. Pakkumise poolel on intervjueeritud kuute meresõidu kindlustusseltsi, ühte merekindlustusseltsi ja kahte kindlustusvahendajat. Nõudluse poolel on intervjueeritud kolme laevafirmat, ühte reisijateveofirma ja ühte munitsipaalagentuuri. Lisaks ühte juhtivtöötajat, kellel on nii laevanduse kui ka tehnoloogia taust.

Uuringud näitavad, et Norra küberkindlustusturg on endiselt neljast Põhjamaade turust kõige vähem arenenenud, kuigi pakkumise pool on viimase kahe aasta jooksul oluliselt kasvanud. Leitakse, et GDPRil on seni olnud turul tagasihoidlik mõju, kuid on olnud tarnijate jaoks jäälõhkujaks arutada klientidega küberkindlustusest. NIS-direktiiv on osalenud Norra küberkindlustusturul siiani minimaalselt või üldsegi mitte.

Peab olema ettevaatlik, et mitte üldistada näiteid nõudluse poolt laiemalt meretööstuses. Tulemused näitavad, et intervjueeritavad on puudulike teadmistega küberkindlustusest ja teadlikus küberriskidest maismaal asuvatele IT-süsteemidele on suurenenud eelkõige lunaraharünnakute tõttu 2017. aastal. On hinnatud, et paljud laevaomanikud soovivad CL380 välja jätta traditsioonilistest merekindlustuse poliitikast kui taotleda spetsiaalset küberkindlustust.

Tulemuste põhjal on arutlusel olnud vähene vastuvõtt, katvuse ebamäärasus, kindlustuse (mitte) ostmise motivatsioon, teabe jagamine, regulatsioonid ja turu põhjalik iseloomustus.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 88 leheküljel, 6 peatükki, 3 joonist, 2 tabelit.

Acknowledgements

First and foremost, I would like to thank my dedicated supervisors, Dr Hayretdin Bahşi and Dr Ulrik Franke, for their support and helpful advice. I'm grateful for the time and effort they have both invested in my project.

I would like to thank all informants and their respective institutions for taking the time to contribute to this thesis. Also, I would like to thank my friend Vesa-Matti Tala for assisting in the process of establishing contact with informants.

List of abbreviations and terms

CL380	Institute Cyber Attack Exclusion Clause CL380
CRO	Chief risk officer
CSIRT	Computer Security Incident Response Team
EEA	European Economic Area
EFTA	European Free Trade Association
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation; Regulation (EU) 2016/679
GPS	Global Positioning System
HSEQ	Health, safety, environment and quality
HSSEQ	Health, Safety, Security, Environment and Quality
IMO	The International Maritime Organization
ISAC	Information Sharing and Analysis Centre
ISM Code	The International Safety Management Code
ISO	International Organization for Standardization
MSSP	Managed security service provider
NDPA	Norwegian Data Protection Authority
NIS	The NIS[1] Directive; Directive (EU) 2016/1148
NIST	National Institute of Standards and Technology
NorSIS	The Norwegian Center for Information Security
OECD	The Organisation for Economic Co-operation and Development
OSLSHX	OSLO Shipping Index
SME	Small and medium-sized enterprises
UN	United Nations

[1]Not to be confused with *the Norwegian International Ship register*; throughout this text *NIS* shall refer to the EU directive

Table of contents

List of figures

List of tables

1 Introduction

1.1 Motivation

Norway is regarded as the market most lagging behind of the Nordic countries regarding organisations' adoption of cyber-insurance [1, p. 136]. At the same time, it's a technologically developed country, with an estimated loss from cybercrime at 0.64% of GDP, which is above the EU average [2]. The US is the most mature market for cyber-insurance, where a survey suggests 55% of organisations have adopted this form of risk-transfer [3]. This is mainly because of a longer tradition of strict laws regarding especially protection of customer's personal information. The European GDPR [4] will take effect in Norway in the first half of 2018, and the NIS Directive [5] is likely to be transposed as the government has found the directive to be of EEA relevance and acceptable.

The maritime sector is important for the country. The Notpetya ransomware attack that affected Maersk Line in the summer of 2017 lead to losses between USD 250-300 million, according to their Q3 interim report [6]. The International Maritime Organization has decided that 'cyber risk management' be mandatory aboard ships from 2021 [7]. These are all possible drivers for increased adoption of cyber-insurance in the Norwegian market.

1.2 Objective

The objective of the thesis is to render the current situation of the Norwegian cyber-insurance market, based on the views and experiences of a representative sample of supply-side actors. In addition, views and experiences of a convenience sample of demand-side actors in the maritime industries will be included.

The intention is to contribute to the research on cyber-insurance that is of an empirical nature, supplementing that of theoretical nature that is more frequently found. Even if the recent results of [1] can be generalized to the Norwegian context, it is interesting to explore the market situation in Norway closer, as factors such as upcoming regulation can be hypothesized to affect the development of the market. The Norwegian market is also interesting in itself as it is frequently mentioned as the least mature of the rapid developing Nordic markets.

1.3 Scope

According to the definition given in section 2.3, and the industry classification suggested there, 4 of the 6 demand-side informants can be categorized as shipping companies: 3 deepsea and 1 shortsea. For the 2 remaining informants, 1 interviewee actually represents

a municipality, which are multifarious organizations. The specific informant was nevertheless included as one of the municipal undertakings is a port authority, which would belong to the broad category 'maritime services'. The interviewee is employed in a municipal agency that manages, not operates, IT and cybersecurity for the port authority. The sixth demand-side informant shall not be assigned to a specific category, but has extensive work experience from both shipping and technology.

It is clear that the sample is not large enough to be representative for the maritime industries, nor for any one sector, as discussed in section 5.8. However, it can be considered appropriate that the majority of the informants belong to the shipping company sector, as this is the group employing most people and creates the highest value of the four main maritime industry groups [8, p. 106].

The supply-side included consists of seven insurance companies, of which one is a marine insurer, one marine broker and one commercial lines broker. The informants all have a presence in Norway. The sample does not include all insurance companies that offer cyber-insurance coverage in Norway[2], but they are major actors providing their products to customers of various sizes and industries. More intermediaries could have been included. More insurers that deal solely with marine risk would have benefited the study, as there are such companies not interviewed that provide some sort of cyber-insurance coverage. Cyber-insurance is of course also bought by Norwegian organizations from international insurers without a physical presence in Norway, but that group was never considered included.

1.4 Research questions

For the demand-side, overarching research questions (RQs) to explore in this thesis are:

- RQ1: What is the awareness of, attitude to and knowledge of cyber-insurance in the Norwegian maritime sector?
- RQ2: What are the main reasons given by the maritime sector for deciding to either take up or leave out cyber-insurance as a risk management tool?
- RQ3: How do the maritime organizations perceive that the sector they are operating in is exposed to cyber risk?
- RQ4: How does the GDPR and the NIS Directive influence the maritime sector's relationship to cyber-insurance?

[2] At least one insurer not included launched their product in February 2018.

- RQ5: What is the maritime sector's attitude to information-sharing about cyber incidents?

These additional questions will be examined using the input from the supply-side:

- RQ6: How can the current market be characterized?
- RQ7: What is the supplier-side's perspectives on how the GDPR and the NIS Directive impact the cyber-insurance market?
- RQ8: What is the supply-side's experience with cyber risk awareness and cyber-insurance uptake among the general demand-side, and especially in the maritime sector?

1.5 Chapter overview

In section 2, we will first go over required background knowledge by recalling the basics of cyber-insurance and its history in Scandinavia, and give a rough sketch of the Norwegian maritime sector and what might be cyber risks for the industry. Also, we will look briefly at the GDPR which will take effect in Norway from May 2018. The NIS Directive that most probably will be implemented into Norwegian law, as Norway is part of the EEA, will be covered, as well as regulation from the UN body IMO that will apply to only parts of the maritime sector, namely shipowners that have to relate to the ISM code.

Subsequently, in section 3, I explain what we already know from earlier conducted research, and how my own attempt at research is designed. In section 4 the results of my study is emphasised, and their implications are further discussed in section 5, together with possible weaknesses of the study.

A conclusion is given in section 6, followed by a reference list and appendices.

2 Background

2.1 Basics of cyber-insurance

Cyber-insurance, also known under various other names such as IT insurance, IT crime insurance, cyber-risk insurance, cyber crime insurance etc. [9], is essentially transferring financial risk arising from the use of IT systems to a third party [10].

Risks can traditionally be managed by avoidance, reduction, acceptance and sharing. There will always be some residual cyber-risk after managing it by avoidance and reduction, and that risk can be shared—either by outsourcing the management to a security partner, by buying insurance, or both [11]. Such insurance products are apt to outsource those risks that occur with a low frequency, but where the impact is high, after implementing other means first, e.g. investing in technical security appliances [12]. Cyber-insurance products stem from the 1980s, but the discussion of the concept as a risk management tool appeared in the literature around the millennium shift [10]. Schneier argued early for the inconceivability of not investing in cyber-insurance, and portrayed it as *'[i]n the future, the computer security industry will be run by the insurance industry'* [13].

ENISA's study from 2017 [14] shows that cyber-insurance products' typical coverage are of three main categories: (a) first party loss; (b) third party loss; (c) other benefits. Figure 1 is reproduced from the report, and depicts what cyber-insurance coverage components for each category were typically found to appear in products.

Regarding cyber-risks, the same report also repeats that these are often excluded or not specifically defined in traditional liability policies. This is for instance the case within marine insurance, where the CL380 clause is a common cyber-exclusion. CL380 is more formally known as the 'Institute Cyber Attack Exclusion Clause CL380'[3]. As [15] points out, for the CL380 exclusion to apply, the insurer must demonstrate that the threat-agent's intent was malicious—that there was a cyber-attack and not simply an IT malfunction—namely that e.g. the IT system, the code or process 'must be used or operated' maliciously, 'as a means for inflicting harm'. The majority of cyber-insurance products available is concentrating on covering for data breaches, [16] concludes, and *'[t]raditional lines may offer limited, if any, cover for cyber-caused perils'*. The same article emphasizes as problematic that some cyber-risks relevant for certain organizations might not be covered for by standalone cyber-insurance products.

[3] Cf. appendix 6 for its standard rendition.

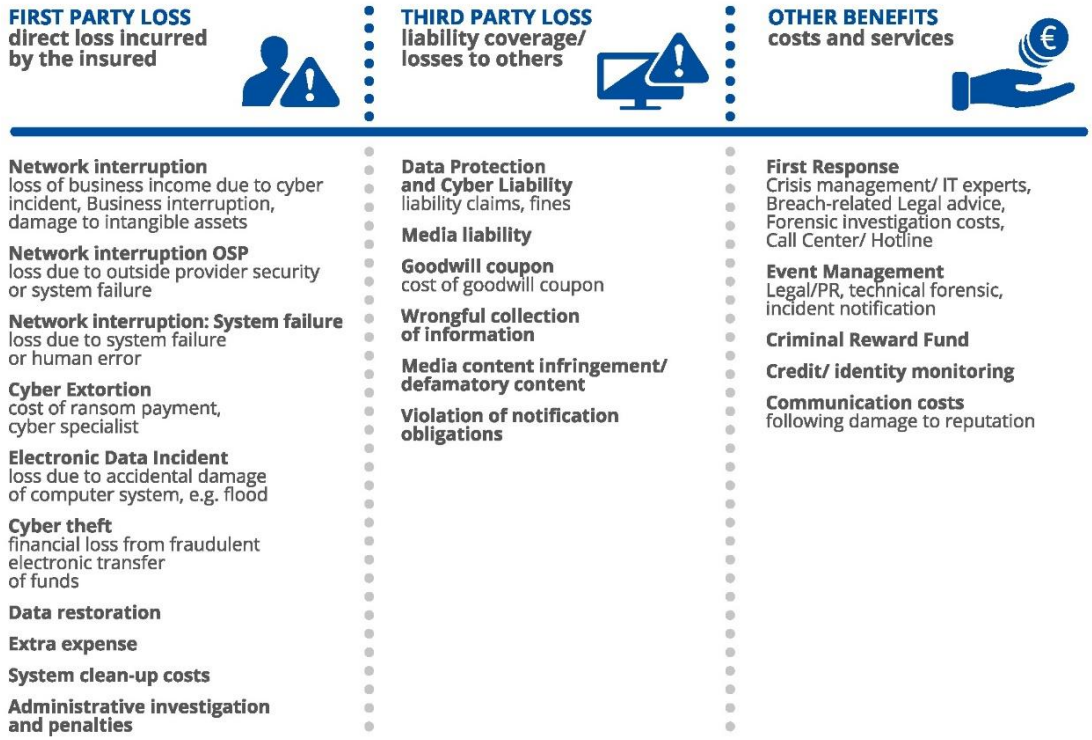

Figure 1: ENISA (2017): **'Proposed taxonomy of general cyber insurance coverage components'**, from [14, Fig. 1]

2.2 Cyber-insurance in Scandinavia

There are several studies relevant to this thesis project. Especially the independent research project *InSecurance* [17] financed by the research organization SINTEF should be mentioned.

An article published in 2016 [18] took the insurance companies' perspective, and is based on interviews conducted in 2015 with a very limited number of key insurance companies operating in the Norwegian market that offered cyber-insurance coverage at the time being, together with knowledge from literature reviews. Input from other relevant actors on the insurance-side, such as that from brokers or third-party risk assessors, were not considered. The objective of that paper was to learn what were the insurance companies' challenges and practices on assessing their customers' cyber-risk. The companies did not give 'any clear priorities on which risk factors they consider most important' [18, p. 7]. However, basic figures on the potential customer, such as annual revenue, size and sector, obviously is considered. *'A broad range of factors (e.g. based on the ISO/IEC 27001 standard [...]'* were addressed as risk factors. Catastrophic risk, i.e. 'risk of incidents which impact the majority of their customers at the same time', was a concern for the insurers, but the interviews gave no answers to how those insurers 'understand and

address such risk'.

Some constraints for the insurance companies are identified: it is difficult for them to keep up with the cybersecurity field; it can be difficult to get access to accurate data and statistics; and the insurance companies need efficient sales, customer risk estimation and adoption processes to spread the risk among more customers.

The paper concludes with proposing two approaches for cyber-insurance companies to have more efficient and systematic analysis of the risk: 'building reuseable sector-specific risk models and collaborating with MSSPs'.

Belonging to the same research project is an article [19] published in 2017 which studies the demand-side of the cyber-insurance market. This is a qualitative study, building on interviews with representatives from 10 organizations in different sectors of the Norwegian economy, 'such as finance, media, retail, critical infrastructure and IT' [19, p. 91]. 1 of these organizations had taken up cyber-insurance coverage; 2 were still in the consideration phase; 3 had concluded the consideration phase with deciding not to take up such coverage. The remaining 4 organizations had not been in a phase of considering cyber-insurance. The main objective of the study was to explore what the customer-side organizations consider to be the 'main uncertainty factors in the consideration phase' [19, p. 90] (i.e. of possibly acquiring cyber-insurance) and how those uncertainties can be reduced.

The study found that coverage and limits were the principal factors in arousing organizations' interest in cyber-insurance products, and not price [19, p. 92]. There was a unison agreement among the organizations that the rationale behind a cyber-insurance product should be to cover for incidents of a catastrophic nature, those that lead to severe consequences but occur with low probability. There was however an understanding that the indemnity limits set by today's products are too low to cover for exactly that kind of incidents. Additionally, several organizations perceived that reputation loss is seldom covered, and this might make cyber-insurance less interesting to reduce the threat of loss of market position.

This study also presents the organizations' opinions on the consideration phase: The cyber risk assessment that they in most cases conduct as a first step 'does not seem to be enough to serve as a foundation for making decisions on whether or not to buy cyber coverage' [19, p. 93]. It is also recounted that organization's insurance personnel tend to be insufficiently knowledgeable about cyber security and thus need more support from both brokers and their own organization's internal IT department. Likewise, there was an experience among parts of the interviewees that the insurance-side itself lacked expertise in cyber security and IT.

To reduce the uncertainties, the article authors emphasize the importance of the ne-

gotiation phase, used for tailoring a standard product to specific coverage and price establishment, since 'such policies are not standard products, but a result of a negotiation between the insuree and the insurer'.

To close insurance gaps, the insured should understand what are insurable and non-insurable risks [19, p. 96]. It is also recommended that a company-specific risk profile be prepared, so it can be used 'to compare expected threat exposure with what the policy offers to cover'.

Further, the same article also features a checklist of cyber-insurance exclusions, compiled from two reports, that organizations that are reviewing their existing and potential policies should think about [19, p. 97]. Finally, the authors suggest that an organization in a negotiation phase with an insurance company about cyber-insurance should clarify 'what kind of costs are covered for different types of incidents, and check these caps' [19, p. 98].

The authors conclude that they have identified uncertainty factors in cyber-insurance for the demand-side, and that these have influenced the organizations' adoption and confidence in the product. They also assert that those of the interviewed organizations that had considered, but not taken up, cyber-insurance, still benefited from having been through that phase in terms of raised awareness of cyber security especially among management, but also across the organization.

A highly relevant qualitative, empirical study not part of the abovementioned project, is that of Franke [1], which is based on semi-structured interviews with the Swedish supply-side, and contributes a characterization of the Swedish cyber-insurance market. The literature is dominated of theoretical works on cyber-insurance, and this study contributes 'knowledge about actual market practices' [1, p. 132]. 10 insurance companies, 2 re-insurance companies and 3 insurance intermediaries were interviewed in the autumn of 2016, and the interviewees represent 'essentially all companies selling cyber insurance on the Swedish market' [1, p. 130].

The findings include information on the coverage offered by the insurance-side, the segmentation of the market, what form the underwriting process takes, and how premiums are determined. Figures detailing the anonymized insurance companies' number of customers, number of annual claims, the typical customer turnover and the typical indemnity limit are given.

Norway is found to be somewhat behind Sweden, Denmark and Finland in organizations' uptake of cyber-insurance [1, p. 136].

2.3 The Norwegian maritime sector

Maritime industry or 'the maritime sector' is vague term, so for a definition of maritime industry we will resort to the definition given in [8, p. 36]: *'With maritime industry we refer to all organizations that own, operate, design, build, provide equipment or specialized services to all sorts of vessels and other floating units.'*

Norway is one of the world's leading maritime nations. In 2015, the Norwegian maritime industry employed approximately 100 000 people [8, p. 26], in all the country's countys [20]. The report [8, p. 24] assesses that the maritime industry is the most significant export industry in Norway after petroleum, and roughly a third of Norway's export is generated from the maritime industry.

One can further divide the maritime industry into some main groups, as suggested by [8, pp. 100-101]:

- Shipping companies: the dominating category
  - Deepsea: e.g. drybulk, tank, LNG, chemicals, container, general cargo, car transportation
  - Shortsea: e.g. domestic cargo, passenger ferries
  - Offshore: e.g. supply, construction and seismic vessels
  - Drilling and production: e.g. semi-submersible rigs, drillships
- Shipyards
- Maritime equipment
- Maritime services: the broadest category
  - Financial and legal: e.g. brokers, banks, legal services
  - Technological: e.g. classification societies, engineering
  - Port and logistics: e.g. port companies
  - Commerce: e.g. apparel retail

The core of the Norwegian maritime industry is still the shipping companies [21]. There is collaboration and mutual dependency between the different maritime actors, and the industry is one of the most knowledge-intensive and innovative in Norway [22].

2.4 Sector-specific cyber risk

Maritime organizations onshore use IT systems as any organization would, and therefore have to consider traditional cyber risks to their IT and communications systems. Maritime organizations, such as a shipping company that owns vessels, also have to consider cyber risks to their operational technology (OT). For those maritime actors that are responsible for vessels, this is essential to keep in mind. IMO's *MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management* highlights the need to be able to distinguish between IT and OT systems in paragraph 2.1.2: *'[…] Information technology systems may be thought of as focusing on the use of data as information. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes. Furthermore, the protection of information and data exchange within these systems should also be considered.'* Because of the development of technology, these IT and OT systems are increasingly being 'networked together', and also connected to the Internet [24, p. 1].

The shipping industry has a need for innovation to save money and work more efficiently. Digitalization, automation and integration mean that maritime organizations increasingly depend on electronic navigation, 'smart containers' and logistics that can be routed and scheduled in real-time: *'Until recently, ships were isolated, and the logistics process was not technologically advanced. This market is changing very quickly to digital communications and connectivity'* [25].

In the UK report *Future of the Sea: Cyber Security*, three broad cyber-attack categories for the maritime industry are identified [26, p. 7]: (a) 'attacks on enterprise and information assets'; (b) 'GPS and navigation attacks'; (c) 'advanced persistent threats'. The NotPetya malware infection that affected *A.P. Møller-Mærsk* ('the Maersk case') in the summer of 2017 [6, p. 54] led to disrupted transport operations and logistics businesses and subsequently loss of revenue, costs to restore IT systems and costs related to operations. That would be an example of a category (a) 'attack'. The 'Port of Antwerp incident' would also belong to this category: in 2013 it was discovered that threat-agents had managed to compromise the port facilities' IT system to get illegitimate access to confidential information that made it possible for drug traffickers to steal arriving containers *'before the arrival of the legitimate owner or overseer'*, as they had knowledge of containers' security and location details [27, p. 4]. The report *Future of the Sea: Cyber Security* considers that such attacks *'are usually low in sophistication'*, and that the risk associated with them is 'low to medium' considering that there is no or little physical disruption.

The report considers that category (b) attacks pose a medium to high risk, as there might be physical damage. A research article analysing how vessels can be vulnerable to counterfeit GPS signals featured a *'field experiment [that confirmed] the vulnerability analysis by demonstrating hostile control of a 65-m yacht in the Mediterranean Sea'* [28].

Category (c) attacks would originate from resourceful actors to achieve ideological goals, threatening national security. Such attacks would be associated with an especially high risk on the grounds that it would typically lead to physical damage to assets or life.

The report further emphasizes that *'[it] should be noted that evidence for the maritime threat landscape is sparse beyond the reported attacks'* [26, p. 9]. This is noteworthy, as several references on the surface web to cyber-incidents that supposedly has lead to physical damage, link to poorly documented news articles.

2.5 Forthcoming regulation

2.5.1 The General Data Protection Regulation (GDPR)

The General Data Protection Regulation [4] will take effect in the EU countries on 25 May 2018, and its focus is the protection of personal data. In Norway the regulation will take effect somewhat later the same year, because of procedures related to the constitution of the EFTA state Liechtenstein, that will delay the the EEA agreement [29].

The GDPR means that data privacy rules will be harmonized in the Union. Its aim is to protect personal data that organizations, regardless of size and sector, hold about individuals. Some essential aspects of the GDPR are described here. It is natural to emphasize that [4, Art. 32] requires of data controllers and data processors to *'ensure a level of security appropriate to the risk'* by implementing *'appropriate technical and organisational measures'*. Organizations should conduct a risk assessment of the personal data processing, and consider what type of personal data is being dealt with, to decide which measures to implement [30, p. 17].

The regulation defines a *personal data breach* as *'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'* [4, Art. 4(12)]. In case of a personal data breach, the regulation requires of data controllers and processors to generally report the incident to the supervisory authority, which in Norway will be the Norwegian Data Protection Authority (NDPA)[4], within 72 hours of becoming aware of it according to Article 33. Article 34 demands that the controller also shall communicate about the incident to the data subject, for instance a company's customer [30, p. 18].

Article 83 in the regulation describes the conditions for how the supervisory authority can impose 'administrative fines', up to 4% of an organization's annual revenue, on organizations that infringe the GDPR's requirements. An example of an infringement that could lead to a administrative fine would be an organization's or data controller's failure to report a personal data breach to the supervisory authority [30, p. 19].

[4]Nor. *Datatilsynet*

It has been expected from various holds that the GDPR will affect the cyber-insurance market in Norway, as a cyber-insurance product could contain elements that help organizations with e.g. technical expertise during an incident, and covering for costs relating to notification to data subjects about a breach. For instance, it is considered that precisely regulation that introduced data breach notification led to an increase in cyber-insurance uptake in the US [14, p. 43]. For the supply-side it would be desirable to take part in the increased amount of incident data that will be reported to supervisory authorities.

2.5.2 The NIS Directive

The Directive on security of network and information systems, the NIS Directive [5], has been adopted by the EU and must be implemented in the member states' national legislation by May 2018. The aim is to enhance the cybersecurity level in the Union [31].

The Directive is under evaluation in the EEA/EFTA countries, to which Norway belongs. However, the Norwegian Ministry of Justice and Public Security has concluded that the NIS Directive has 'EEA relevance' and is 'acceptable' [32]. The ministry further comments that 'the intention of the directive can better be taken care of by its implementation in the whole EEA rather than only in the EU'. The possibility for Norway to contribute positively and benefit from the CSIRT network was stressed as a reason to accept the directive. It is also worth noting that the ministry received 40 responses to a request for comments about the directive, and that none of the consultative bodies assessed the directive to be 'not acceptable', and that 13 bodies assessed the directive to be of 'EEA relevance'. It is regarded that Norway as a state already has in place the foundational capacities that the directive instructs the member-states to establish [33, p. 51], [32].

The NIS Directive differs from the GDPR in that it relates to loss of service instead of loss of data. Essentially, the directive will require that:

- the implementing states establish at least one CSIRT unit
- these national CSIRTs participate in a union-wide CSIRT network
- the implementing states establish a coordination group
- 'operators of essential services' implement technical and organizational measures to 'manage the risks posed to the security of network and information systems which they use in their operations', and that those operators notify a CSIRT or an authority about incidents 'having a significant impact on the continuity of the essential services they provide' [5, Art. 14]
- 'digital service providers' implement technical and organizational measures to 'manage the risks posed to the security of network and information systems which they

use in the context of offering services' and that those providers notify a CSIRT or an authority about 'any incident having a substantial impact on the provision of a service […] that they offer within the Union' [5, Art. 16]

The implementing states must create a list of 'essential operators' that belong to one of seven societal sectors that are specified in the directive's Annex II [30, p. 27]. Those operators will then be subject to the directive's obligations. Article 5 further specifies what is meant by an 'essential operator': *'(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service'*.

For maritime companies it is interesting to note that Annex II specifies 'Water transport' as a subsector of 'Transport'. Governments will have to identify 'essential operators' among:

- 'Inland, sea and coastal passenger and freight water transport companies […] not including the individual vessels operated by those companies'
- 'Managing bodies of ports […] including their port facilities […] and entities operating works and equipment contained within ports'
- 'Operators of vessel traffic services […]'

To ensure that the identified operators comply with the NIS Directive, i.e. implement security-enhancing measures and report cyber incidents, penalties will be put in place [30, p. 29]. The size of these have not been decided for Norway's case, but the Swedish government has proposed that fines should lie in the range of SEK 5000 and SEK 10 000 000 [30, p. 29]. In the Netherlands, a draft law suggests fines up to EUR 5 000 000 [34], and in the UK fines could reach to GBP 17 000 000 or 4% of global turnover [35].

It is reasonable to believe that the NIS Directive could affect the cyber-insurance market. Especially those companies that eventually will have obligations under the directive might want to consider cyber-insurance and the possibility to insure against fines, getting assistance with incident notification and technical expertise help during an incident. The supply-side might be interested in the incident data that will be reported to authorities to increase their actuarial data on cyber-incidents. Askvik points at the need for private-public cooperation to enable supply-side actors to take part in this information-sharing [30, p. 54].

2.5.3 Additions to the IMO's ISM code

The International Maritime Organization (IMO), which is a UN specialized agency that deals with issues of a technical and nautical art related to international shipping, adopted *Resolution MSC.428(98)* [7] in June 2017 which requires that cyber risk management should be addressed by shipowners' safety management systems. The resolution further 'encourages' those that have to relate to the ISM Code to 'appropriately address' cyber risks in their safety management systems *'no later than the first annual verification of the company's Document of Compliance after 1 January 2021'*.

The ISM Code is an international standard adopted by the IMO, which main purpose is to ensure 'the safe management and operation of ships and for pollution prevention' [36]. The code has been integrated into national legislation in most countries [37, p. 10]. The criteria for which vessels have to comply with the code varies slightly between national legislations. In essence, the entity that is responsible for the operation of a vessel, be it a shipowner or a charterer, must establish a safety management system according to the code. All vessels must be issued a 'safety management certificate' to comply with the code [37, p. 15].

The resolution itself does not specify how this should be done, but references *MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management* [23], which were issued earlier that year and are high-level maritime cyber risk management recommendations. Those guidelines further recommends to generally observe industry standards and best-practices, and names *The Guidelines on Cyber Security Onboard Ships* [24], the requirement standard ISO/IEC 27001 [38] and the NIST Cybersecurity Framework [39].

IMO's guidelines does not specifically mention cyber-insurance as a mean to manage cyber risk, but emphasizes in [23, par. 2.1.9] that one should take *'a number of potential control options for cyber risk management […] into consideration, including amongst others, management, operational or procedural, and technical controls'*. Major international supply-side actors have already picked up on the decision by the IMO to make cyber risk management onboard ships mandatory, exemplified by [40], so it would not be unreasonable to expect that the resolution can affect the cyber-insurance market.

3 Methodology

3.1 Research method

A qualitative research method was chosen for this thesis project. To gather the market's first-hand experiences, views and opinions, and certain figures, it was decided to conduct semi-structured interviews with relevant actors on the demand- and supply-side. The interviews were semi-structured in the sense that two sets of interview-guides were produced (cf. appendices 6 and 6) and sent to the interviewees prior to the agreed meeting. The questions were formulated in advance, but answer alternatives were not defined—the questions were open-ended.

An advantage of such open-ended questions is the interviewee's possibility to provide additional information, e.g. in the form of examples from his/her experience, or the interviewer's ability to inquire for an elaboration on the given answer. Moreover, the use of a prepared interview guide makes it possible to ensure that all interviewees belonging to the same category[5] are asked the same set of questions, which increases the reproducibilty of the interview, thus strengthening its reliability [41].

3.2 Data collection

3.2.1 Supply-side informants

The different kinds of organizations that together constitute the supply-side of the Norwegian cyber-insurance market are *insurance companies*, *re-insurers* and *insurance brokers*. An ideal study would have included all these actors.

In an attempt to swiftly establish contact with the relevant insurance companies, Finance Norway[6], an industry organization representing the Norwegian financial industry, were inquired in October 2017 for any detailed overview in of the providers of cyber-insurance products operating in the Norwegian market. The organization was also asked if they possessed any statistics on cyber-insurance. They responded with a list of insurance companies that at the time held a *liability insurance* portfolio. This was of limited use, as such a list does not necessarily reveal if the company actually offer a cyber-insurance product. Finance Norway's at the time included cyber-insurance under liability insurance, and did not possess separate statistics on the product. The employee at Finance Norway that I was in contact with recommended me to individually contact the insurance companies on the received list.

[5] Here: representing either the supply-side or the demand-side of the market
[6] Nor. *Finans Norge*

These company names were added to my spreadsheet of relevant actors, and I used the surface web to determine which insurance companies that explicitly advertised for a dedicated cyber-insurance product at the time, or for cyber-insurance coverage included in a different product.

I sent an enquiry by email to actors on the supply-side presenting my thesis project and asked if they would be willing to contribute by participating in an interview. In the early phase of the project during the autumn, I did not have an interview guide worked out and informed that this would be handed over in a later phase. Some of the insurance companies had the contact details of a designated public relations, press or communications officer published, and in those cases that became the first point of contact. In other cases I had to resort to impersonal office email addresses. In those cases I asked that my request be redirected to a relevant employee.[7]

18 demand-side actors were inquired to contribute as interviewees: of these 13 were insurance companies, 5 were insurance brokers. Interviews were conducted with 7 insurance companies and 2 insurance brokers, in total 9 demand-side actors. In addition, I had input from an insurance broker by email, with which I did not conduct an interview. The demand-side actors that I did not manage to set-up interviews with gave implicit declines, in that they did not respond to my request.

3.2.2 Demand-side informants

To establish contact with the demand-side, the publicly available member lists of the organization *Maritime Forum Norway*[8] was used as a starting point. *'Maritime Forum Norway is an interest organization which represents the entire maritime sector in Norway, with about 750 members'* [42]. Primarily, their member lists of shipping companies[9], shipyards[10] and maritime service providers[11] were used.

In addition, I presented the *Norwegian Shipowners' Association*[12] via email with my interview guide for the demand-side and asked if they had members that could contribute to my project as interviewees. The Norwegian Shipowners' Association is *'[...] a trade and employment organisation for Norwegian controlled companies within the shipping and offshore industry. The primary fields are national and international industry policies, employer issues, competence and recruitment, environmental issues and innovation in addition to safety at sea. Our members are the core and driving force in the Norwegian*

[7] Cf. appendix 6 to understand what form the typical first request to the supply-side looked like.
[8] Nor. *Maritimt Forum*
[9] Cf. http://maritimt-forum.no/om-oss/rederi/
[10] Cf. http://maritimt-forum.no/om-oss/verft/
[11] Cf. http://maritimt-forum.no/om-oss/leverandor/
[12] Nor. *Norges Rederiforbund*

maritime cluster. NSA's members employ over 55,000 seafarers and offshore workers from more than 50 different nations' [43]. I was recommended to individually approach the companies on their publicly available member list[13].

The online directory service *Proff - The Business Finder*[14], which provides information about Norwegian companies, was also used to find relevant demand-side actors to contact. The service allows for sorting of companies according to parameters such as industry, location, size and revenue. Tags used in my search include *Shipping and sea transport*[15], *Transport*, *Transport of freight and goods*[16], *Passenger transport*[17] and *Offshore services*[18]. One company can be assigned to several tags. The website of a candidate was then examined to determine whether the company was relevant, and how it could be contacted.

Relevant demand-side companies were approached in a similar approach to that outlined above for supply-side actors[19]. In many cases the email address of a press officer was available, and became the first point of contact. In other cases contact details of individuals holding the position of e.g. risk officer, health, safety, environment, quality (HSEQ) officer or member of the executive management were available. Inquires sent and responded to were logged in a spreadsheet in the same manner as when approaching the supply-side actors.

In one case a supply-side actor assisted me in establishing contact with a risk officer in a shipping company. Unfortunately it did not work out to conduct an interview with this potential demand-side actor. This is an example of an attempt at *snowball sampling* [44, p. 562]. As interviews were conducted from January 2018 onwards, interviewees were often asked at the end of the interview if they had contacts in maritime companies that could be attempted to be recruited as new interviewees, or if they had other ideas in how to establish contact with potential demand-side interviewees.

116 demand-side actors, mainly shipping companies, implicitly declined to participate as interviewees, by not responding. 24 demand-side actors explicitly declined to participate, by responding to my inquiry and occasionally expand on their decision. 6 demand-side actors agreed to an interview; 1 of these under the condition of not going into details on their specific company but instead giving expert opinions on topics in the interview guide based on many years of experience from companies in both shipping and technology.

[13] Cf. https://www.rederi.no/om-oss/medlemmer/
[14] Cf. https://www.proff.no/
[15] Nor. *Shipping og sjøtransport*
[16] Nor. *Gods- og varetransport*
[17] Nor. *Passasjertransport*
[18] Nor. *Offshoretjenester*
[19] Cf. appendix D to understand what form the typical first request to the supply-side looked like.

3.2.3 Interview situation

All but one demand-side interview was conducted face-to-face at the premises of the company of the interviewee, in the south-eastern part of Norway or in Bergen. Two supply-side interviews were conducted in Stockholm as the Norwegian office could not receive me. Also in these cases the market discussed was however the Norwegian. One interview was conducted via Skype. All interviews were conducted in Norwegian or English.

The interviewees had received the interview guide in electronic format on beforehand, but were offered a printed version when the meeting began. The interviewees were asked if they allowed me to record the conversation with an audio recorder for my subsequent transcription of the interview. This was agreed to in all cases. This allowed me to concentrate on the conversation as it was unfolding and eased the need to take notes.

After ensuring the interviewees had no more immediate questions about the interview or my project that needed resolving, I made use of the interview guide to ask the questions I had prepared. In some cases the order of questions was changed from that of the guide, or a question could not be answered. This is natural as the open-ended questions allowed for elaborate answers which sometimes lead to conversation on a related topic. After the interviews were concluded, the audio-recording was stopped and the interviewees were informed of my further process.

3.3 Analysis

3.3.1 Transcription

After the interview was concluded, the digital audio-recording was transferred to my laptop and transcribed using the software *MAXQDA 2018*. The software facilitates transcription of multimedia files by allowing a record to be played at various speeds. Segments that are difficult to interpret can easily be repeated.

3.3.2 Inferring essentials

After an interview was transcribed, MAXQDA was used to assign codes to text segments. Codes can be thought of as tags. In every interview transcript, the interview guide questions and their corresponding answers were identified and assigned a code, such as e.g. *IG-Tilbyder-02*[20] which was the code name that identifies question 2 from the supply-side interview guide. This was important, as the transcripts documents a conversation of approximately one hour's duration, and a specific question and its answer could be found in different parts of the texts.

[20]Nor. *IG-Supplier-02*

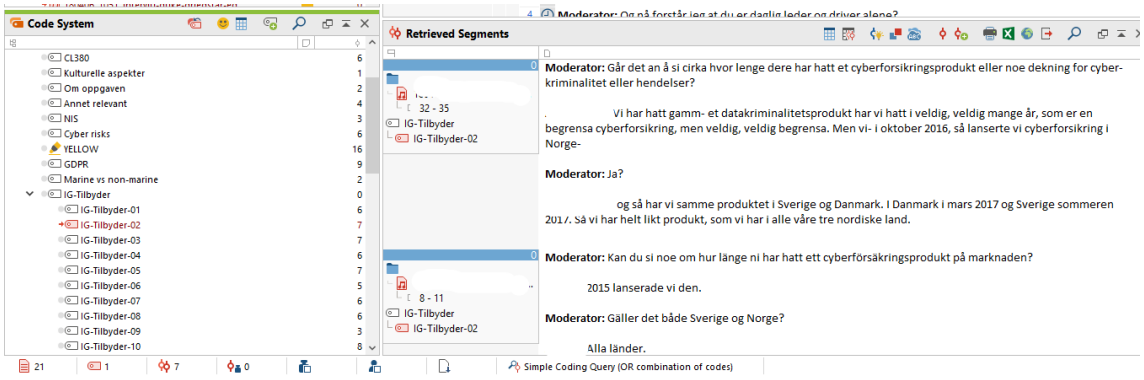

Figure 2: Example of retrieval of coded text segments in MAXQDA 2018.

Figure 2 exemplifies how all text segments assigned with the same code can be retrieved. The window to the left contains the code system, and the selected code (marked in red) retrieves all text segments assigned to that code in the window to the right from all transcripts selected. The window where relevant transcripts are selected is not shown in the figure.

In addition to codes identifying questions and answers from the interview guides, additional codes (e.g. 'NIS', 'GDPR', 'information-sharing', 'CL380', 'Maersk') where created for assigning text segments that dealt with interesting topics, but out of order with the interview guide, for instance when an elaborated answer to a question led to a separate discussion about a topic.

In connection with writing up the results, text segments were retrieved by running a code query based on the relevant interview transcripts and the codes that related to the topic, interview guide questions and research questions. The retrieved segments were then exported to a spreadsheet or a PDF file.

3.4 Ethics

Assuring that interviewees understood why I wanted to conduct the interviews was important, therefore the first email inquiry contained a presentation of myself and the project.

Meeting with interviewees face-to-face gave them the opportunity to ask any further questions. A couple of the demand-side actors asked me during the interviews if I was sponsored by e.g. a insurance company to conduct my study. As this was not the case, this could have been made even more explicit in the initial inquiry to the interviewees. An advantage of conducting the interviews face-to-face at the interviewees' workplace also gave the interviewees an opportunity to verify that I was in fact who I presented myself to be, namely a student conducting a master thesis project on cyber-insurance. I was open about my place of study, and that I had supervisors that could have confirmed my status

as a student. Before conducting the Skype interview, the interviewee wanted to verify my identity. This was solved by providing a copy of my driving licence and a copy of a document signed by the university confirming my status as a student. Both documents contained my Norwegian ID number.

The use of a audio-recorder was also chosen on the basis of being able to more precisely reproduce the information given by the interviewees.

Anonymization. It was decided to anonymize all interviewees in the final text, with no mentioning of names of individuals or companies. As Norway is a small market, especially with a limited number of supply-side actors, giving out too much information characterizing a company could make it possible to have an educated guess at which company the interviewee represents. It is doubtful that confidential information is revealed, even if some of the information given in interviews is not publicly available. The interviewees were given an opportunity to correct the interpreted information I drew from the interview transcripts into the results section of this thesis.

Sound handling of interview artefacts. After the master thesis project has come to an end, the media files on the audio recorder and my laptop relating to the project will be attempted to be securely deleted. NIST provides guidelines on how media can be sanitizated by clearing, purging or destroying [45, pp. 36,39]. As pointed out by [46], due to the functioning of certain storage mediums such as SSDs and USB flash drives, it is very hard to securely delete files from such devices. The files on my laptop are encrypted, but the audio-recorder might have to be destroyed.

Interviewee	Org. type	# customers	# claims	Coverage launch	Main market segment
IC1	insurance company	N/A	YES	2016	SME
IC2	insurance company	∼several hundred	∼15	2015	SME
IC3	insurance company	∼50	2	2012	large enterprises
IC4	insurance company	∼250	0	2017	SME
IC5	insurance company	∼5	0	2017	SME
IC6	insurance company	∼10	0	2014	large enterprises
B1	marine broker	∼5	N/A	2016	marine
B2	broker				
MIC1	marine insurance company	N/A		N/A	marine

Table 1: Overview of supply-side interviewees

Interviewee	Role	Industry	Presence	Cyber-insured	Considered CI?
C1	HSEQ Director	maritime - shipping	Multinational	NO	NO
C2	CRO	maritime - shipping - dry bulk	Multinational	NO	NO
C3	∼Insurance Director	maritime - shipping	Multinational	NO	YES
C4	∼HSEQ Director	maritime - passenger transport	Domestic	NO	NO
C5	Senior Consultant ICT	municipal agency	Domestic	NO	NO
EX1	executive management			N/A	N/A

Table 2: Overview of demand-side interviewees.

4 Results

4.1 The maritime interviewees are largely lacking knowledge of cyber-insurance, but do not reject it as a concept

In trying to address RQ1 and RQ2, especially questions 14, 15e, 16, 21, 23, 29 from the demand-side interview guide (cf. appendix 6) have been considered relevant.

Summary: None of the maritime sector organizations interviewed has taken up cyber-insurance, but one of them is currently in a process of considering cyber-insurance. None of the four maritime organizations are principally rejecting cyber-insurance as a means for their organization; one will probably take it up, three needs to learn more about the products offered. The municipal agency is more sceptical that this risk management method is apt for their particular type of organization. None of the organizations remark that the insurance-side has approached them about cyber-insurance, and one interviewee holds this as a main reason it has not been considered. Interviewee C3 remarks that the broker they are in a consideration phase with has told them that they haven't sold cyber-insurance to any shipping companies in Norway yet.

C1: C1 has not taken up cyber-insurance, and it has not yet been considered. The interviewee adds that the concept might have been mentioned, but that they lack the overall understanding of what it entails. The company has taken up insurance cover for those risks that it is more familiar with. The interviewee consider that the organization is working towards achieving a more systematic approach to information and cybersecurity than

before.

The interviewee is in favour of taking a proactive approach, and especially ensuring that the organization is complying with rules and regulations. An emphasis is also placed upon conducting risk assessments for all domains the organization is involved in, and then implementing measures. Insurance in general can be appropriate to address residual risk, the interviewee admits. The interviewee expects that the insurance-side will place requirements on customers to be confident that they are taking on acceptable risk, and that insurers will be interested in getting to know what the prospective customer has implemented of means to be proactive in regards to cyber-risk: *'So it's really not risk reducing, it's rather consequence reducing, that [insurance]'*.

The interviewee expresses in a humorous tone that *'as the world evolve, the insurance industry always comes up with something new to insure […] of which I consider cyber-insurance as yet another example.'*

In coming up with a 'main reason' of why cyber-insurance has not been considered, the interviewee explains that no actors have approached the organization trying to sell it, and that this can be interpreted as an expression of cyber-insurance being a relatively recent product. But it is emphasized that the organization has grasped that 'IT and ownership to data, etc.' are important topics.

The interviewee is unsure of whether there might be cyber-insurance coverage embedded in the policies that C1 already has signed, and that this must be examined. The interviewee places an importance of understanding the policies' exclusions. The interviewee presumes that the insurance-side has been meticulous in regards to specifying what is covered, and what is not. Should one take up cyber-insurance, it would be important feel confident that there is value in the policy when 'something happens'.

C1 does not rule out that the organization will consider cyber-insurance in the near future: *'We need to know what it [cyber-insurance] is. If you dismiss it after getting to know what it entails, that's radically different from dismissing something you don't even know.'* If that happens, the interviewee doesn't take a clear stand on whether they will proceed through a broker or directly through the insurer. Firstly, the interviewee adds, the organization needs a better understanding of their own vulnerabilities and threats.

C2: C2 has not taken up cyber-insurance. Cyber-insurance has not been discussed formally in the organization, and therefore no stand has been taken of whether to say 'yes' or 'no' for further consideration with an insurer or insurance broker. It might have been talked about informally, the interviewee adds. The interviewee comments that as an organization, they are not familiar with cyber-insurance, they have not made a study of it—still, the interviewee considers that the employee responsible for insurance probably is more informed, but that possible knowledge has not been spread in the organization.

When posed with the challenge to formulate a 'main reason' for why cyber-insurance not has been considered, the interview answers that it probably is that they are lacking a more mature understanding of the overall cyber risk scenario. *'I consider that we, as probably many more organizations, have been thinking that this is a risk that is not too pronounced with us.'* As C2 knows that it is exposed to many different risk factors, it is important for the organization to prioritize its resources towards those risk factors it assumes have the greatest potential to inflict harm. C2 has not yet identified cyber risk exposure to be urgent enough to consider cyber-insurance.

The interviewee believes that the organization will probably look closer at cyber-insurance in the near future, even if it involves simply scanning the market to understand better what solutions are being offered.

Assistance from technical expertise during a serious cyber-incident, if it could delimit the impact of an incident, and especially coverage of costs related to 'tidying up' and possibly having to recover systems back to normal operations, are mentioned as elements that could make cyber-insurance coverage attracting. The interviewee expresses that quantifying lost business in a sensible way could be challenging. Coverage of more specific costs would be useful, the interviewee adds.

The interviewee adds, as an 'unqualified', immediate concern, that a cyber-insurance policy could be overly specific on what were its valid triggers, such that in case of an emergency scenario, the organization would have invested in illusory security.

In general, it is important for C2 is to understand what a cyber-insurance policy covers, how that coverage is triggered, and how losses are quantified. Too much uncertainty on the criteria for granted coverage would make the product less appealing. *'If there is always going to be a grand discussion on what the loss has been, and what will be covered by insurance, then it makes the product less valuable, I think.'*

C3: C3 is currently in a formal consideration phase of whether or not to take up cyber-insurance. They are working with a consultancy to assess and improve their cybersecurity. The interviewee is leading the project of considering cyber-insurance, working closely with the IT department.

The organization started to consider cyber-insurance in the end of 2017, partially because the Maersk case illustrated cyber risk exposure, according to the interviewee. Experiencing an incident of cyber crime in their organization was also a contributing factor. The incident was handled in time, but it can be understood from the interviewee that it was a close call. The decision was also influenced by the consultancy's views during a meeting involving an insurer and C3's IT department.

The organization has been in contact with one insurance agent business and two insurance broker firms. They are still in contact with one of the insurance brokers, from

which they will be given several insurers' quotations later in the spring of 2018. Firstly, they will return a risk assessment questionnaire to the broker. Then further underwriting meetings will take place, where tailor-made cover will be discussed.

It is of importance to the organization, and a motivating factor to enhance, that a cyber-insurance premium will take into the account their cybersecurity level. The interviewee says the organization is eager to improve their cybersecurity 'in any room' they can improve, and to discover insurance gaps and how they can be insured. The interviewee emphasizes that a maritime organization might have to relate to two different products depending on their company structure and whether or not they own vessels: cyber-insurance for a maritime organization's commercial onshore operations, and shipboard cyber-insurance.

Some aspects of cyber-insurance is highlighted by the interviewee: coverage for business interruptions and loss of income, costs related to recovering systems after an incident and crisis management featuring a pool of technical expertise that can be brought in to delimit an incident's impact.

Since the organization has had contact with more insurance-side actors, they have been presented with two questionnaires to fill. The interviewee characterizes the insurance company's questionnaire as being 'too extensive' and including questions that the they as an organization doesn't find relevant for identifying cyber risk. The broker's questionnaire was characterized as 'good', 'simplified' and 'too the point'. The whole process, both with the broker and the consultancy is characterized as mainly sensible and 'satisfying'.

The interviewee tells me that upon asking the insurance broker, he was told that they hadn't sold cyber-insurance to any shipping companies in Norway yet, even if they had been providing cyber-insurance solutions for several years. The interviewee was however told that the broker now had meetings with several shipping companies, and this was attributed to the media coverage of the Maersk case.

On asking if one has a sense for what the consideration process is likely to end up with, the interviewee consider it highly likely—*'maybe exceeding a 90% chance'*—that the organization will decide to take up cyber-insurance. The reasoning is that the consultancy that is assisting the organization to improve their cybersecurity by implementing technical means, has expressed that there is 'no 100% security at all times', and thus there is residual risk, *'and then that risk needs to be insured'*, the interviewee adds.

C4: C4 has not taken up cyber-insurance, and has just recently become aware of the concept. The interviewee found that the online information that the insurance-side gave about the concept varied considerable in its descriptive quality, from simply confirming that they had some kind of cyber-insurance to offer, to giving a decent introduction to the concept, summarizing the overall cyber risk scenario and outlining what their policy could

cover. The interview has the first-impression of the concept being more about providing practical assistance than monetary compensation.

The interviewee believes that for most smaller organization like themselves, cyber-insurance is a new concept, and that many struggle to absorb the 'new reality' of cyber risk: *'It is easier to close the stable door when the horse is gone'*.

The interviewee has notified the general manager about the product's existence and suggested that they as an organization should keep an eye on it. The interviewee believes that they might consider cyber-insurance more thoroughly in the near future, but does not hold it likely that the organization will take it up: *'Maybe in a year or two, when our situation might be a different one.'*

C4 has until recently had minimal cyber risk exposure, the interviewee thinks. The organization's website is mentioned as the main asset exposed to cyber risk. Since their cyber risk is currently self-assessed as low, it is limited how much they would be willing to pay for a cyber-insurance policy. The organization has most of their insurances placed with a marine insurance company, and the interviewee has not examined whether that actor offers some form of cyber-insurance coverage.

C5: C5 is not a pure maritime representative. Municipalities as organizations consists in reality of a lot of different specialist environments, or sectors. One of the subunits, or municipal undertakings, of the organization is a port authority. C5's interviewee therefore offers perspectives that might not be suitable in answering RQ1 and RQ2 in terms of 'maritime organization'.

C5 has not taken up cyber-insurance, and has not considered it formally. C5's interviewee judges that there might be some main reasons why the organization has not considered cyber-insurance. The first factor is that the organization is lacking knowledge of what the supply-side is offering. The second factor, the interview considers, is that as a large organization they should be able to assess events, and manage their own incidents, as resources and processes have been put in place for the purpose of that. The organization continuously conduct risk assessments and evaluate how incidents should be handled, and practise e.g. reputation management. Additionally, the interviewee is of the belief that public sector entities in general are aware of cyber risk, partially because of requirements in law.

C5's interviewee is of the opinion that cyber-insurance might be more relevant to especially smaller organizations that completely lack in-house IT resources and the apparatus to manage incidents, supervise or understand own risk—such organizations may suffer huge financial losses from downtime in IT systems that they depend on.

4.2 Maritime organizations' awareness of cyber-risk might be lagging behind when compared to other sectors, but they're not all 'in the dark ages'

When addressing RQ3, especially questions 20, 26, 27 in the demand-side's interview guide (cf. appendix 6) are relevant.

While requesting demand-side companies to act as interviewees for this thesis project about cyber-insurance, I received the following answer from a company that owns and manages vessels for the offshore industry, which might serve as an example of the diversity of attitudes found in the maritime sector:

> *'Hei*
> *Vi er en liten shipping bedrift som er 6 mann på land og bryr os meget lite om cybersecurity. Så jeg tror ikke det er så mye vi kan bidra med der.'*
>
> *'Hello*
> *We are a small shipping company of 6 men on land and we care very little about cybersecurity. So I don't think we can contribute much there.'*[21]

C2's interviewee considers that their organization is not sufficiently, but 'to an increasing extent', aware of cyber risks. They understand that they need to relate more systematically to those risks. The organization conducted a risk analysis some months ago. The interviewee says that the organization might be most vulnerable because of the information it possesses, that might be valuable to external parties. The interviewee comments: *'The knee-jerk reaction might be that we don't possess much valuable information, but everyone says that—at the least we need to do the job of evaluating if we do.'* Financial loss caused by downtime to systems that the organization relies on to perform work, is an obvious risk that the organization needs to be more aware of. The organization has not yet started to consider the cyber risk onboard its vessels, but that has to be done at some point, the interviewee adds.

C2's interviewee emphasizes that he hasn't been thinking meticulously through what could be relevant cyber risks for the company and the wider sector. Ransomware, ID theft and variations on CEO fraud are mentioned by the interviewee as risks. However, as a shipboard cyber risk for the sector he imagines a digital hijacking of a ship, *'which would be less hazardous and maybe easier to do than a physical hijacking of a ship'.* The reasoning is that a threat agent that manages to do this could control a cargo worth potentially millions of dollars, and would have the upper hand on 'someone'. Because

[21] My free translation from Norwegian

of the high amount of transactions, and relatively high value per transaction, the sector would make an attracting victim to for-profit criminals.

C3 considers data loss (such as of contracts and documentation) and business interruption caused by 'not being able to use IT systems for some period of time' as obvious cyber risks to the maritime sector. For shipping companies the loss of data could lead to not being able to 'collect the money we are supposed to'. Keeping certain business related information confidential, such as of the 'common share' is essential. Exposure of the freight rate might lead to loss of customers.

The interviewee explains that the business email compromise [47] incident mentioned in section 4.1 was an eye-opener for the organization regarding the need to implement technical and organizational mean to enhance their cybersecurity: a malicious actor managed to compromise the email account of an employee and alter solely the payee account number of an invoice the organization intended to send a customer. The debtor detected the account number change and notified C3. The incident raised awareness and led to i.a. routine changes such as a renewed credentials policy.

The organization is aware that as a shipping company there are cyber risks for IT systems used onshore, that are relevant to all modern organizations, and cyber risks for operational systems (OT) onboard vessels, and that there are different cyber-insurance products that address them. The interviewee was aware of *The Guidelines on Cyber Security Onboard Ships* [24] that addresses OT cyber risk, but didn't recognize being familiar with the IMO decision regarding inclusion of cyber risk management into the ISM code by 2021.

EX1 points out that to say anything on the risk profile of a company in e.g. the maritime sector, one should consider both the risk that apply to all organizations, in addition to the company-specific risk.

The interviewee considers that any maritime company would think of the cyber risk coming from

1. internal employees
2. for-profit criminal individuals or organizations, *incl.* industrial espionage
3. nation states

For cyber-risk from nation states, the interviewee exemplifies with the Maersk case: *'That malware was not designed to take down Maersk, right? It was designed to take down the Ukrainian government—it's just that they [Maersk] had that application used in one of their offices, and they had a flat network structure.'*

The interviewee emphasizes that what makes the shipping industry special, *'is that many shipping companies are not at the same level of sophistication and management*

control in people, technology and process, on-board their vessels'. EX1 lists some complicating factors on-board a ship:

- slow internet connections
- inability to manage complicated IT solutions, alternatively lacking the funds to buy licences
- level of crew competency
- seldom 24/7 IT support available

This means, the interviewee continues, that the shipping companies need to (a) perform more tasks at land, (b) draw more (sensitive) data from the ships back to base, which is currently being enabled through the development of IoT solutions. Thus, IT and OT—including automation systems, engine management and control, navigation, cargo management—meet and are getting bridged. *'And **that's** the risk for the shipping industry at the moment'*, EX1 explains.

EX1 emphasizes the challenge of getting the maritime companies to understand the importance of improving their classical administrative IT skills.

When asked to imagine the course of an undesirable cyber event and potential consequences for a maritime company, the interviewee points out that the consequences will completely depend upon the nature of that event: Is it related to IT, or OT? One must also take the context into account, for instance, is the vessel's GPS signal being jammed because of an external event such as a conflict?

The interviewee knows for a fact that an increasing number of maritime companies are making use of emergency response management training (ERMT), during which cyber-related incidents are simulated and tested. These are opportunities to test hypotheses and weaknesses in technology, process and organization. This is often done in partnership with a technologically strong actor, such as a consultancy. Having established a sound partnership could be of key importance should there be an incident, the interviewee explains, as resources can be mobilized quicker. *'[...] in terms of having good partnerships: sometimes investing in preventive measures also means it's easier when you have to do reactive measures.'* Good partners to have would be insurance companies, consultancy companies, IT companies.

EX1 places an importance on

- training the maritime organization: including crew—which for a shipping company will be the first and last line of defence—the security officer, IT specialists, risk specialists, insurance specialists. An example of training the crew could be as simple

as to make them aware of, e.g., the damage a maliciously crafted USB stick could pose to a vessel if connected.

- that there are processes in place: An example of a process could be that crew always supervise an untrusted individual let onboard the vessel, to make sure that the IT system is not tampered with.
- configuring technology: e.g. disabling USB ports
- enacting policy: e.g. prohibiting USB sticks, and firing those who break the rule

The interviewee is not of the opinion that the whole maritime world *'is in the dark ages'* with regards to their understanding of cyber risk. Part of the reason is that the interviewee has experienced that more, especially major companies, are prioritizing to strengthen their executive management with individuals who have a sound digital competency. However, in EX1's experience, in the merchant shipping segment that is characterized by less complicated, open-hatch vessels, such as dry bulk, *'there is still a lot of key decision makers that are not digital natives'*. This shows in less willingness to pay the cost of for instance the cybersecure digital platforms and technical devices that are being developed and offered on the market. This reluctance to invest more in cybersecurity is also related to the downturn in a stressed shipping industry.

The interviewee regards initiatives such as the *The Guidelines on Cybersecurity Onboard Ships* [24] as a useful tool to reduce cyber-risk for the maritime sector. He is sympathetic to the idea of using cyber-insurance to share residual risk, providing it is not a substitute for following best-practices, awareness-raising, implementing technical controls, etc. EX1 also believes the cyber-insurance industry will play a pivotal role in establishing best-practices, by demanding that prospective customers are compliant with them before taking on their risk. He is less persuaded about the effectiveness of IMO's requirement to include cyber risk management in the ISM code: *'It's the UN you know, so everything takes-[forever]'*.

4.3 The maritime sector, like other industries, sees the potential of information-sharing, but anonymization is needed

All interviewees acknowledge the value of information-sharing. The four 'pure' maritime companies seem to suggest that information-sharing could be much improved, but there are some mechanisms in place. The interviewee that represents a municipality that includes a port, seems to have in place somewhat more mature information-sharing mechanisms, even if it can be improved. The external expert consulted suggest that shipping

lacks mechanisms to discuss cyber risk; businesses of most industries are careful with information-sharing because of the threat of damage to reputation; technology partners are suggested as anonymizing information-sharing actors.

It is not clear from the interview with C1 how they find that information-sharing with parties outside the organization functions today, but mentions that a CEO fraud attempt was reported to the police, and half a year later a letter from the police said that the case was dropped. However, the interviewee is clear on the need to have input from competent people, for e.g. addressing and assessing risk. The interviewee says that the organization has formed the habit of obtaining external expertise when it is needed.

C2 comments that their IT manager has a certain number of connections to other IT managers of organizations in the same sector, but that is mainly confined to Norway, and it is not a formal forum. C2 believes it is a potential for improvement of sharing information, both to heighten the risk awareness and to realize what vulnerabilities the organization can mitigate.

C3 has also reported invoice fraud to the police. Additionally, the organization reported the incident to the Norwegian Shipowner's Association as the interviewee informs that *'they have some kind of diplomatic channels to make the industry aware of risks'*. The interviewee believes it is 'very important' that the maritime sector share knowledge from incidents, so one become aware and can prepare for the risk. For any future incidents the organization might experience, the interviewee considers the Norwegian Shipowner's Association to be a relevant party to notify on a national level, but that IMO might bring attention to a issue internationally.

C4 are not aware of any detected undesirable cyber-incidents for their organization, taken that they are a small actor in the beginning of their digitalization phase. They do have a small-scale operative market cooperation with other passenger transport operators in their geographical area. They communicate about physical risk, e.g. to avoid collisions. Communicating about cyber risks has not been a topic.

C5 explains that in case of a serious incident, the municipality has quite a lot of internal resources, in addition to agreements with consultants in place, which makes it efficient to call up extra temporary workforce.

The organization does not spread information about vulnerabilities to external parties, but the interviewee considers that a planned 'municipality CSIRT' might contribute to that. Information-sharing is already happening within and between municipalities. The interviewee adds that the organization already has a cooperation with their ISP's security operations centre. The interviewee emphasizes that any municipality consists of many different specialist environments, or sectors, and that some of these sectors already have established CSIRTs: *'What might be missing, is a KommuneCERT, that works across sec-*

tors, and that might be forming, that could improve information-sharing. Because it could be better, but it is not absent.'

EX1 establishes that the shipping industry in fact has a lot of information-sharing points related to 'everything else' except cybersecurity. The interviewee points out that there is a considerable amount of mechanisms to talk about the industry, and discuss e.g. IMO regulations for chemical tankers or CO_2 reporting.

The interviewee considers that it is not the instinct of boards of directors, neither in shipping or in general, to come out publicly after an information leakage or hack with *'not half the truth, but the whole truth, and all the dirty parts of what's happened'*. To exemplify this, the interviewee mentions Sony's long silence on their Playstation credentials leakage. Maersk did 'quite a good job' to come out, but then they *'didn't have much choice, did they, because their terminals didn't work anymore'*. The interviewee perceives that there is a lot of 'lessons learned' internally of organizations, but that there isn't much knowledge-sharing at the moment, except with security expert partners the company might have. Further, the interviewee raises the idea that such security expertise might be a relevant actor to gather and anonymize experiences from organizations, and then share the knowledge.

The interviewee emphasizes that cybersecurity professionals see time and again 'that companies don't really admit it when it's gone wrong'. Even an incident that might be well tackled internally, and prevented from developing, might not be appetizing for a board to come out with, despite all the knowledge the wider industry could have gained from such openness: damage to reputation is too threatening.

Additionally the interviewee airs the idea that transparency might be better in the long run, e.g. by stating some figure of cyber-incidents in yearly reports, but *'I don't have the answer to it.'*

4.4 Insurance-side has increased during last two years; few if any claims; challenges are understanding the product and internal friction in organizations

For key numbers characterizing the supply-side interviewees, such as approximate number of customers, approximate number of claims, how long a cyber-insurance product has been offered in Norway and main target customer group, cf. table 1.

Coverage: IC5 and MIC1 are the interviewed insurance companies that stand out more pronounced from the rest in terms of coverage. IC5 emphasizes that they are in a starting phase of offering cyber-insurance coverage, and that their standard product is very limited in scope, namely covering for first party data restoration and system clean-up costs

following a cyber-attack. The interviewee however emphasizes that they can, and have, offered more comprehensive coverage upon request from the broker.

MIC1 is a mutual marine insurance company, which means they are owned jointly by their members ('customers'), several hundreds of them, Norwegian and foreign companies. They offer 'protection and indemnity' (P&I) insurance to their members, which is a marine liability insurance. MIC1 also offers a commercial hull insurance product, which is not mutual, and therefore also offered to non-members.

MIC1 does not have a dedicated cyber-insurance product on the market, but contributes as an interviewee because they're in a process of deciding how to think about cyber-insurance coverage in an increasingly digitalized maritime sector. The interviewees clarify that it as of now is out of the question to launch a cyber-insurance product comparable to that of other interviewees in this study. However, (a) their P&I insurance, *does not* rule out covering for P&I liabilities arising from a cyber-attack, since there is no express cyber exclusion in the policy (with exception of the case that the cyber-attack is categorized as an act of war or terrorism, in which other insurances than P&I would respond); (b) their hull insurance, like the majority of hull insurance policies, *does* rule out covering for damages arising from a 'malicious cyber-attack', as the policy includes the CL380 clause. The informant however inform that there are other marine insurance companies that have launched cyber-insurance products, offering to remove the CL380 clause from policies where it traditionally has been included, in addition to products more similar to the ones offered by the non-marine insurance companies included in this study.

The insurance companies offer standard cyber-insurance package solutions, and tailor-made coverage can be offered. A rough overview of the standard packages will be given, even though different conditions apply. Of the six insurance companies with a dedicated cyber-insurance product on the market, only one does not have cooperation with a consultancy to offer IT expertise first response crisis management in case of an ongoing cyber-incident. All of the six will cover costs for restoration of data, software and systems. Five covers business interruption caused by a cyber-incident. Covering for business interruption loss due to an incident at an outside service provider is less common. Communication costs following damage to reputation is covered by three out of six. Three of six can cover for the cost of a ransom payment in the case of cyber extortion.

For third party costs, data breach liabilities, including notification costs, are covered by five out of six. Four out of six emphasize that GDPR administrative fines will not be insurable.

Underwriting: Generally, questionnaires containing questions on cybersecurity, i.a. technical and organizational measures implemented, security culture, employee awareness raising etc., are an essential source of information to assess the risk of the potential cus-

tomer, and whether to offer the organization insurance or not. Questionnaires also contain fundamental questions on the company's size and business activities. In many cases the questions are of a such nature that both management and technicians need to be involved in order to answer satisfactorily.

IC1 and IC2 offer automatized underwriting online, where a customer can type in the corporate identity number and immediately receive an offer for cyber-insurance. This is subject to restrictions, so highly complex organizations, organizations operating belonging to certain high-risk industries, companies with a revenue exceeding a certain limit, etc., will have to follow a traditional approach by being individually assessed by an underwriter. IC3 and IC6 are working on developing similar solutions for 'simple', smaller-sized customers associated with lower risk.

IC5 says that for smaller organizations, very little individual underwriting is involved. The interviewee considers that for organizations having an annual turnover of less than EUR 50 000 000, the underwriting process is 'relatively simple'. In those cases a turnover-premium matrix is normally used. There is more work involved in assessing the risk profile, loss potential and sample space for larger organizations. Sometimes the insurer ask for a quotation from the London insurance market.

IC6 emphasizes that the underwriting process varies considerably in length—in working hours from a couple to more than 30—depending on the complexity of the potential customer, and whether or not tailor-made coverage is required.

Claims: IC1 confirms that there has been several claims since the product was launched in Norway, without specifying the number, and adds that in most cases costs have been covered. Some cases can be somewhat challenging in that CEO fraud is not covered in the policy.

IC2 presents the interesting fact that of approximately 30 Nordic claims, 50% have come in Norway, even though Norwegian organizations hold merely 900 out of 6000 policies in the Nordic countries.

IC3 has had 2 Norwegian claims that were both granted. The claims were related to ransomware incidents, and in both cases the first response IT assistance managed to decrypt the organizations' files without having to resort to backups, and without the insurer having to pay the ransom.

IC4 emphasizes that even though there have been no claims so far in Norway, there have been some in Sweden. Some Danish claims have been rejected, as they were related to CEO invoice fraud.

Market challenges: IC1 designates it as a challenge that many customers don't really understand why they should invest in a cyber-insurance product. IC2 answers similarly, and says that it can be difficult to have potential customers realize that all organizations

are exposed to cyber risk. Some of them have the attitude that 'this will never happen to me', and this especially relates to those organizations that still not have experienced a major cyber incident.

IC3 assesses that the first obstacle to overcome is to get the potential customer to understand what the product covers for, and sets this into relation with the fact that cyber-insurance is still a relatively novel product in Norway. The interviewee experiences that cyber-insurance is met with a certain degree of opposition from organizations' IT staff, and judges that this might be because they perceive insurance as an 'attack' on their roles, and that their work is mistrusted. The interviewee tells that they as insurers prioritize to involve both management and IT staff in meetings, as the decision of whether to take up insurance is made by management, but the input from IT staff is essential in getting to know the organization's systems and what their approach to cybersecurity is.

IC4 experiences that the main obstacle in selling cyber-insurance to customers is to make the customer understand that cyber risk poses a real threat to the organization. *'It will not happen to us […], that's the prevailing mentality'*, the interviewee assesses. The lack of a conscious attitude to cyber risk is a contributing factor to why many organizations perceive themselves to be of little interest to threat agents and 'not very vulnerable'. IC4 is of the opinion that until now many organizations have left their cybersecurity completely with their IT department or IT operations supplier, but that there is a change under way. The interviewee emphasizes his opinion that cyber risk is principally a commercial risk *'that the management, executive board and employees must take deadly seriously'*. The interviewee has experienced that several IT departments initially consider that they are competent enough to prevent and reduce the effects of a cyber-attack by themselves. Another problematic aspect is the fact that on occasions when IT departments change their attitude towards the need for insurance all round, the organization might demand an unrealistic 'coverage for everything'.

IC5 judges that especially for organizations that are not aware of any cyber-incidents having affected themselves, but solely relates to the topic from media reporting, it can be difficult to understand why one should prioritize to pay for cyber-insurance, especially if the management are consisting of 'cost-conscious' individuals. The interviewee considers that potential customers have a tendency to think that incidents is something that 'only affects the others'.

IC6 considers that the main obstacle in providing cyber-insurance is related to internal frictions and hostility between departments in the customer organizations. After first having come to a common understanding with the risk manager about the appropriateness of cyber-insurance for the organization, the company's board needs to approve an additional budget for taking it up, the interviewee adds, *'[…] and usually the budget—if it's*

granted—it's granted next year […] so the budget is closed.' IC6 is of the opinion that IT peoples' resistance towards cyber-insurance has diminished significantly recently, but that it is not unfamiliar to meet the attitude of *'So, do you think that we're doing a bad job?'*

B1 describes that it can be difficult to make the potential customer understand what are their organization's main cyber risks, and how a policy's coverage addresses that exact risk. As brokers, they call for tenders from several insurance companies, and the coverage can be tailored. Customers often questions the insurance premium they have to pay, which can vary a lot. The lack of actuarial data makes it difficult to state the reason for a premium. The different products available on the market are often communicated differently from the insurers, and that is a complicating factor the interviewee says. The broker also states the uncertainty concerning systemic risk: that possible major incidents in the future might strike several organizations simultaneously. The interviewee describes that some insurers have set a global limit for claims in case of a systemic incident, and that this potentially means that 'suddenly there aren't sufficiently money left', i.e. that not all affected customers can have their costs covered. This uncertainty would also apply to a product's first response component: if 'everyone' needed IT or legal expertise assistance simultaneously, then obviously some customers would feel left out.

B2 says that they as brokers so far have not been successful in selling cyber-insurance to customers. The interviewee tells that repeatedly, after meetings with clients, the response is along the lines of *'we will discuss this with our IT department'*. B2 has the feeling that many IT departments then get on the defensive and feel the need to express that they have their cybersecurity in order and do not need external parties to meddle with that.

Differences from other markets: The insurance companies that offer their product also in the other Nordic countries say that qualitatively there are minor, if any, differences between their products offered there and in Norway. There might be small differences in pricing, and since Norway is not a member of the EU there might be some minor differences in the product as not all EU legislation apply to Norway.

IC4 states that their cyber-insurance product is categorized as a property product in Norway, but a liability product in Sweden and Denmark.

IC3 is of the impression that Denmark is the most mature market in the sense that more companies take it up, followed by Sweden.

IC6 is of the understanding that the cyber-insurance concept was introduced to the Norwegian market later than in the other Nordic countries. The interviewee finds that the market is definitely behind that of Finland and Sweden. IC6, that mainly deals with larger companies as customers, says that in the Finnish case, brokers had started to talk about

cyber-insurance around 2010, so when the insurance company launched their product some years later, the market was already prepared. The interviewee adds that he believes the Norwegian market to be at a breakthrough, and that risk managers' discussion about the concept will contribute to higher uptake in the near future.

IC2 does not immediately recognize the brokers' part in preparing the Finnish market for cyber-insurance as a concept, but adds that there has existed limited cyber aspects in insurance products in Finland for many years, if not dedicated products. IC2 comments that their company's cyber-insurance has seen the most uptake in Sweden. The interviewee adds that organizations in Norway are more hesitant in taking up this type of insurance, and the interviewee is of the impression that the Norwegian demand-side does not consider that they are that exposed to cyber risks.

IC1 assesses that there might be a cultural element that can help explain why cyber-insurance is more widespread in Finland than in Norway.

It was also suggested that Norwegian organizational culture is somewhat less consensus-oriented than in the other Nordic cultures, and less hierarchical. In Norway, one individual might have more power of attorney to make an organizational decision, for instance of whether or not the organization should formally consider to take up cyber-insurance. The advantage of being less reliant upon hierarchy would be that swift decisions can be taken, but a disadvantage could be that there is a higher chance that a less optimal decision is taken since less objections are heard.

4.5 GDPR

4.5.1 Insurers consider GDPR as icebreaker, but its importance as an uptake driver will still have to show

The insurance-side is split on whether the forthcoming implementation of the GDPR has affected the adoption rate of cyber-insurance: opinions differ from it having already played a significant role, to it being less important.

IC1 believes the regulation has not been the driver behind increased adoption of their cyber-insurance product just yet, but rather media's reporting of ransomware wreaking havoc all over the world. The interviewee believes that a cyber-insurance adoption effect will show itself first after the implementation date has passed and the media highlights the very first companies that will be investigated or punished for GDPR non-compliance. IC1 already offers coverage for loss of personal information and assistance in relation to that.

IC5 is of a similar opinion, and predicts that media coverage after May 2018 will drive more companies to look for cyber-insurance cover. The source also emphasizes that due to the limited number of customers that have bought or inquired for cyber-insurance

coverage from the company through a broker, to elaborate too much on their motivation would be on unsound grounds.

IC2 states that the pending regulation has contributed 'a little bit' to providing more cyber-insurance customers, but is of the opinion that there are many who don't properly understand the implications of the GDPR, because it is not the intention of a cyber-insurance to give complete coverage for the regulation. The interviewee continues, *'GDPR is primarly about how you deal with personal information, what documentation you keep, and when you are to shred information—those are the perspectives that GDPR really is about.'* The interviewee maintains that those are elements that relates more to traditional liability insurance than to cyber-insurance. In the case that one offends against personal information regulations, and one is to pay indemnity to the individual that has been stricken, *'it has nothing to do with cyber'.* A normal liability insurance and a cyber-insurance might complement each other in regards of covering for GDPR: the cyber-insurance can cover for the costs of notification. Additionally, IC2 considers that the GDPR functions well as a topic to start conversations about cyber-insurance with a customer. Customers who are taken care of by a broker have had more questions to IC2 about GDPR and the implications, larger companies have had more questions while smaller companies seem less 'worried' about the regulation's implications.

B1 remarks that even though most organizations keep information about their customers or employees, the pending GDPR is hardly any prominent reason for considering cyber-insurance among B1's customer base, the marine sector. The broker has not experienced that the shipping companies bring the regulation up as a topic.

IC4 states that the regulation is a starting point for dialogue with the customer about cyber-insurance in general. Brokers are mentioned as being especially keen on GDPR. It has partly been a driver for uptake of cyber-insurance in the sense that it has led to meetings with customers.

The interviewee most clear on the importance of the regulation's imminent implementation is IC3: GDPR is stressed as being the number one reason why organizations are considering whether to buy cyber-insurance or not. *'One is obliged to have in place organizational and technical means after GDPR [has been implemented], and insurance can be one of those means.'* The interviewee remarks that one can often sense during discussions with companies that the enquiry about cyber-insurance comes as a result of their organization's preparatory work on GDPR, which has been started. The insurer sees the regulation as an opportunity to get more cyber-insurance customers, but has not actively tried to influence the customers except for linking the topics of GDPR and cyber-insurance at some events.

IC6 is positive that the regulative is a factor for increased adoption of cyber-insurance,

but comments that *'it is not as important or critical as one might think'.* The interviewee says that this is primarily because organizations are still focused on getting ready for the GDPR in their own merit. GDPR is also less important because of the nature of insurance: against any sort of implications, it comes at the end. First you have to be investigated by authorities because your organization is found to be in breach of the regulation. Further, insurance is limited against the GDPR because the insurability against the punitive fines is currently a greyzone in Europe, as it will differ from country to country.

4.5.2 Insurer's think fear of personal data breach is not a main reason to take up cyber-insurance

None of the interviewees consider that a main reason for customers' uptake of cyber-insurance is that they fear a data breach where personal data goes astray. IC1 comments that many customers are engaged with the question of punitive fines, see section 4.5.3. IC2 adds the opinon that customers have realized that the 1st party costs—on which European cyber-insurance traditionally has focused—are more important. IC4 supports this view, and perceives that customers are more worried about business interruption and consequential loss. The interviewee is unsure how aware the customer-side is of personal information and the protection of it.

4.5.3 Insurability question of punitive fines

IC4 emphasizes that *'punitives, or fines, the whole point of them is that you cannot insure against them, because then they will not give the effect that they are meant to have'.* The interviewee concludes that they will generally not be insurable, and that the insurance company will not be covering any possible administrative fines a customer might be issued because of breach of the GDPR's provisions.

IC1 and IC2 are aligned with IC4 in that they will not be covering such fines. IC2 adds that insurability of GDPR fines is different in different European countries. IC1's interviewee believes that a niche of worldwide-operating, foreign companies might appear that will offer to cover GDPR fines, even in Norway: *'That's the way it is in insurance, that someone comes and covers what the others won't.'*

IC3 says that the insurability of administrative GDPR fines is a 'gray area' in all of Europe. Theoretically, IC3 could cover for the fines, but the insurability depends on whether the NDPA will issue infringing organizations a 'violation fee' or a fine as a penal sanction. In the case that penal sanction fines will be issued, the interviewee assesses that they will not be insurable. IC6 aligns with IC3 on this.

4.5.4 The GDPR's influence on the product

Two insurance companies consider that the implementation will change parts of their policies in regards to covering for notification costs; the four remaining says that it doesn't affect their policies as such. Two insurers highlight that their risk assessment of customers are affected by the GDPR's implementation in Norway; the two insurers whose main market segment is larger organizations are used to regulations similar to the GDPR from other parts of the world.

IC1 comments that the implementation of the GDPR will change the risk assessment of prospective customers: smaller customers that doesn't necessarily require individual evaluation by an underwriter, will need to meet more 'standardized requirements', in the sense of complying with the specific regulation. E.g., if your organization lets a 'data processor' process personal data on your behalf, there will have to be a data processing agreement between the controller and the data processor in-place before the prospective cyber-insurance customer can be accepted.

The interviewee reasons that customers that comply with the GDPR, pose a lower risk for the insurer. The interviewee admits that there are many insurers that will demand compliance from their customers with the regulation, and that this will have an effect on the market.

The cyber-insurance product will change in coverage of notification costs arising from a data breach: Today's requirements that the Norwegian Data Protection Authority (NDPA)[22] is notified, and then third-parties are considered notified, will change into the situation that both the NDPA and affected third-parties will have to be notified, within a shorter time frame. The interviewee considers that legal position on how notification shall be carried out is unclear at the moment.

IC2 agrees with IC1 on that the cyber-insurance product will change on coverage of 3rd party liabilities, because of the GDPR's notification obligations after a privacy breach. The interviewee believes the fuzzy legal position will resolve after the first GDPR rulings will establish a precedent. IC2 comments that they have had to alter some terms slightly.

IC3 says that their cyber-insurance policies has included terms on the general concept of data protection legislation all along, and that the GDPR will sharpen the legislation in Norway, but there has been no need for the insurer to conceptually change their polices. IC3's interviewee will not rule out that the regulation might result in more claims for the insurer to handle.

IC4 believes the business community will be more secure after the directive's implementation, and that it's beneficial for the insurance companies. The cyber-insurance policy will not be changed because of GDPR's implementation.

[22] Nor. *Datatilsynet*

IC5's cyber-insurance has not been changed, and the interviewee stresses that any change to a product comes as a result of what the demand-side through the brokers are requesting.

Since IC6 operates globally, their cyber policies have from the outset taken regulatory fines into consideration, because regulations similar to the GDPR have existed since long in many parts of the world; the answer resonates with that of IC3. What the GDPR does influence for IC6 is their underwriting approach. During meetings, customers are always asked about their GDPR project preparations, and the companies that show signs of not being sufficiently prepared, will be considered more risky to cover for: *'The companies that really are on top of things, the really sophisticated risk management cultures, they have their projects for GDPR ongoing from 2013, and they still believe that they might not be fully ready. […] and then the other guys [might ask]: "Do we need a Data Protection Officer?"'*

4.5.5 Demand-side say they have been preparing for GDPR, some are concerned with reputational loss, and the GDPR has been used as a selling point for cyber-insurance

All customer interviewees have been working on getting compliant with the GDPR. Two interviewees consider that their organizations are less vulnerable to a privacy breach. Concerning the topic of regulative fines, two organizations found it important to sort out, while one interviewee finds the question less relevant. The one organization that is currently in a consideration phase of whether or not to take up cyber-insurance, states that the GDPR's implementation is part of the reason they started to consider it, and that the supply-side is using the GDPR as a selling point.

C1 says that they need to be in compliance with the GDPR and regulations generally. They are developing an integrated management system as part of their preparations. The interviewee raises the opinion that even if the requirements in the regulation might be perceived as quite clear, they still need to consider 'do we possess personal data, or do we not? According to the regulation's definitions.'

The interviewee believes that should they have had taken up cyber-insurance, it would be important to be able to show the insurer that they are compliant with regulations in order to avoid reduction of amount in any claim.

The interviewee is curious about what cyber-insurers' stands on possible insurability of regulative fines are, but considers well as important to combat the direct consequence of reputation loss in case of a privacy breach.

C2 does not consider that they are particularly vulnerable to a privacy breach, not in the same way that the interviewee considers financial institutions or private health enterprises

to be.

C2's interviewee establishes that the organization doesn't possess sensitive personal data in the same way that e.g. a retail operator would, as they don't have personal customers. For the personal data they have on employees, which would include on shipboard crew, they would be typically non-EEA citizens. The interviewee continues: 'So I don't consider that we are particularly exposed to GDPR related risk, and neither especially in the spotlight of supervisory authorities with regard to that.'

It is also emphasized that the organization has spent a considerable amount of resources on analysis of the GDPR, 'and we carry out what we feel is necessary to deal with it, but the conclusion nevertheless is that we don't consider our organization to be particularly vulnerable—the overall risk scenario is pretty lucid—seeing as we don't posses much personal data.'

C3 expresses that the organization is well-prepared for the GDPR's implementation in Norway. Since C3 operates worldwide, and i.a. employ crew from the Philippines, they already have to relate to a similar, in effect, Philippine regulation, that the interviewee characterizes as 'stricter' than the GDPR.

C3's interviewee confirms that the GDPR has been an influencing factor in the organization's decision to consider cyber-insurance. The interviewee describes that brokers and insurance companies are using the regulation as a selling point for their cyber-insurance products.

The interviewee says that personal data breaches is a risk the organization needs to consider because they posses sensitive data e.g. related to employees' workplace injuries. It is emphasized that the organization needs to have good procedures in place, follow best-practices and implement technical means to reduce the chance of being in breach of GDPR. The interviewee also explains that the organization has inquired insurance companies whether it would be possible to insure against regulatory fines, and that the answer they had was that it varies from country to country in Europe, but that regulatory fines are uninsurable in Norwegian jurisdiction. The interviewee gives voice to the thought that even if the fines would have been insurable in Norway, the fact that it varies in Europe would be problematic: 'our business is worldwide. So if one of the countries says no, then it's no. Because we operate everywhere.'

C4 are working on their project to be prepared for the GDPR's implementation. The internal group in the organization that works on it have regular meetings on protection of personal data. The interviewee expresses that it is expensive to conduct: 'GDPR, yes. Well acquainted with. Can we afford? No. Who can?' C4 is working on an internal management system that will help them to be compliant.

The interviewee has the impression that there are a lot of companies that struggle with

their GDPR preparations and has amounts of work remaining. The organization recently received the first data processing agreement from a partner organization. Further the interviewee expresses the understanding that during the first year after the implementation date, the authorities will not be especially strict on the enforcement of the regulation as long as an organization can show they are working hard to live up to the requirements: advice will be given rather than fines imposed.

The interviewee categorizes the information into groups of employees, customers and suppliers. The work regarding employees' personal data have come the furthest; remaining is that of customers and suppliers. The interviewee raises the question of how to notify third-parties in case of a privacy breach. The interviewee consider the risk highest with employees' data: Personal data on employees contains sensitive information, but will be trivial to reach out to. Customer data is typically solely credit card information, often of foreigners, so a notification process will be more problematic. That data is probably the most interesting for for-profit criminals. The interviewee assigns the lowest risk to information on suppliers that document long-term business relationships, where reaching out to affected parties would be easy.

C5 comments that the GDPR generates a lot of interest at the present time, and that it will have a direct consequence for the organization and all its subunits. The organization has worked on getting compliant with the regulation. All the units have been put under stricter demands, and it will affect how they follow up on and document their work on information security and risk management.

The topic of GDPR regulative fines is less relevant, as the interviewee doesn't believe a public administrative body such as the NDPA will issue a massive fine to e.g. a municipal enterprise: 'It's the same money'. However, the interviewee emphasizes, it's crucial for any public enterprise to be GDPR compliant, as a matter of fact, to be compliant with all regulations. To keep the organization's sound reputation is paramount.

4.6 Low awareness of the NIS Directive

4.6.1 The NIS Directive does not seem to have impacted the cyber-insurance supply-side

To address the NIS Directive part of RQ7, it appears from the conducted interviews with the supply-side that the Directive has not yet impacted the market. It has not been a topic, neither with the supply-side itself, nor are the interviewees of the impression that the customer-side sees an evident connection between cyber-insurance and the NIS Directive. The supply-side did not consider that it had changed their product policies.

IC1's interviewee dismisses that the concrete Directive has been a topic in conversa-

tions with customers, or that it has been used to e.g. communicate with customers about cyber-insurance. The interviewee adds that more generally, those customers that take new regulations that aim to enhance cybersecurity into account, will be regarded as 'more secure' than those that don't: *'It will be easier to undertake that risk and say: 'We will help you. You have done what's up to you, and if still something should happen to you, we will help you."* IC1 also adds that the Directive might be relevant depending on which customers one decides to engage with.

IC2 does not have the impression that the NIS Directive affects customers' interest in cyber-insurance. However, the interviewee considers that typical organizations that will have to relate to the directive are typically larger actors in critical infrastructure, and do not belong in the product's target group. Such organizations are generally not customers of IC2. The Directive has not been analyzed or worked with, and has not been communicated about.

IC3 is aware of the Directive and especially believes it represents a great improvement from the current Norwegian incident reporting requirements. However, the interviewee keeps the impression that the NIS Directive is something organizations are less aware of; the interviewee does not believe the Directive has been considered during insurance uptake by their customers: *'it's rather the risk of consequential loss that has triggered the inquiry'*. It has also not been communicated about the legal act to their customers.

IC4 establishes that Norway already has in place much of the Directive's framework. The interviewee states that NIS has not been a topic: *'But it has not been talked about at all. We have quite a few customers in electricity, principally taken care of through brokers, but NIS has hardly been talked about.'* Additionally, the interviewee answers that the insurance company has not used resources to analyze it or communicate about it.

To the question of whether the NIS Directive has influenced customers to seek cyber-insurance coverage, the interviewee from IC5 answers that they didn't pick up that. IC5 adds that they haven't dealt with the Directive yet, but that they are prepared to act quickly should it be integrated into Norwegian legislation.

IC6's interviewee comments that the NIS Directive has not been implemented in their underwriting process yet.

B1's interviewee reports that as a broker, s/he doesn't have a particularly conscious relationship to that specific directive. The interviewee has not picked up that the shipping companies are preoccupied with the NIS Directive, or that its possible integration into legislation has been a reason for them to seek cyber-insurance cover. B1 has not communicated about it with the maritime sector. The interviewee doesn't rule out that there might be shipping companies that will be affected by the directive, but cannot comment further on that.

4.6.2 Demand-side reflections on the NIS Directive

To highlight the NIS Directive part of RQ4, especially the interviewees' answers to questions 18c and 25c in the interview guide used with the demand-side (cf. appendix 6) are of importance.

Three (C1, C3, C4) of the six interviewees from the demand-side were not previously aware of the NIS Directive. C2, C5 and EX1 are aware of it.

C4 has not used resources to look into it, but does not immediately self-identify as an essential service operator or part of critical infrastructure.

C1 will not rule out that the organization might be part of some transport value-chain that falls under the scope of the Directive. The interviewee mentions that the relevant logistics part of the organization must be part of the '*Achilles* database', that is, if they wish to be competitive as a supplier to e.g. the oil and gas industry. The interviewee explains that *'you must have an ISO certificate, you must have done this and that, there are many criteria you must satisfy, to be part of that database'*. The interviewee remarks that if an organization wants to be present in critical infrastructure markets, then it is evident that one must relate to 'those things that regulate the market'. The organization has to assess the external business context: 'And that means the market you operate in, regulations, your customers, every actor that has practical relevance. In regards to if we could be an attractive service provider, or a supplier of products into such markets, then'.

When C2 is asked if they believe that the NIS Directive might influence their decisions on cyber-insurance, the interviewee answers negatively. 'I don't consider that we can be classified as critical for society in any way. I don't see that we're part of a value-chain critical for society, either—so no, I don't think so'. The organization has not analyzed the Directive.

C5 believes the Directive is relevant to the organization, as the interviewee sees the Directive in relation to a new law on national security that will replace the Security Act[23]. There is only a minority of the municipality's suborganizations that are subject to the Security Act. There is a different part of the municipality organization that works with the Security Act, and probably the NIS Directive, *'we have some dialogue about it, but not much'*.

EX1, that is currently part of executive management in a shipping company, but will not comment much on their specific organization, is aware of the NIS Directive, and consider it to be very important. The interviewee has prior experience from a different organization that delivered a digital product to i.a. the maritime, energy and renewables industries. That is an example of when one clearly has to follow the NIS Directive. Whether

[23] Act relating to Protective Security Services [The Security Act]: https://lovdata.no/dokument/NL/lov/1998-03-20-10

the NIS Directive is relevant to the general shipping industry, the interviewee considers that might vary and ultimately depends on what the company actually transports: *'So the world's not going to stop if we can't make cardboard boxes, I don't think'*. The interviewee further comments on his/her understanding that organizations that for instance sells or transports anything related to the military, food industry, critical infrastructure industries, certainly will be touched by the directive. However, the interviewee adds that whether an organization is directly subject to the directive or not completely decisive, but that it is of key importance to move towards best-practices in any case: *'You can wait for the legislation to hit you, but I think, just trying to move towards best-practices and existing legislation in a sensible way is going to mean that you protect yourself both in terms of risk, but also in terms of not suddenly having a big investment down the line.'* The interviewee has not spent time considering NIS for their current organization.

4.7 The supply-side's experiences with customers of varying degree of sophistication recently showing slow market more interest; Maritime demand-side reluctant to buy dedicated cyber-insurance products

In addressing RQ8, especially answers from interviewees to questions 7 in the supply-side interview guide (cf. appendix 6) are of importance.

The insurance-side consider that organizations' understanding of both cyber risk and how cyber-insurance can cover for them varies considerably, with larger organizations generally being at a more sophisticated level than smaller. This is the impression across all industry sectors, including maritime, with reservations that 'maritime supply-side interviewees' in this study are limited in number. The Norwegian demand-side has shown more interest in, if not taken up, cyber-insurance since 2017, with media reporting of ransomware attacks, and a supply-side consisting of more providers and more active brokers, seeming to be contributing factors. Maritime organizations that are e.g. vessel-owners need to take a stand on both normal, 'non-physical' cyber-insurance offered to the general market, and how to address any CL380 exclusions in their hull insurance policies.

B1, when considering the customers' consciousness of cyber risk, describes a wide spectrum. The interviewee clarifies that, as insurance brokers, they are not first and foremost cybersecurity professionals, but rather knowledgeable of the cyber-insurance market. Additionally, the interviewee remarks, they necessarily need to have an overview of what the threats are. In the least cyber-risk aware organizations, the brokers have to *'basically start from scratch, and tell them: this has happened, this is the overall picture, this is the exposure'*. At the opposite end of the spectrum are *'those that hardly can envisage themselves as threatened, those who have the complete overview'*. When meeting with e.g. the

IT departments of larger, sophisticated enterprises, B1's interviewee describes a need for them as brokers to work hard to ensure themselves that they know what they talk about and understand the maritime clients' situation.

MIC1 believes that the cyber-risk awareness among their members varies considerably, and that some are extremely aware. The interviewee continues: *'Take Maersk*[24] *for example; if they weren't conscious before, they for sure are very conscious now'.* The interviewee also acknowledges that there are also less aware shipping companies, especially smaller ones that might severely underestimate their vulnerability often because they think of themselves as small-sized organizations, or deludes themselves into thinking they are 'safe from all forms of cyber crime' simply because they e.g. have a sound policy on how to treat email originating from unknown senders. MIC1 continues *'and that sort of consciousness, or unconsciousness more rightly said, we have to put to an end.'* The other interviewee of MIC1 adds that shipping companies small and large, might think that the chance for them 'to be hit by something' is minimal, and that they might reassure themselves into thinking they are safe because they possess the latest in e.g. firewalls and other security devices. The interviewee considers that one should also have thought about what to do—e.g. by having emergency plans in place—in case one detects that some incident has in fact already occurred, to prevent the consequences to be graver than necessary. The interviewee suggests that companies should adapt to the idea that *'a talented and motivated adversary will be able to hurt your organization, in spite of all the means you have prepared to counter it'.*

MIC1 consider that they should contribute in raising awareness of cyber-risks among shipping companies. The organization has a section of their website dedicated to the topic of cybersecurity, even though they do not offer cyber-insurance coverage as of yet. One of the interviewees adds that the organization might have to increase their level of cybersecurity competency, because *'we simply cannot copy-paste someone else's emails filled with truisms—we must have something of value with which to contribute'.* That might happen by either cooperating with a partner organization, employ new people with domain-knowledge or build competency internally.

IC5, that typically deal with non-maritime customers, remarks that since they depend on insurance brokers as an intermediary between them and the customer, the impression they get of the demand-side's cyber-risk awareness depends on the quality of the questions they ask the customer, the quality of answers they receive back, and the brokers' processing of the information exchange. Questionnaires are this insurer's best mean to form an impression of a customer's general cybersecurity and their awareness level of cyber-risks. Since IC5 has few customers that have taken up cyber-insurance coverage,

[24]Clarification: Maersk is not among this P&I club's members

the interviewee is cautious to generalize, but the impression is that larger organizations tend to be more systematic in their cybersecurity approach, whereas smaller companies employ more ad-hoc solutions and may lack dedicated IT personnel.

IC2 says that customers belonging to the IT industry are the most risk-aware and have been for a long time. The interviewee is of the opinion that generally the larger enterprises have a better understanding of cyber-risk, and that this understanding and awareness spreads successively to midsize companies and lastly reaches the smaller ones. In 2017 the interviewee noticed an increased interest from SME companies regarding the insurer's solutions for coverage of cyber incidents—the interviewee attributes this change partly to the WannaCry ransomware attacks that took place that year, and the emergence of 'GDPR' as a buzzword.

During discussion of general customers' cyber-risk awareness, IC4 characterizes customers as being in large part 'unconscious' until 2017. Like IC2, IC4's interviewee considers that the WannaCry outbreak has been a wakeup call to some extent. Increased media coverage of cybersecurity as a topic, and the Maersk incident is mentioned aswell. That even very competent actors, such as Deloitte[25], for which cybersecurity consultancy represents an important revenue stream, can be affected by incidents is known. The interviewee finds that the typical SME still do not seem to identify with such problems at hand. The interviewee nevertheless declares increased attention from customers regarding cyber-risks during the last year, and believe that the fact that more insurers on the Norwegian market now offer cyber-insurance coverage has contributed to that. A related factor is increased activity from brokers in the Norwegian cyber-insurance market. The interviewee adds that brokers are more active partly because of their advisory responsibilities that requires them to inform clients of what possibilities there are to insure against cyber-risks. Another factor the interviewee believes might increase adoption of cyber-insurance in the Norwegian market is that *'board members, in companies, may be held accountable for failing to manage the company's cyber-risk, and the same goes for the executive management'*. That is to say that they have a duty to uncover the risk—by conducting risk and vulnerability analyses—and subsequently take some measure to mitigate that risk.

It is the interviewee's understanding that many organizations are sitting on the fence trying to figure out if they should take up cyber-insurance or not: *'There is a lot of interest, but little acceptance and action'*. The sale of cyber-insurance policies is described as having progressed from 'low' to 'low, moderate'.

Regarding maritime organizations' adoption of cyber-insurance, IC4 comments that there has been surprisingly little interest so far, except for a few requests. At the same

[25]The interviewee makes a reference to the '2017 Deloitte Cyber Incident': https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-FactsSheetforGlobalWebsite-cyber-attack.pdf

time, the interviewee comments that marine cyber-insurance *'is a scary field to enter'* and that they as the insurer needs to be careful. It is scary partly because certain marine organizations, often larger, can have complicated value-chains, which can make it challenging for an insurer to identify where the loss will arise in the case of a cyber-incident. The cyber vulnerability of organizations vary enormously, and the interviewee poses the question of *how to relate to that risk* as a question that the whole cyber-insurance industry is currently trying to figure out.

IC6's reflection is that there is a broad spectrum of understanding not only cyber-risk, but also the insurance that can address it.

The 'sophisticated buyers', usually larger companies, typically goes about buying insurance 'the correct way', the interviewee continues. That is, they have have identified their company's IT related risks; they have done a risk-mapping of those risks where they have figured out which of those risks are currently covered by already existing policies, and which of the remaining risks they can mitigate themselves, e.g. by investing in own systems; they are left with residual risks. The customer then brings these specific, residual risks to the discussion with the insurer, looking for tailor-made cover.

IC6 contrasts these sophisticated buyers with organizations that *'have heard about the Maersk incident'* and ask for cyber-insurance cover because they 'wonder if that can happen to us', without having engaged in the activities mentioned above.

When discussing policy details such as coverage, the interviewee explains, it sometimes emerges that the company has an immature understanding of cyber-insurance as a concept, as they might suggest 'fire at the data centre' as their prominent risk—*'and this is exactly what cyber does not cover, because that's a property insurance, right?'*

Regarding general customers IC6 reports that the interest for cyber-insurance in Norway has come from larger companies in retail, production, technology and IT.

Regarding interest from the maritime sector, interviewee IC6 informs that the insurance company are in talks with industries belonging to that sector, and that the Maersk incident certainly generated a spike in interest. Most of the requests are about CL380 buy-back: *'The primary concern is for the hull, for physical damage to vessels because of a cyber-attack'*. The interviewee adds that there is also a minor interest from maritime actors on topics such as social engineering, or crime, e.g. *netbank hacking*, which the interviewee does not necessarily consider to pertain to cyber, but rather be crime committed with a computer.

IC3 describes a market that has seen an increased uptake of cyber-insurance from in 2017, and continued positively so far in 2018. The interviewee believes that especially ransomware attacks during 2017 have led many organizations to begin the process of considering cyber-insurance cover.

Financial institutions are designated as having been the 'prime movers' in terms of taking up cyber-insurance coverage. The IC3 interviewee understands this in the light of the nature of data these organizations possess, and them being a desirable victim in the eyes of for-profit criminals. Large industry enterprises and infrastructure companies have followed suit.

IC3 is of the opinion that the marine industry has been slow at adapting cyber-insurance, but confirms that some shipping companies are now in a consideration phase with the insurer. The interviewee describes the decision-making process for such organizations to be typically long—one year is not unusual. That has partly to do with the need to know the product, the coverage, and how it fits in their existing insurance portfolio.

IC3 considers it 'somewhat exciting' that there are shipping companies in a decision-making process with them, as IC3 is a non-marine insurance company. The interviewee mentions that the Maersk incident was 'non-physical' in nature—there was no physical damage to vessels or individuals—but the downtime of logistics systems resulted in a monetary loss, for which non-physical cyber-insurance could have provided cover. The interviewee emphasizes the need to understand that the cyber-insurance market for the marine sector is split in two: one product that provides cover for physical damages resulting from a cyber-incident, and one product for covering non-physical consequences of a cyber-incident. The interviewee believes that the insurers dealing solely with marine risk will continue to concentrate on physical damage, and possibly include cyber-insurance cover in policies.

In personal communications with an insurance broker (B3) who is employed in a large multinational risk management company with presence in Norway, B3 stated that there currently aren't many marine companies that have bought cyber-insurance, but that they are often more preoccupied with having the CL380 clause, which is a cyber exclusion, removed from their 'all risk terms'.

5 Discussion

The discussion will be divided according to topics that were identified in the results section.

5.1 Low adoption

The statement that a specific insurance broker company has not yet sold cyber-insurance to Norwegian shipping companies, occurs in 4.1 from C3 and in 4.7 from B3. B3 works with the same insurance broker company that C3 is referring to. There are other actors from which Norwegian shipping companies can obtain cyber-coverage, but it nevertheless suggests that the uptake is low, as B3's employer is a considerable international actor. Not all companies in the maritime sector are shipping companies, but they account for a considerable part.

IC3, in 4.7, support the assertion that maritime companies has been slow in adopting cyber-insurance, but adds that there are more interest from maritime companies since around the summer of 2017. The long-drawn consideration-phase with maritime organizations is also mentioned. The recent interest resonates well with a survey conducted in November 2017 by Danish Shipping [48]. Senior executives in Danish shipping companies, representing 79% of the Danish merchant shipping fleet, shows that 69% of respondents' organizations has increased the spending on cybersecurity in their budgets. More than two thirds of the organizations answer that they have experienced attempted attacks to their IT systems during the last 12 months. It is plausible that there is some transferability to the Norwegian merchant fleet, however we need to consider that Denmark's cyber-insurance market is considered more active, generally, than that of Norway's. IC6 also reports of more interests from maritime, but that most requests are with removing the CL380 clause from hull insurance, as B3 reports as well.

C3 relates their organization's consideration of cyber-insurance partly to the Maersk case which highlighted the non-physical cyber risk to onshore IT-systems, and consequential loss from downtime. A newspaper's interview [49] with the Chief Risk Officer of A. P. Møller-Mærsk published in late autumn 2017, might have caught the eyes of some Norwegian maritime actors. The attitude to cyber-insurance given is that of an immature market; the fact that Maersk was in a consideration phase before the ransomware incident but had not taken up insurance; that the CL380 present in most hull policies, is unreasonable, because it would exclude cover for consequences of a malicious actor e.g. managing to crash a vessel through a cyber attack.

It is slightly interesting to note C1's quotation on the nature of the cyber-insurance concept in section 4.1, when discussing what requirements the insurance-side will place

on a customer to accept its risk: '[…] not risk reducing, it's rather consequence reducing, that [insurance]'. Terms such as 'risk' is known to be heavily used imprecise in colloquial conversation, but in this case the saying occurs strange when considering risk more mathematically, for instance as an increasing function of consequence and probability. Then reducing consequence would reduce risk. One way to interpret the quotation is that the interviewee perceives cyber-insurance to be more, or only, about reactive aspects (e.g. covering for IT system recovery costs) than proactive aspects (e.g. an insurer's insistence upon letting security expertise run a penetration test on the IT systems to expose technical vulnerabilities before taking on the customer's risk).

In 4.1, the fact that companies are attracted to the assistance that could be offered in relations to a cyber incident, confirms the rationality of the finding in [1, p. 142] that 'first response incident management […] is an important sales driver', and thus that cyber policies in fact are several services bundled into one.

The need expressed by customers to understand policies in terms of cover, cover triggers and loss quantification, resonates well with the finding in [19, p. 92].

Regarding C5's opinion in the same section that he believes public sector entities in general to be quite aware of cyber risk, partially because they have to follow requirements in law, but without specifying which laws, it would be plausible to believe that the word 'laws' must be referring to the GDPR or the NIS Directive. This is not necessarily so. For instance it is clear that in the regulation *eForvaltningsforskriften*[26], applying to all public sector entities , § 15 prescribes that those bodies should have an internal information security management system in place, 'that is based on' recognized standards for such management systems. That paragraph also decides that the scope of that system shall be adjusted according to identified risk. So, even if the specific law was not named by the interviewee, it is at least expected of a public administrative body to be information security risk aware.

5.2 Ambiguity of coverage

C1 draws attention to the known cyber-insurance market challenge of *ambiguity of coverage*, when he admits to be unsure of whether their already in-place, traditional policies features any cyber risk coverage. Franke phrases this as the phenomenon where the customer 'might think that cyber incidents are covered, the insurer thinks they are not' [1, p. 135]. OECD mentions this issue frequently being considered central to explain generally low cyber-insurance uptake by the demand-side globally [50, p. 192].

The same topic comes up in section 4.4 when IC2 asserts the view that the GDPR's

[26]Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften): https://lovdata.no/dokument/SF/forskrift/2004-06-25-988

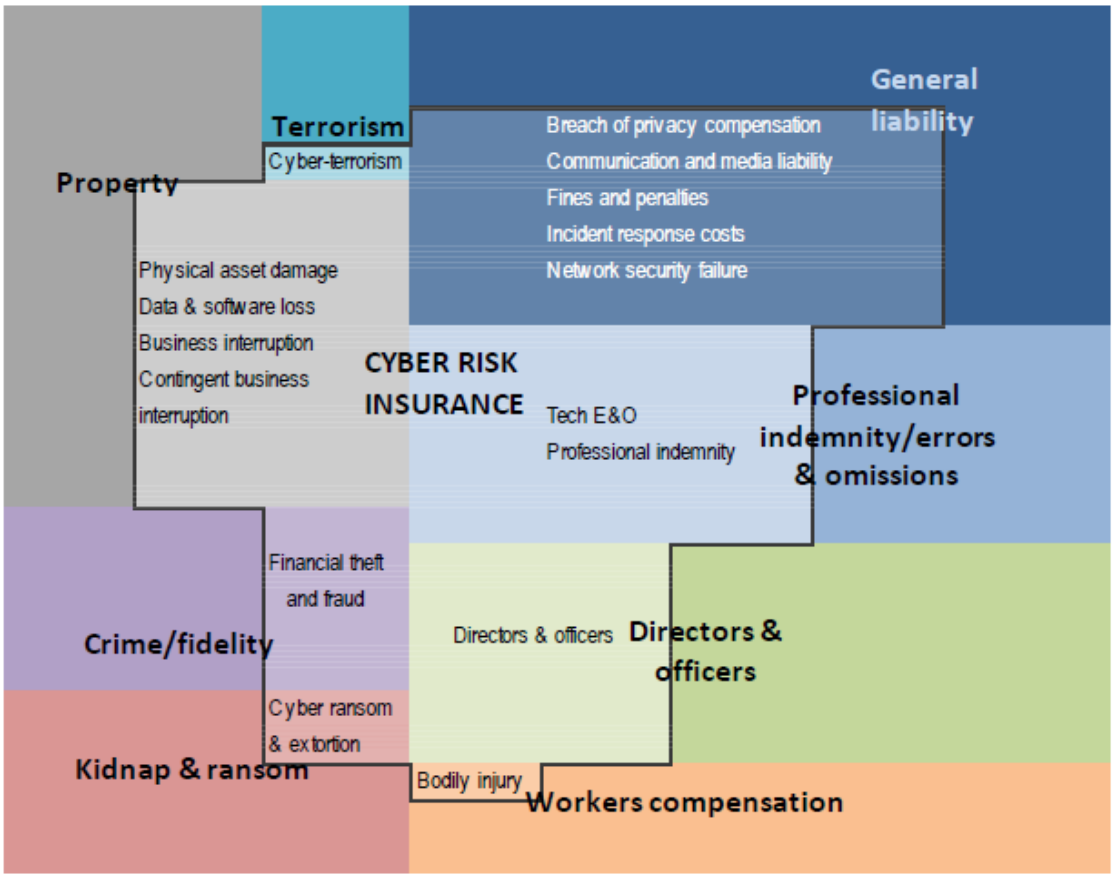

Figure 3: OECD based on JLT Re (2017): **'The potential for overlapping coverage for cyber risk in stand-alone and traditional policies'**, from [50, Fig. 4.1].

main elements relate more to traditional liability insurance than to cyber-insurance, and that it seems that many customers misperceive the cyber-insurance product to have an almost total overlap with any GDPR related costs. Cyber-insurance might cover for notification costs in the aftermath of a privacy breach, but not, according to IC2's traditional view, for any indemnity compensation that an individual who 'has suffered material or non-material damage as a result of an infringement of this Regulation' ([4, Art. 82] has the right to. This view is supported by [50, Fig. 4.1], reproduced here as figure 3, where potential overlap between traditional insurances and cyber-insurance is shown. Note the 'Breach of privacy compensation' in figure 3. [50] further suggests that different supplier-side actors' might either extend their dedicated cyber policy's scope, or extend the scope of traditional policies to include a cyber aspect.

A 2015 study [51, p. 6] found that 70% or more respondents'[27] perception of cyber-insurance was for 'third party liabilities' to be included, and 30% or less for 'notification costs to data breach victims' to be included—i.e., the opposite view from that presented

[27]The respondents are representing several hundred companies throughout 15 countries in Europe, the Middle East and Africa [51, p. 8]

above.

5.3 Motivations for (not) buying cyber-insurance

From findings in section 4.1, the interviewees' formulation of a main reason for why they think their organizations have or have not taken up cyber-insurance can be roughly stated as:

- insufficiently knowledgeable about the product (C1; C4)
- a need to better understand their own cyber-risk exposure first (C1; C2)
- regarding the product as less relevant for the organization
  - have been thinking that cyber-risk is less pronounced with the organization (C2; C4)
  - because of organization type (C5)

In a survey conducted in the autumn of 2017 by Forrester Consulting on behalf of Hiscox, reported in [52][28], 46% of respondents representing organizations that had not taken up cyber-insurance answered that 'cyber insurance is not relevant for me'. This response is similar to the third bullet point in the list above.

However, in a different survey conducted by Ponemon during the same year [53, p. 17], the two top reasons given by respondents for not taking up 'cyber security insurance' were tied between 'premiums are too expensive' and 'coverage is inadequate based on our exposure'. Both of these surveys included respondents from a wide array of industries, not confined to a maritime segment or transport companies. These surveys consisted of closed questions with answer alternatives.

In the autumn of 2017, the Danish newspaper FinansWatch reported of an increased interest from Danish shipping companies to take up cyber-insurance [54], based on comments from representatives from two insurance brokers operating in the country. In the article, the malware infection at Maersk is cited as the driver for that increased interest. One of the insurance brokers commented to the journalists that *'it is exactly the loss of revenue that the shipping companies wish to insure against'*. This resonates well with the finding in section 4.1 concerning C3, the organization that is currently considering to take up cyber-insurance, which stated that

- a better understanding of their own cyber risk exposure

[28] Respondents were professionals in charge of their organizations' cybersecurity strategy, from the UK, Germany, the US, the Netherlands and Spain [52, p. 20]

resulted from (1) witnessing the Maersk case, (2) experiencing a cyber crime attempt, (3) listening to the advice of their technology consultancy partner—all factors that motivated them to consider cyber-insurance.

5.4 Information-sharing

The findings in section 4.3 seems to suggest that the current information-sharing mechanisms of the interviewees are quite limited. This resonates well with EX1's view on information-sharing about cybersecurity in the maritime sector.

Both C1 and C3 mentions that they have reported incidents to the police. C3 judges that they have a channel for communicating about future cyber-incidents on a national (the Norwegian Shipowner's Association) and on an international level (IMO). C5 is the only interviewee that mentions that a CSIRT could facilitate information-sharing for their sector in the future: such a CSIRT is not in place, but NorSIS recommended the establishment of a CSIRT for municipalities in a 2015 report [55, p. 5]. In the Official Norwegian Report *NOU 2015: 13*, in which a committee attempted to map out Norwegian society's digital vulnerability in addition to propose measures to reduce it, section 18.5.2 [56, p. 216] addresses the committee's judgement that there is a need for a common 'reporting channel' about 'ICT incidents', both from authorities to the sector [general transport sector including maritime] and from the sector to authorities. The committee further recommends that the Ministry of Transport and Communications should report on how the reporting on ICT incidents should happen.

There is no Norwegian incident response team for the maritime sector participating in *the Forum of Incident Response and Security Teams* (FIRST) as of spring 2018[29]. It is however important to mention that there already are at least 13 CSIRTs in Norway, some private and some governmental, and that the authorities not necessarily will establish a CSIRT dedicated only to the maritime or transport sector, but possibly give that responsibility to an already existing entity. The NIS Directive [5, Art. 9] requires the implementing states to designate one or more CSIRTs to be responsible for handling of risks and incidents in specified sectors and services, 'in accordance with a well-defined process'.

To facilitate information-sharing in the maritime sector, one source of inspiration could be the Dutch *Haven-ISAC*, one of at least 14 sector-specific *information-sharing and analysis centres* (ISACs) in the Netherlands [57]. Information-sharing in the primary function of an ISAC: 'In the Port-ISAC, governments and major port companies take part to share their knowledge and exchange experiences that other companies can benefit from' [58]. This initiative is also emphasized by ENISA in as an example of a *'trust-based network of*

[29] https://first.org/members/teams/

representatives from the public and private sector and [which] allows a secure exchange of views / experiences on cyber security issues and good practices' [59, p. 17]. It is clear that both maritime actors and the insurance industry could potentially gain from the establishment of such an entity.

It is also interesting to note that no interviewees explicitly mention the *Maritime Cyber Alliance* which was established in late 2017 and aims at *'[creating] a global 24/7 anonymous cyber crime reporting platform for the rapid sharing of cyber incidents against, ship owners, ships, ports and the wider maritime supply chain'*. The initiative allows for anonymous cyber incident reporting [60] and vetted members can access reported incidents [61]. The project is supported by some major actors [62], but is also clear that the development is in a 'pilot phase'. The online platform seems to be an example of how certain maritime industry actors has the ability to self-organize, but it might simply be that the initiative is too recent for knowledge of its existence to have spread throughout the maritime industries. It might be speculated that the project is more well-known in the United Kingdom, as one of the project's founding organizations is British.

Regarding EX1's experience in section 4.3 that management boards generally are reluctant to communicate openly about cyber-incidents, especially because they fear damage to an organization's reputation, there is research to support this as a valid fear. Bharadwaj, Keil and Mähring found that investors do care about companies IT failures, and on average a firm's market value is lowered by 2% when experiencing a IT failure. The same study found that the market takes into account the nature and the context of companies' IT failures, implementation failures being considered more negatively than operational ones, and that companies suffering from a history of IT failures 'tend to suffer greater negative impact' [63, p. 74].

This preference of management boards in general to communicate less about cyber incidents is also interesting in the light of GDPR. If an incident leads to a personal data breach which sets at risk a natural persons 'rights and freedoms', the company should notify the 'supervisory authority' within 72 hours of becoming aware of it [4, Art. 33], outlining i.a. the nature of the breach, the category and numbers of data subjects concerned, what might be consequences of the breach, and how it is being dealt with. Similarly, the company might have to communicate to the data subjects according to [4, Art. 34]. As Askvik points out in [30, p. 19], the supply-side through *Insurance Europe* has argued that insurers should be able to access such reported data in an anonymized form to improve their products. This will not solve the problem of reluctant information-sharing in full—that the regulation will force boards to communicate about breaches that have occurred can be an improvement, but one would think that there will still be incidents that are well-handled within the organizations so they never lead to a data breach and do not need to be

reported neither to a supervisory authority or data subjects. That knowledge would preferentially be communicated to other actors in the same sector, through a trusted entity such as a sector ISAC as mentioned above or technology partners the company might have, as suggested by EX1 in section 5.4.

EX1 also reflects briefly on whether cyber-incidents could be mentioned e.g. in companies' annual reports to give more transparency about the industry. This is not how it functions today: Upon manual inspection of the annual reports[30] of the 23 companies[31] featured on the OSLO Shipping Index (OSLSHX)[32] 6 companies somehow address cyber-risk as a factor the company has to take into account, even though there are no mentioning of any incidents that might have taken place.

5.5 Characterization of the market

In section 4.4, several interviewees mention that they have experienced employees in organizations' IT departments to be sceptical about cyber-insurance. The findings suggest that some IT staff of a technical background can perceive their organization's consideration of taking up cyber-insurance as a sort of lack of confidence in that the IT department is doing its job. Schneier argued already in 2001 that many 'computer science professionals' would have a hard time understanding risk management through insurance, because *'they are so used to technologies solving their problems'* [13]. Findings in section 4.7 however suggests that IT and technology companies, especially larger ones, are among the more risk-aware. It appears however from the interviews that this 'internal struggle between departments' has become less of an issue during the last couple of years. It is plausible to believe that the increased number of actors that offer cyber-insurance on the market, and increased media-reporting of cyber-incidents also affecting technologically strong companies, such as Deloitte, has contributed to making IT departments somewhat less sceptical towards cyber-insurance. It can also be thought that as more individuals with a strong technological background joins executive management, IT staff can more readily be convinced of cyber-insurance as a valid method to handle residual risk.

The interviewees share the understanding that cyber-insurance uptake has been lower in Norway than in the other Nordic countries. This confirms the finding in [1, p. 136].

Interviewee IC1 suggests that there might be a cultural element that could partly explain why cyber-insurance is less widespread in Norway than in the other Nordic countries. Warner-Søderholm finds Denmark to be the least hierarchical culture in the Nordic countries, followed by Norway, Sweden, and Finland, which is the most hierarchical. The

[30] As of April 2018, 4 of the 23 were annual reports for 2016, the remaining for 2017.

[31] These are multinational companies not limited to companies with headquarters in Norway.

[32] The index contains stocks that is related to the shipping sector, and that are listed on either the Oslo Stock Exchange or Oslo Axess, cf. https://www.oslobors.no/markedsaktivitet/#/details/OSLSHX.OSE/overview.

findings of that study then supports that *'a dominant feature of the Scandinavian management style in general is delegation of responsibility'* [64]. However, cyber-insurance is more widespread in both Denmark and Finland—the least and most hierarchical Nordic cultures—than in Norway. Even if Norwegian delegation of responsibility might influence the adoption of cyber-insurance among Norwegian organizations, other factors must also be relevant, such as the the later introduction of the product on the Norwegian market.

The finding that one of the insurance companies report that approximately 50% of Nordic claims have come from Norway, even though less than one sixth of policies are held in Norway is interesting. It could suggest that Norwegian organizations' are more exposed to cyber risk, or that cybersecurity of Norwegian organizations is somehow weaker than that of organizations in other Nordic countries, but the finding is not supported by similar figures from the other interviewees.

5.6 GDPR

According to the findings in section 4.5.5, the informants agree that the GDPR influences the cyber-insurance market in that it functions as a topic to start the conversation with customers about cyber-insurance, but there is some disagreement to what degree the regulation itself has been in providing new customers so far. The informants that deal mainly with larger customers assign a greater importance to GDPR as a contributing factor than the informants that deal more with SME customers. This makes sense when considering that larger, more sophisticated companies have been preparing for the GDPR for a longer period of time and are generally more prepared for the regulation. Additionally, brokers are mentioned as being especially preoccupied with the GDPR, and intermediaries are more often part of the equation when insurers deal with larger companies.

The findings in section 4.5.5 indicate that some organizations might feel less at risk to be fined for infringement of the GDPR because they are not privately owned, but part of the public sector. In Sweden, the government has proposed that even public sector entities can be fined, but that less serious infringements can only lead to fines up to a new cap of SEK 5 million, and more severe infringements can only lead to fines up to a new cap of SEK 10 million [65, p. 139]. In Norway, the government has proposed to carry on the possibility for the NDPA to fine public sector entities for infringements of the GDPR, without proposing caps on those fines [66, p. 136]. Some commenting bodies to the proposition voiced that the size of the fines should be upwards limited, or that the NDPA should not have the possibility to fine public sector entities, e.g. because such a fine would function simply as a redistribution mechanism and interfere with political authorities' prioritization of resources to solve administrative tasks [66, pp. 137-139].

5.7 The NIS Directive

The findings are consistent with regards to the NIS Directive's possible influence on the cyber-insurance supply-side in Norway: it has not had an influence yet. The supply-side has a favourable view of organizations that generally strive to be compliant with regulations.

The interviewed demand-side varies in its awareness of the NIS Directive. Those who are aware of it either considers that their own organization does not fall under the scope of the directive, or is uncertain to what degree the organization has prepared for the directive.

The findings for both the demand- and supply-side are understandable considering that the directive is still under evaluation in the EEA/EFTA countries, even if the Norwegian authorities have found it EEA relevant and acceptable. It is somewhat surprising that the supply-side has not expressed a stronger desire to access incident data that will have to be reported to authorities from operators of essential services and digital service providers, since the insurance companies interviewed also operate in EU countries where the directive will take effect soon.

5.8 Reliability

The supply-side's findings can be characterized as decent, in terms of reliability. 7 insurance companies were interviewed, 6 non-marine and 1 marine. The 6 non-marine companies focus on different segments of the market: two of them mainly deal with larger enterprises through brokers, while 4 of them have mostly SME customers.

At least one company launched their product in February 2018 during the project work, and was not included in the study. At least 3 relevant insurers did not participate, but they cannot be considered to represent significantly different actors. All in all, 6 out of the 7 insurers included currently have a cyber-insurance product on the Norwegian market, and it is reasonable to consider them to make up a representative sample of the full population of insurance companies with a presence in Norway offering cyber-insurance coverage. Thus, a different sampling strategy would probably not have significantly affected the conclusions.

The reliability of the demand-side's findings can be characterized as low. The 3 shipping companies, 1 municipality port operator and 1 passenger transport company represent a *convenience sample* [44, p. 124], i.e., they where the most willing and able to participate and were selected on that basis. Thus, a different (more exhaustive and more random) sampling strategy might well have affected the conclusions. The inclusion of EX1 as an expert interviewee, on the grounds of him having more than 15 years of experience from both shipping and technology, from several companies, can be seen as a strengthening

factor for the reliability, in the sense that it diminishes the dependence on the small convenience sample of companies. However, it does introduce a sampling problem of its own, since only a single expert participated.

Semi-structured interviews are problematic from a reliability perspective, because of the possibility to elaborate on an interesting topic and thus vary the ordering that questions are asked, or skipping a question. Nevertheless, reliability is better than that of the freer unstructured interview.

Reliability was increased by the fact that the interviews were allowed to be audio-recorded and subsequently transcribed, which reduces the chance that relevant information is missed, as could easily happen if the interviewer is only relying on hand-written notes and keywords taken while conducting the interview.

5.9 Validity

Validity is threatened from using interviews as the research method. One danger threatening validity is *manipulation*, of conscious and unconscious type, i.e., the possibility that interviewees in some cases might have a need to 'push an agenda', or that they might rationalize a narrative of events that has happened [67, pp. 288,292].

The interviewees on the supply-side—underwriters, analysts, product managers—are qualified interviewees with knowledge of cyber-insurance, which strengthens validity.

The interviewees on the demand-side are HSEQ Directors, an Insurance Director, a Chief Risk Officer, and a Senior ICT Consultant. These roles are varied, but should be considered qualified to answer most questions in the interview guide, even if there were occasions where a different individual in the organization probably would have been more apt to answer. Still, these positions must be be considered to be relevant. The sixth interviewee, who agreed to do an expert interview without going into details on their particular organization, and who is part of executive management, must also be considered relevant. This also strengthens validity.

6 Conclusion

The cyber-insurance market in Norway has grown significantly on the supply-side during the last two years, with insurers catering to customers of varying size, risk-profile and industry segment. Insurers that are mostly dealing with larger companies as customers are increasingly approaching also SME customers. Most cyber-insurance suppliers offer to cover against non-physical consequences of a cyber-incident, but marine insurers increasingly have to consider whether to offer a 'CL380 buy-back' from e.g. their hull insurance policies.

The study confirms other studies' assertions that the Norwegian cyber-insurance market is the least mature of the Nordic markets.

Earlier studies and commentators have anticipated the GDPR's implementation to lead to an increase in the uptake of cyber-insurance. This study suggests that most suppliers consider that the effect so far has been modest, and that the regulation first and foremost functions as an icebreaker to talk to customers about cyber risk, and to introduce cyber-insurance. The regulation will also impact the market in that customers who show that they are compliant will be associated with a lower risk for insurers to take on. Some suppliers that are not used to similar legislation from outside the EEA have had to make minor changes to their policies with regard to covering for notification costs in case of a privacy breach.

The study suggests that the NIS Directive has had little or no impact on the Norwegian cyber-insurance market so far, based on the response from both the demand- and the supply-side interviewees.

The supply-side experiences that actors on the demand-side are all over the range from ignorant to highly sophisticated in their understanding of and approach to cyber risk. Larger enterprises in finance and technology are more eager to insure residual risk, but there is an increased general interest in the products, with many actors sitting on the fence. The maritime sector has been showing less interest than other segments on the demand-side, but there has been an increasing interest in cyber-insurance solutions especially after the Maersk case exemplified what costs can arise from downtime of traditional IT systems. Vessel-owning companies tend to be more interested in getting rid of any cyber exclusions in their traditional insurance policies, than to pursue dedicated cyber-insurance for their onshore IT systems.

The interviewed maritime organizations have not taken up dedicated cyber-insurance, but one of them is in a consideration phase. Ideally the study would have included demand-side actors that had already adopted insurance to better address the research questions concerning the demand-side, but this did not succeed.

Most interviewees had little knowledge of cyber-insurance for their onshore IT systems and emphasized the need to better assess their own cyber risk exposure before possibly proceeding with considering uptake. This is also largely the main motivations for not having bought cyber-insurance.

The demand-side interviewees are examples of organizations that acknowledge that they are currently not sufficiently concious of the cyber risk they are exposed to. It is clear that maritime industry organizations are diverse, having quite different risk profiles. The IMO has provided the maritime industry with high-level risk management recommendations, and industry actors have published best-practises addressing cyber-risk for both IT and OT systems. Manual inspection of the annual reports of 23 maritime organizations that are listed on the Oslo Stock Exchange show that only 6 of them address cyber risk.

The GDPR is found to not be a major driver for maritime organizations to consider taking up cyber-insurance. The demand-side interviewees have been preparing for the regulation, and the study additionally suggests that non-maritime insurers have been using GDPR as a selling point for cyber-insurance.

The maritime industry has mechanisms to discuss issues other than cyber risk. It is suggested that Norwegian maritime actors closer should examine the recently established vetted-members-only online reporting platform *Maritime Cyber Alliance*, originating from the UK. None of the interviewees knew of this initiative. Interviewees acknowledge the value of information-sharing, but it is clear that the fear of reputation loss is a hindrance. The creation of a public-private maritime ISAC is suggested as an alternative means to exchange knowledge between actors.

A suggestion for further study will be to clarify better, for example through a quantitative study, how many (Norwegian) vessel-owning companies have actually bought back the CL380 cyber-exclusion from their marine insurances. This study has suggested that this is increasingly being done, but has not succeeded in establishing to what degree. It is suggested by the author to conduct such a study in collaboration with maritime interest organizations to improve the chances of getting an acceptable response rate.

References

[1] U. Franke, 'The cyber insurance market in Sweden', *Computers & Security*, vol. 68, pp. 130–144, 2017, ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2017.04.010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404817300883.

[2] 'Net losses: Estimating the global: Cost of cybercrime', McAfee; CSIC, Report, 2014. [Online]. Available: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

[3] 'The Hiscox Cyber Readiness Report 2017', Hiscox Ltd., Hamilton, Bermuda, Report, 2017. [Online]. Available: https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf.

[4] 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)', *Official Journal of the European Union*, vol. L 119, 2016. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/oj.

[5] 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union', *Official Journal of the European Union*, vol. L 194, pp. 1–30, 2016. [Online]. Available: http://data.europa.eu/eli/dir/2016/1148/oj.

[6] *2017 Annual Report*. A.P. Møller - Mærsk A/S, 2017, https://www.maersk.com/-/media/press/press-release-archive/2018/20180209-annual-report-2017/20180209-a-p-moller-maersk-annual-report.ashx.

[7] (2017). Annex 10: Resolution MSC.428(98) - Maritime cyber risk management in safety management systems, International Maritime Organization, [Online]. Available: http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428(98)%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf.

[8] E. W. Jakobsen and C. S. Mellbye, *Maritim Verdiskapingsbok for 2017*. Oslo, Norway: Maritimt Forum, 2017. [Online]. Available: https://www.menon.no/wp-content/uploads/2017-Maritim-verdiskapingsbok.pdf.

[9] U. Choudhry, *Der Cyber-Versicherungsmarkt in Deutschland: Eine Einführung*, 1st, ser. essentials. Wiesbaden, Germany: Springer Gabler Verlag, 2014, ISBN: 978-3-658-07098-4. DOI: 10.1007/978-3-658-07098-4.

[10] R. Böhme, G. Schwartz *et al.*, 'Modeling cyber-insurance: Towards a unifying framework.', in *WEIS*, 2010. [Online]. Available: http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf.

[11] R. Böhme and G. Kataria, 'Models and measures for correlation in cyber-insurance.', in *WEIS*, 2006. [Online]. Available: http://sec2013.crysys.hu/~mfelegyhazi/courses/EconSec/readings/09_BohmeK2005insurance_correlation.pdf.

[12] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti and S. K. Sadhukhan, 'Cyber-risk decision models: To insure it or not?', *Decision Support Systems*, vol. 56, pp. 11–26, 2013, ISSN: 0167-9236. DOI: https://doi.org/10.1016/j.dss.2013.04.004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167923613001115.

[13] B. Schneier, 'Insurance and the computer industry', *Communications of the ACM*, vol. 44, no. 3, pp. 114–114, 2001. DOI: https://doi.org/10.1145/365181.365229.

[14] ENISA, *Commonality of risk assessment language in cyber insurance: Recommendations on Cyber Insurance*. 2017, ISBN: 9789292042288. DOI: DOI10.2824/691163.

[15] A. J. Lathrop and J. M. Stanisz, 'Hackers are after more than just data: Will your company's property policies respond when cyber attacks cause physical damage and shut down operations?', pp. 286–303, 2016. DOI: https://doi.org/10.1080/10406026.2016.1197653.

[16] M. Payne and P. Komisarczuk, 'Insuring the uninsurable: Is cyber insurance really worth its salt?', *ISG MSc Information Security thesis series 2017*, 2017. [Online]. Available: https://www.royalholloway.ac.uk/isg/documents/pdf/technicalreports/2017/michaelpayneisg.pdf.

[17] (2018). InSecurance - SINTEF, SINTEF, [Online]. Available: https://www.sintef.no/en/digital/software-and-service-innovation/secure-iot-software/insecurance/.

[18] I. A. Tøndel, F. Seehusen, E. A. Gjære and M. E. G. Moe, 'Differentiating Cyber Risk of Insurance Customers: The Insurance Company Perspective', in *International Conference on Availability, Reliability, and Security*, Springer, Cham, 2016, pp. 175–190, ISBN: 978-3-319-45507-5. DOI: https://doi.org/10.1007/978-3-319-45507-5_12.

[19] P. H. Meland, I. A. Tøndel, M. Moe and F. Seehusen, 'Facing Uncertainty in Cyber Insurance Policies', in *International Workshop on Security and Trust Management*, Springer, Cham, 2017, pp. 89–100, ISBN: 978-3-319-68063-7. DOI: https://doi.org/10.1007/978-3-319-68063-7_6.

[20] (2018). Maritime næringer, Nærings- og fiskeridepartementet, [Online]. Available: https://www.regjeringen.no/no/tema/naringsliv/maritime-naringer/id1337/.

[21] (2015). Slik ser rederiene ut, KarriereStart.no, [Online]. Available: https://karrierestart.no/bransje/shipping-off-onshore-maritim/779-norske-rederier-slik-ser-rederiene-ut-i-den-norske-maritime-naeringen.

[22] (2018). Om næringen, Maritimt Forum, [Online]. Available: http://maritimt-forum.no/om-oss/om-naeringen/.

[23] (2017). MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management, International Maritime Organization, [Online]. Available: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20%28Secretariat%29.pdf.

[24] *The guidelines on cyber security onboard ships*, 2nd ed., BIMCO et al., 2017. [Online]. Available: https://www.bimco.org/-/media/bimco/ships-ports-and-voyage-planning/security/cyber-security/guidelines_on_cyber_security_onboard_ships_version_2-0_july2017.ashx.

[25] G. D. L. Morris. (2016). Marine risks: Filling the cyber coverage gap in marine, [Online]. Available: http://riskandinsurance.com/filling-cyber-coverage-gap-marine/.

[26] *Future of the Sea: Cyber Security*. Government Office for Science, 2017. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/671824/Future_of_the_Sea_-_Cyber_Security_Final.pdf.

[27] K. D. Jones, K. Tam and M. Papadaki, 'Threats and impacts in maritime cyber security', *Engineering & Technology Reference*, vol. 1, no. 1, 2012, ISSN: 2056-4007. DOI: 10.1049/etr.2015.0123.

[28] J. Bhatti and T. E. Humphreys, 'Hostile control of ships via false gps signals: Demonstration and detection', *Navigation*, vol. 64, no. 1, pp. 51–66, 2017.

[29] K. Kolsrud. (2018). Gdpr forsinkes igjen – nå er datoen 1. juli, [Online]. Available: http://rett24.no/articles/gdpr-forsinkes-igjen--na-er-datoen-1.juli.

[30] C. Askvik, 'En effektiv marknad för cyberförsäkringar i EU: Om cybersäkerhet och cyberförsäkringar i EU och hur de kan komma att påverkas av NIS-direktivet samt GDPR', Master's thesis, Linköpings universitet, Linköping, Sweden, 2018.

[31] (2017). The directive on security of network and information systems (nis directive), European Commission, [Online]. Available: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[32] (2016). NIS-direktivet, Regjeringen, [Online]. Available: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/.

[33] J. Hagen, O. Hermansen, Ø. Toftegård, J.-M. Pettersen, R. Steen and S. L. Paulen, *Rapport nr 26-2017: Regulering av IKT-sikkerhet*. Oslo, Norway: Norges vassdrags- og energidirektorat, 2017, ISBN: 9788241015786. [Online]. Available: http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf.

[34] C. Maynard, N. Ijzinga and D. van Veldhuizen. (2017). Why do you need to know about the NIS Directive?, [Online]. Available: https://www2.deloitte.com/nl/nl/pages/risk/articles/why-do-you-need-to-know-about-the-nis-directive.html#.

[35] Department for Digital, Culture, Media & Sport. (2017). New fines for essential service operators with poor cyber security, [Online]. Available: https://www.gov.uk/government/news/new-fines-for-essential-service-operators-with-poor-cyber-security.

[36] (2018). ISM code and guidelines on implementation of the ISM code, International Maritime Organization, [Online]. Available: http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx.

[37] K. A. Kopperud, *ISM-koden*. Oslo, Norway: Norsk sjøoffisersforbund, 1999. [Online]. Available: http://urn.nb.no/URN:NBN:no-nb_digibok_2015020308058.

[38] *ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements*. Geneva, Switzerland: International Organization for Standardization, 2013.

[39] (2018). Cybersecurity framework, NIST, [Online]. Available: https://www.nist.gov/cyberframework.

[40] (2018). Expert risk articles: Cyber risk on the rise in shipping, Allianz Global Corporate & Specialty, [Online]. Available: http://www.agcs.allianz.com/insights/expert-risk-articles/cyber-risk-on-the-rise-in-shipping/.

[41] U. Malt, 'Strukturert intervju', in, vol. Store norske leksikon, 2015. [Online]. Available: https://snl.no/strukturert_intervju.

[42] (2018). Maritimt forum, Maritimt Forum, [Online]. Available: http://maritimtforum.no/.

[43] (2014). About, The Norwegian Shipowners' Association, [Online]. Available: https://www.rederi.no/en/about/.

[44] L. Given, *The SAGE Encyclopedia of Qualitative Research Methods*. SAGE Publications, 2008, ISBN: 9781452265896. [Online]. Available: https://books.google.no/books?id=byh1AwAAQBAJ.

[45] R. Kissel, A. Regenscheid, M. Scholl and K. Stine, *SP 800-88 Rev. 1: Guidelines for media sanitization*. US Department of Commerce, National Institute of Standards and Technology, 2014. DOI: https://doi.org/10.6028/NIST.SP.800-88r1.

[46] E. F. Foundation. (2015). How to: Delete your data securely on windows, [Online]. Available: https://ssd.eff.org/en/module/how-delete-your-data-securely-windows#Anchor%201.

[47] J. Stewart and J. Bettke. (Jun. 2016). Wire Wire: A West African Cyber Threat, [Online]. Available: https://www.secureworks.com/research/wire-wire-a-west-african-cyber-threat.

[48] 'Rederierne opruster på it-sikkerhed', Danske Rederier, Nov. 2017. [Online]. Available: https://www.danishshipping.dk/analyse/download/Basic_Model_Linkarea_Link/1021/rederipanel_nov2017_rederierne-opruster-pa-it-sikkerhed.pdf.

[49] J. Skouboe and M. Duelund. (Oct. 2017). Maersk: Markedet for cyberforsikringer er umodent, [Online]. Available: https://finanswatch.dk/secure/Finansnyt/Forsikring__Pension/article9976581.ece.

[50] OECD, *Enhancing the Role of Insurance in Cyber Risk Management*. 2017, p. 140. DOI: https://doi.org/http://dx.doi.org/10.1787/9789264282148-en. [Online]. Available: https://www.oecd-ilibrary.org/content/publication/9789264282148-en.

[51] Ponemon Institute LLC, *2015 EMEA Cyber Impact Report: The increasing cyber threat – what is the true cost to business?* Aon Risk Solutions, 2015, p. 12. [Online]. Available: http://www.aon.com/sweden/attachments/Kunskapsledare/2015cyberimpactreport_ponemon.pdf.

[52] 'The Hiscox cyber readiness report 2018', Hiscox Ltd., Hamilton, Bermuda, Tech. Rep., 2018. [Online]. Available: https://www.hiscox.co.uk/sites/uk/files/documents/2018-02/Hiscox_Cyber_Readiness_Report_2018_FINAL.PDF.

[53] Ponemon Institute LLC, *2017 Global Cyber Risk Transfer Comparison Report*. Aon Risk Solutions, 2017, p. 32. [Online]. Available: http://www.aon.com/attachments/risk-services/cyber/2017-Global-Cyber-Risk-Transfer-Report-Final.pdf.

[54] K. G. Raun and N. Krigslund. (Sep. 2017). Rederier har fået øjnene op for cyberforsikringer, [Online]. Available: https://finanswatch.dk/secure/Finansnyt/Forsikring__Pension/article9849756.ece.

[55] (2015). Kommune cert: Utredning av behov og muligheter, NorSIS, [Online]. Available: https://norsis.no/d18ba623c92d1ded748a61ae70/KommuneCSIRT_print.pdf.

[56] *NOU 2015: 13. Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Justis- og beredskapsdepartementet, 2015. [Online]. Available: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf.

[57] (2015). ISAC's | NCSC, Nationaal Cyber Security Centrum, Ministerie van Justitie en Veiligheid, [Online]. Available: https://www.ncsc.nl/samenwerking/isacs.html.

[58] A. A. Oosting, 'Haven moet cyber security zeer serieus nemen', *Seaport Magazine Transport & Logistiek*, pp. 6–7, 7 2016, ISSN: 1387-5671. [Online]. Available: http://seaport-magazine.nl/wp-content/uploads/2016/10/70528-Seaport-7-LR.pdf.

[59] D. Cimpean, J. Meire, V. Bouckaert, S. Vande Casteele, A. Pelle and L. Hellebooge, *Analysis of Cyber Security Aspects in the Maritime Sector*. ENISA, 2011. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport.

[60] (2018). Submit anonymous report, Wididi, [Online]. Available: https://air.wididi.com/pages/air-report.php.

[61] (2018). Incidents overview, Maritime Cyber Alliance, [Online]. Available: https://www.maritimecyberalliance.com/page/37828-news-overview.

[62] (2018). Security through community, Maritime Cyber Alliance, [Online]. Available: https://www.maritimecyberalliance.com/download/?ID=30000078158%5C&file=45497367884343940 0%5C&filename=Maritime+Cyber+Alliance+2+Page+Introduction+.pdf.

[63] A. Bharadwaj, M. Keil and M. Mähring, 'Effects of information technology failures on the market value of firms', *The Journal of Strategic Information Systems*, vol. 18, no. 2, pp. 66–79, 2009, ISSN: 0963-8687. DOI: https://doi.org/10.1016/j.jsis.2009.04.001. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0963868709000158.

[64] G. Warner-Søderholm, 'But we're not all vikings', *Journal of Intercultural Communication*, no. 29, 2012.

[65] (2017). Regeringens proposition 2017/18:105: Ny dataskyddslag, [Online]. Available: http : / / www . regeringen . se / 492373 / contentassets / 561c615d11104ad38c42b59cda9c33bc/ny-dataskyddslag-prop.-201718105.

[66] (2018). Prop. 56 ls (2017–2018), [Online]. Available: https : / / www . regjeringen . no / contentassets / 1a36e88f124d4a1ea92a9c790be2d69a / no / pdfs / prp201720180056000dddpdfs.pdf.

[67] S. S. Andersen, 'Aktiv informantintervjuing', *Norsk statsvitenskapelig tidsskrift*, vol. 22, no. 03, pp. 278–298, 2006.

Appendix 1 – Interview guide for the demand-side

Interview guide, customer-side

Even Langfeldt Friberg [redacted]

A. Introduction

1. (Briefly about the background for my interview.)
2. Do you have comments to the interview consent form, or about how I use information drawn from the interview in my master thesis work?
3. What is your position in the organization and what does it entail?
4. Did your organization take out cyber-insurance?
    - Yes: go to branch B, then branch E
    - No, but it has been considered: go to branch C, then branch E
    - No, and it has not been considered: go to branch D, then branch E

B. The organization has taken out cyber-insurance

5. Can you say which insurance product the organization chose?
6. For how long has the organization been cyber-insured?
7. Why did the organization take out cyber-insurance?
    a. From where did the initiative come?
    b. Was the decision based on a risk assessment?
    c. Did you consider other forms of risk management instead of cyber-insurance?
8. Can you say something about the acquisition phase?
    a. Which roles in your organization were involved?
    b. Did you make use of an insurance broker?
    c. What was it like to evaluate and compare the different provider's cyber-insurance products?
        i. Would you say that the organization has the in-house competence to evaluate the insurance conditions, and the coverage of the product?
    d. What was it like to answer the questions asked from the insurance provider?
        i. Did you consider as relevant the questions asked, the requirements set, the examinations made (from the provider's side)?
    e. Did the insurance provider put forth requirements for how your organization manage cyber risk, for them to offer your organization cyber-insurance?
        i. Did you have to take specific technical or organizational measures?
        ii. Did the provider e.g. require the organization to follow a specific standard, best-practise, or to implement a management system for cyber/information security?
    f. Can you say approximately how long time passed from the organization started to consider cyber-insurance till insurance was taken out?
    g. How did you experience the process?
        i. Were there problematic aspects in taking out cyber-insurance?
9. How did you decide what the insurance had to cover?
    a. Do you consider that the cyber-insurance is sufficiently adapted to your organization, or are there e.g. coverage overlap with other insurance products the organization has taken out?
10. Are you satisfied with your organization's cyber-insurance?
    a. Are you confident in the choice of insurance, and that it is sufficiently adapted to the organization?

b. Do you have comments to e.g. the insurance premium; technical/organizational support given in case of an incident (emergency response); the product's flexibility; the kinds of incidents the product will cover

11. Does the cyber-insurance influence how you work with cyber security in your organization?
12. Can you say if the organization has experienced incidents where the cyber-insurance has been of use?
    a. If so, how is the experience with the product?
13. Do you consider that legislation and regulations have influenced your organization's decision to take out cyber-insurance? Are any of the following relevant?
    a. The General Data Protection Regulation (GDPR – EU regulation 2016/679)
        i. Are "personal data breaches" relevant to your organization?
        ii. Would it be possible to pay a regulatory fine? (Depending on which provisions have been infringed: a fine up the greater of up to EUR 10 million or 2% of annual worldwide turnover OR a fine up the greater of up to EUR 20 million or 4% of annual worldwide turnover)
    b. The International Maritime Organization's decision to demand that cyber risk management be included in the ISM code onboard ships by 2021 (IMO resolution MSC.428(98))
    c. The "NIS directive", concerning measures for a high common level of security of network and information systems – especially relevant to "operators of essential services and digital service providers" (EU directive 2016/1148)

C. The organization has not taken out cyber-insurance, but it has been considered

14. Why did the organization take out cyber-insurance?
    a. From where did the initiative come?
    b. Was the decision based on a risk assessment?
    a. Did you consider other forms of risk management instead of cyber-insurance?
15. Can you say something about the consideration phase?
    a. Which roles in your organization were involved?
    b. Did you make use of an insurance broker?
    c. What was it like to evaluate and compare the different provider's cyber-insurance products?
        i. Would you say that the organization has the in-house competence to evaluate the insurance conditions, and the coverage of the product?
    d. What was it like to answer the questions asked from the insurance provider?
        i. Did you consider as relevant the questions asked, the requirements set, the examinations made (from the provider's side)?
    e. Did the insurance provider put forth requirements for how your organization manage cyber risk, for them to offer your organization cyber-insurance?
        i. Did you have to take specific technical or organizational measures?
        ii. Did the provider e.g. require the organization to follow a specific standard, best-practise, or to implement a management system for cyber/information security?
    f. How did you experience the process?
        i. Were there problematic aspects?
    g. Can you suggest what are the main reasons for not taking out cyber-insurance?
    h. Can you say approximately how long time passed from the organization started to consider cyber-insurance as a tool to manage risk, till it was decided not to take it out?
        i. Are you confident in that decision?
        ii. Has the organization later implemented other security-enhancing means instead of taking out cyber-insurance?

16. If the organization had taken out cyber-insurance, how to you consider that would have influenced how you work with cyber security in your organization?
17. Can you say if the organization has experienced incidents where cyber-insurance might have come to use?
18. Do you consider that the following legislation and regulations will influence how the organization manages cyber risks?
    a. The General Data Protection Regulation (GDPR – EU regulation 2016/679)
        i. Are "personal data breaches" relevant to your organization?
        ii. Would it be possible to pay a regulatory fine? (Depending on which provisions have been infringed: a fine up the greater of up to EUR 10 million or 2% of annual worldwide turnover OR a fine up the greater of up to EUR 20 million or 4% of annual worldwide turnover)
    b. The International Maritime Organization's decision to demand that cyber risk management be included in the ISM code onboard ships by 2021 (IMO resolution MSC.428(98))
    c. The "NIS directive", concerning measures for a high common level of security of network and information systems – especially relevant to "operators of essential services and digital service providers" (EU directive 2016/1148)

D. The organization has not taken out cyber-insurance, and it has not been considered

19. What do you think are reasons that the organization has not considered cyber-insurance as a mean to manage cyber risk?
20. To what degree do you consider that the organization is aware of cyber risk?
21. Are you familiar with the concept of cyber-insurance, and what products exist on the market?
22. Do you consider that the organization already has other forms of insurance that should cover certain cyber incidents and computer crime? What are those?
23. Do you think that the organization will consider cyber-insurance in the future?
    a. What could make cyber-insurance relevant?
    b. How do you think the organization would start the process of considering cyber-insurance? (E.g. by contacting a broker, utilize already existing relationships to an insurance provider, technology consultants, etc.)
24. Can you say how the organization manages cyber risk today, and how it is considered what technical and organizational measures to implement?
    a. What roles in the organization are involved in this work?
    b. Does the organization follow specific standards, best-practises, frameworks? Do you know if the organization has implemented a management system for cyber/information security?
25. Do you consider that the following legislation and regulations will influence how the organization manages cyber risks?
    a. The General Data Protection Regulation (GDPR – EU regulation 2016/679)
        i. Are "personal data breaches" relevant to your organization?
        ii. Would it be possible to pay a regulatory fine? (Depending on which provisions have been infringed: a fine up the greater of up to EUR 10 million or 2% of annual worldwide turnover OR a fine up the greater of up to EUR 20 million or 4% of annual worldwide turnover)
    b. The International Maritime Organization's decision to demand that cyber risk management be included in the ISM code onboard ships by 2021 (IMO resolution MSC.428(98))

c. The “NIS directive”, concerning measures for a high common level of security of network and information systems – especially relevant to “operators of essential services and digital service providers” (EU directive 2016/1148)

E. Cyber risk

26. What do you consider to be the risk profile and main cyber risks relevant to the organization? (Also for the industry sector?)
    a. What is the background for this risk estimation?
    b. How do you imagine the course of an undesirable cyber event, and the potential consequences, for your organization?
        i. Which players will the organization rely on to handle such an event?
            1. Sufficient in-house capabilities? External resources?
27. Can you say if the organization has experienced undesirable cyber incidents? Do you have a figure?
    a. Can you outline the course of the event and any possible consequences?
    b. Did this influence how you manage cyber risk in your organization?
    c. Did your organization report the incident to an external party?
        i. Do you have opinions on information-sharing about events, current risks, etc. in the industry sector that your organization belongs to? (Between e.g. your organization, competitors and partners, government agencies, other external parties.)

F. End

28. (Thank you. On my work process from here.)
29. Are there other aspects of cyber-insurance you would like to highlight?

Appendix 2 – Interview guide for the supply-side

Interview guide, supplier-side

Even Langfeldt Friberg [redacted]

Introduction

1. What is your position in the organization, and what does it involve?
2. How long has your cyber insurance product been on the (Norwegian) market?

Customers – characterization of the demand-side

3. How many (Norwegian) customers have taken up your cyber insurance?
4. What kind of customers (sectors) are these mainly?
    - Is it possible to say something on the number of customers that can be classified as belonging to the maritime sector (e.g. shipping companies, shipyards, etc.)?
5. How did you reach the customers?
    - E.g. Already existing relationships? Through insurance agents and brokers? High-profile cyber incidents referred in the news have moved customers towards you?
6. How do you segregate the customers?
    - Risk profile of the company?
    - Size of the premium the company pays?
7. Do you perceive differences in customers' awareness of cyber risk?
    - Can anything be said about those more/less conscious of cyber risk?
8. What kind of customers would you want to attract with your product?
9. What portion of the customers are small and medium sized-enterprises?
    - Is it possible to say if this portion has changed discernible since your cyber insurance product was launched?

Product, coverage

10. What are the greatest difficulties in selling or providing cyber insurance to the customer?
11. What is included in your cyber insurance product?
    - E.g. help from external expertise in case of an ongoing incident
12. What incident types are you more interested in covering?
13. Are there certain incident types the product will not provide cover for?
    - E.g. non-malicious events (mistakes, power outage, etc.)

Claims

14. Can you say how many claims have been received since the launch of the product (in Norway)?
    - Number of granted/rejected?
15. What category of cyber incidents (leading to claims) dominate?
16. What category of cyber incidents are more problematic?

Underwriting

17. What does your underwriting process look like?
18. How can one determine if a potential customer has an acceptable risk profile?
19. Do you set requirements for the customer to live by specific standards, best-practises, to be allowed to take up cyber insurance with you?

20. Can one say something on how the insurance premium the customer pays depends upon risk profile, or what standards the customer lives by, or the sector the customer belongs in?
21. To what degree do the lack of (actuarial) data and statistics on cyber incidents pose a challenge for the underwriting process?
22. Do you have opinions on whether the lack of standardized cyber terminology create difficulties for underwriters and (potential) customers?

Information-sharing

23. Do you consider that customers communicate reliably about cyber incidents to you? (Also about cyber incidents that they have successfully dealt with internally, and/or that does not lead to a claim.)
    - How is this done?
24. Have you taken measures to increase the customers' propensity to share relevant (e.g. risk assessment, incident management) information to you? If so, what measures are they?
25. Do you share information with other organizations? (E.g. other insurance companies, competitors, professional associations, other customers, authorities, etc.)
    - Do you make use of statistics from external parties?

GDPR (Nor. *Personvernforordningen*, Swe. *Allmänna dataskyddsförordningen*)

26. Do you consider that the imminent implementation of the regulation (into Norwegian law) has contributed in obtaining (Norwegian) customers?
    - Do you consider the implementation of the regulation as an opportunity to increase the number of cyber insurance customers?
27. (What is your opinion of how regulation in general affects the cyber insurance market?)
28. Have you conducted any form of analysis on how the GDPR will impact the market?
29. Have you changed the product policy because of the GDPR – for instance by including relevant items on compensation in case of a customer's violation of the regulative?
30. Have you in any way communicated with your customers about the GDPR – e.g. by running an awareness campaign; informed about possible GDPR consequences and their practical solutions?
31. What portion of the customers state fear of a personal data breach as a main motivational factor for taking up cyber insurance?
32. Do you have an opinion on whether it will it be feasible to cover possible administrative fines customer's might be subjected to because of their infringement of the GDPR's relevant provisions?
    - Whichever is higher of 10 000 000 EUR or 2 % of the total worldwide annual turnover of the preceding financial year (cf. article 83, point 4 of the GDPR[1])
    - Whichever is higher of 20 000 000 EUR or 4 % of the total worldwide annual turnover of the preceding financial year (cf. article 83, point 5 of the GDPR)

The NIS directive

33. Do you perceive that the EU's NIS directive on critical infrastructure[2] will drive your customers to seek more help to handle cyber risk?
34. Have you conducted any form of analysis on how the directive might affect the cyber insurance market?
35. Have you in any way communicated with your customers about the directive?

[1] http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
[2] each member country will incorporate the directive into their own national laws

The International Maritime Organization's (IMO) decision to make cyber risk management mandatory onboard ships from 2021 (cyber risk management must be incorporated into the ISM code)[3]

36. Do you consider that the IMO's decision to include cyber security into the ISM code as an opportunity to increase the number of cyber insurance customers?
37. Have you in any way communicated with your customers about this addition to the ISM code which might require certain customers to reconsider their approach to cyber security?

Conclusion

38. (Thank you. On my further process.)
39. Are there other aspects of cyber insurance you would like to discuss?

[3] http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428(98)%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf ; ISM code: "International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code)"

Appendix 3 – Generic first request to the supply-side

From: Even Langfeldt Friberg <address>
To: <recipient>
Subject: Forespørsel om mulig intervju/informantrolle for masteroppgave om cyberforsikring

[Fant deres kontaktdetaljer via <url>]

Hei,

forstår det slik at dere driver med cyberforsikring som [...].

Jeg er sisteårsstudent ved masterprogrammet for «cyber security» ved Tallinna Tehnikaülikool (Tallinn University of Technology), hvilket betyr at jeg skal gjøre en masteroppgave som skal leveres til sommeren. Veilederen min og jeg har diskutert muligheten for at jeg kan gjøre en studie på cyberforsikringsmarkedet i Norge. Slik jeg har forstått fra de rapporter jeg har kommet over, og forskningsartikkelen som har inspirert meg [1], er markedet bl.a. mindre utviklet i Norden enn f.eks. det amerikanske markedet er. En kan tenke seg at cyberforsikring alt har fått et løft, og vil bli mer sentralt, kanskje særlig grunnet Personvernforordningen som snart trer i kraft. Som en del av oppgaven er ideen min er å gjøre datainnsamling i form av semi-strukturerte intervjuer hos informanter på (a) tilbydersiden (relevante forsikringsselskaper, evt. også gjenforsikrere, forsikringsmeglere) og på (b) kundesiden, da et (mindre) utvalg av virksomheter innen en næringssektor, muligens i maritim næring (en mulig driver for utbredelse av cyberforsikring her kan tenkes å være Den internasjonale sjøfartsorganisasjonens beslutning om å gjøre cyberrisikohåndtering om bord på skip obligatorisk f.o.m. 1. januar 2021 [2, fire siste avsnitt]).

Håpet er jo at en slik oppgave kanskje også kunne være av verdi for dere.

Jeg sonderer nå hvilke potensielle informanter som kunne tenke seg å bidra - altså finner jeg ut om oppgaven vil la seg skrive. Jeg tenker at selve datainnsamlingen ville kunne finne sted i januar (da jeg er i Norge), da fortrinnsvis i en face-to-face-intervjusetting. Anslagsvis tenker jeg at en ville kunne behøve å sette av en times tid til dette.

I et forsøk på å presentere meg på en skikkeligere måte har jeg forsøkt å forklare situasjonen nærmere i denne ikke-oppførte videoen:

https://www.youtube.com/watch?v=An-COD1qiIs

Har dere spørsmål eller kommentarer tar jeg gjerne en samtale på telefon eller en e-post. Jeg ville sette stor pris på en tilbakemelding på om dere kunne tenke dere å være med på dette, men også i det fall at det er uaktuelt for dere.

Takk for tiden deres!

Best regards,

Even Langfeldt Friberg
2nd year student in MSc Cyber Security programme
Tallinna Tehnikaülikool (Tallinn University of Technology)
+47 926 28 270
evfrib@ttu.ee

[1] Franke, Ulrik. "The cyber insurance market in Sweden."

Computers & Security 68 (2017): 130-144.
[2]
http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/
Resolution%20MSC.428(98)%20-%20Maritime%20Cyber%20Risk%20
Management%20in%20Safety%20Management%20Systems.pdf

Appendix 4 – Generic first request to the demand-side

From: Even Langfeldt Friberg <address>
To: <recipient>
Subject: Forespørsel om mulig intervju/informantrolle for masteroppgave om cyberforsikring / Inquiry for possible thesis interview about cyber insurance
[...]
[English below]
Hei, god dag.
Jeg er sisteårsstudent i masterprogramstudiet i cybersecurity ved Tallinn University of Technology. Jeg holder på med datainnsamling til min masteroppgave om cyber-/dataangrepsforsikring i Norge, på tilbyder- (forsikringsselskaper, meglere) og kundesiden (virksomheter i maritim sektor). Cyberforsikring kan være ett mulig verktøy for deling eller overførsel av risiko. Emnet er aktualisert, delvis grunnet at IMO har bestemt at cyberrisikohåndtering skal inn i ISM-koden for skip.
Det er enklere å få representanter for «tilbudssiden» til å bidra i datainnsamlingen, enn representanter fra «kundesiden», noe som ikke er overraskende. Perspektiv fra «kundesiden» ville derimot kunne være meget verdifullt.
Kunne dere tenke dere å stille som informant til oppgaven min, ved at jeg får intervjue en relevant person hos dere? Kanskje er dette f.eks. en risikomanager, HSSEQ-person, ansatt som har med forsikring å gjøre, e.l. Fortrinnsvis ville dette skje ved at jeg møter personen, og jeg antar at en måtte sette av cirka en times tid i kalenderen. Jeg er interessert i både virksomheter som har tegnet, og ikke har tegnet, cyberforsikring. Alle informanter vil naturligvis anonymiseres (se forslag til samtykkeerklæring - denne kan tilpasses ved behov). Se vennligst også vedlagt intervjuguide for å forstå gangen i intervjuet/samtalen.
Mange takk, håper på respons fra dere.
Even
Best regards,
Even Langfeldt Friberg
2nd year student in MSc Cyber Security programme
Tallinna Tehnikaülikool (Tallinn University of Technology)
+47 926 28 270
evfrib@ttu.ee
Dear Sir or Madam
I'm a second year student in the cyber security master programme at Tallinn University of Technology. Currently I'm conducting interviews with companies from the supply (insurers, agents) and demand side (maritime sector) of the Norwegian cyber-insurance market, as part of the data collection for my thesis on cyber-insurance in Norway. Cyber-insurance might be one possible instrument for sharing or transfer of risk. The topic has been brought up to date, partly because of the IMO's decision to include cyber risk management in the ISM code for ships by 2021.
It's been easier to have representatives of the supply side contribute to my data collection than representatives from the demand side, which is hardly surprising. However, the possible perspectives of the demand side could be of

great value.
Would you be willing to contribute to my thesis, by letting me interview a relevant employee at your company? This individual could probably be e.g. a risk manager, HSSEQ officer, employee dealing with insurance matters, etc. If possible, I would meet the person to a face-to-face interview, and the time needed would be approximately one hour. I'm interested in having your company as a source for my thesis, regardless of whether or not the company has taken up cyber-insurance. All sources will of course be anonymized (please see my suggested interview consent form - can be adjusted if necessary). Please also find my interview guide attached, to understand the flow of the conversation.
Thank you for taking the time to consider my inquiry, I hope to hear from you.
Best regards,
Even Langfeldt Friberg
2nd year student in MSc Cyber Security programme
Tallinna Tehnikaülikool (Tallinn University of Technology)
+47 926 28 270
evfrib@ttu.ee

Appendix 5 – Institute cyber attack exclusion clause, CL380, 10/11/2003

1.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to, by, or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting froma politicalmotive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.