This is the accepted version of a paper published in *Information and Computer Security*. This paper has been peer-reviewed but does not include the final publisher proof-corrections or journal pagination.

Citation for the original published paper (version of record):

The cyber-insurance market in Norway
https://doi.org/10.1108/ICS-01-2019-0012

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

License CC BY-NC 4.0

Permanent link to this version:
http://urn.kb.se/resolve?urn=urn:nbn:se:ri:diva-40584
The Cyber-Insurance Market in Norway

<table>
<thead>
<tr>
<th>Journal:</th>
<th>Information and Computer Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manuscript ID</td>
<td>ICS-01-2019-0012.R1</td>
</tr>
<tr>
<td>Manuscript Type:</td>
<td>Original Article</td>
</tr>
<tr>
<td>Keywords:</td>
<td>cyber-insurance, Norway, NIS Directive, GDPR, insurance coverage, insurance adoption</td>
</tr>
</tbody>
</table>
1. Introduction

Cyber-insurance is an essential tool to transfer financial risks related to IT from an insured to an insurer (Böhme and Schwartz, 2010). Such insurance products are apt to transfer the residual risk remaining after suitable technical precautions, particularly low-frequency-high-impact risks (Mukhopadhyay et al., 2013). Cyber-insurance products stem from the 1980s, but the scholarly discussion of it as a risk management tool dates to the turn of the millennium (Böhme and Schwartz, 2010). Schneier argued early for the inconceivability of not investing in cyber-insurance, stating that ‘[i]n the future, the computer security industry will be run by the insurance industry’ (Schneier, 2001).

Conceptually, modern cyber-insurance products typically provide three main kinds of coverage: (a) first-party loss; (b) third-party loss; (c) other benefits (e.g. regular security audits, credit or identity monitoring, public relations costs after an incident) (ENISA, 2017). Though products are similar on this conceptual level, ambiguity and misunderstandings about coverage remain a significant obstacle to the cyber-insurance market (OECD, 2016). For example, incidents considered acts of war or terrorism are excluded from policies (Payne and Komisarczuk, 2017) although there is a huge ambiguity regarding the definitions and attributions of these threats in the cyberspace. Similarly, system management failures or interruptions in external IT services are not covered in all policies (Franke, 2018).

Cyber-insurance is receiving much attention in policy circles. International organisations such as the OECD (2017, p. 140) and ENISA (2017) are studying its policy implications, in efforts to improve cybersecurity decision-making and societal cyber resilience. When the World Economic Forum presented a ‘playbook’ for public-private collaboration for increased cyber resilience in January 2018, cyber-insurance had a dedicated chapter (World Economic Forum, 2018). The market is also growing: for example, the premiums written on the US market grew 32% in 2017, with direct premiums reaching $1.8
billion (‘Smaller Firms…’, 2018). However, there is also scepticism about cyber-insurance.

One notable sceptic is investment guru Warren Buffett, who in May 2018 urged caution,
quoted as saying that ‘I don’t think we or anybody else really knows what they’re doing when
writing cyber [insurance]’ (Chiglinsky and Basak, 2018).

This article explores the Norwegian cyber-insurance market from the supplier-side
perspective from the viewpoint of two recent significant European legislation efforts; the
General Data Protection Regulation (GDPR) and the Network and Information Security (NIS)
Directive.

Norway is a technologically advanced country that ranked fourth in the World
Economic Forum’s Networked Readiness Index 2016 (Breene, 2016), second only to
Singapore and its Nordic neighbours Finland and Sweden. Nevertheless, Norway is regarded
as a cyber-insurance adoption laggard among the Nordic countries (Franke, 2017), and
estimated Norwegian cybercrime loss is 0.64% of GDP, above the EU average of 0.41%
(McAfee and CSIS, 2014). The GDPR and its administrative fines are widely regarded as an
important factor in increasing the demand for cyber-insurance (OECD, 2017; Woods and
Simpson, 2017). Therefore, it is interesting to note that Norway is one of only two countries
in the European Economic Area which allow GDPR fines to be insurable (DLA Piper &
AON, 2019). Additionally, critical infrastructures covered by the NIS Directive are very
important to Norway, with its highly developed oil and maritime industries.

Thus, Norway is an interesting object of study, where it is reasonable to believe that
valuable lessons can be learned about the adoption and dynamics of cyber-insurance markets
outside the US, which is the earliest adopter of the cyber insurance.

More specifically, the following three research questions were investigated by semi-
structured interviews with a representative sample of Norwegian insurance actors:

- RQ1: How can the current market be characterised?
• RQ2: What are the supplier-side’s perspectives on how the GDPR and the NIS Directive impact the cyber-insurance market?

• RQ3: What is the supply-side’s experience with cyber risk awareness and cyber-insurance uptake among the general demand-side?

The remainder of this paper is structured as follows. The next section offers a literature review of related work. Section 3 provides some background on the GDPR and the NIS directive, followed by a description of methodology in Section 4. The results are presented in Section 5 and further discussed in Section 6. Finally, Section 7 concludes the paper.

2. Related work

Cyber-insurance has received increasing academic attention in recent years. In particular, theoretical studies have contributed to an increased understanding of relevant topics such as asymmetric information (Shetty et al., 2010), interdependence (Böhme and Kataria, 2006; Zhao et al., 2013), and externalities (Pal et al., 2014). However, the development of cyber-insurance theory has not been matched by empirical research. For example, Böhme & Schwartz (2010) noted that general insurance research differs from cyber-insurance research in that the former follows existing business practices, whereas the latter develops theory first, in the hope of finding a practical business solution. In a more recent review, Eling & Schnell (2016) conclude that more empirical research is needed, both on the demand- and the supply-sides. Our study aims to contribute to the growing body of more practice-driven and empirical cyber-insurance research, by investigating actual market practices in Norway. Though this is a novel object of study within cyber-insurance research, some closely related work does exist, outlined in the following.
The Norwegian cyber-insurance market has previously been investigated by Tøndel et al., who conducted interviews with a limited number of key insurance companies offering cyber-insurance on the Norwegian market in 2015 (Tøndel et al., 2016). This differs from our study, in that no other relevant actors such as brokers were included.

Tøndel et al. aimed to identify challenges and cyber-risk assessment practices of insurance companies. However, findings were scarce as companies did not give ‘any clear priorities on which risk factors they consider most important’ (Tøndel et al., 2016). Dependent risks, i.e. incidents impacting many customers simultaneously, was identified as a concern to insurers. This finding is in line with the established cyber-insurance literature (Böhme and Kataria, 2006; Anderson and Moore, 2006). Some insurer dilemmas were also identified, e.g., the difficulty to keep up with a fast-moving cybersecurity field; the lack of accurate historical data and statistics; and the need to spread the risk among more customers. Again, these dilemmas are well-known from the literature (Franke, 2017; Shetty et al., 2010; Bandyopadhyay et al., 2009; Wheeler et al., 2015).

Our work updates that of Tøndel et al. with data some three years more recent – which is significant for a fast-expanding market like cyber-insurance – and complements it with investigations GDPR and NIS, which are widely seen as central factors for the cyber-insurance market (OECD, 2017; Franke, 2017).

Another relevant empirical study is Franke’s characterisation of the Swedish cyber-insurance market based on semi-structured interviews (Franke, 2017). The ten insurance companies interviewed represent essentially the entire Swedish supply-side at the time, and findings include information on coverage, market segmentation, the underwriting process, and how premiums are determined. An interesting finding in our context is that Norway is found to be somewhat behind Sweden, Denmark and Finland in cyber-insurance uptake (Franke, 2017, p. 136).
To summarise, our investigation complements previous work by investigating the Norwegian market. The unique contribution of this study is an investigation of GDPR and NIS impacts on the cyber insurance take-ups in a European country. This is significant, as the impact on cyber-insurance companies of this new legislation has, to our knowledge, been systematically investigated in the literature previously. The obtained results would guide the national/European level decision makers and insurance sector in shaping policies on cyber insurance.

3. GDPR and NIS

The GDPR (EPEC, 2016a) took effect in the EU on 25 May 2018, and in Norway on 20 July 2018. The regulation protects personal data, e.g. by requiring data controllers and data processors to ‘ensure a level of security appropriate to the risk’ by implementing ‘appropriate technical and organisational measures’ (2016a, art. 32). Personal data breaches must be reported to the national supervisory authority within 72 hours of the data controller becoming aware of them (2016a, art. 33), and incidents must also be communicated to the data subject (2016a, art. 34). Arguably, the most famous, or infamous, feature of the regulation is the possibility of imposing administrative fines of up to 4% of an organisation’s annual worldwide turnover, or up to 20 million EUR, whichever is greater, for certain infringements (2016a, art. 83).

The GDPR has widely been seen as a driver of increased cyber-insurance adoption in Europe (OECD, 2017; Woods and Simpson, 2017) and also as a potential game-changer for the sharing of cyber-incident data (Camillo, 2017), possibly enabling more actuarial pricing. An important uncertainty concerning GDPR has been whether the administrative fines will be insurable or not, and some have argued that this must be the case for the regulation to increase demand for insurance (Woods and Simpson, 2017).
EU member states’ have been obliged to implement the directive on security of network and information systems, the NIS Directive, in their national legislation since May 2018 (EPEC, 2016b), and the directive is under evaluation in the EEA/EFTA countries, to which Norway belongs. The aim is to enhance the cybersecurity level in the Union (European Commission, 2016). In contrast to the GDPR, the NIS Directive addresses the loss of service rather than the loss of data. Essentially, the directive requires that every country establishes a CSIRT unit which participates in a union-wide CSIRT network, and ‘operators of essential services’ (EPEC, 2016b, art. 14) and ‘digital service providers’ (2016b, art. 16) implement technical and organisational security measures and notify CSIRTs about significant incidents.

It is reasonable to believe that the NIS Directive could affect the cyber-insurance market. Especially those companies that eventually 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. Similarly to the GDPR, the impact of the NIS mandatory incident reporting has been discussed in the literature (OECD, 2017; Laube and Böhme, 2016), and it is possible that such incident data could become useful as actuarial data on cyber-incidents. Askvik thus points at the need for private-public cooperation to enable supply-side actors to take part in this information-sharing (Askvik, 2018, p. 54).

4. Methodology

To gather the market’s first-hand experiences, views, opinions, and certain figures, semi-structured interviews with relevant supply-side actors were conducted. The interviews were semi-structured in the standard sense that though questions were defined beforehand (and also sent to informants prior to the interviews) they were open-ended, allowing informants to provide additional information, e.g. examples, and giving the interviewer freedom to ask follow-up questions. Still, adhering to an interview guide with a set of questions increases
reproducibility, strengthening reliability (Malt, 2015).

4.1. Informant selection

The supply-side of the Norwegian cyber-insurance market consists of insurance companies, reinsurers, and insurance brokers.

In a first attempt to get an overview of relevant insurance companies, Finance Norway was contacted in October 2017. Unfortunately, they could not provide a list of all insurance companies offering cyber-insurance. Instead, they offered a list of all actors offering liability insurance and recommended it as a starting point. 18 supply-side actors were approached; 13 insurance companies and five insurance brokers. In the end, nine of these (seven insurance companies and two brokers) agreed to be interviewed. In addition, another broker gave some input by email. The study is not a census, as it does not include all insurance companies that offer cyber-insurance coverage in Norway. Still, the study covers a sample of informants that are major actors offering their products to variously sized customers from many industries. Cyber-insurance can also be bought by Norwegian organisations from international insurers without a physical presence in Norway, but these organisations were deemed out of scope. We assessed that their specific views about Norway would be limited; Norwegian organisations being sufficient to characterise the local market.

4.2. Interviews

All nine interviews were conducted face-to-face at the office of the company in Norwegian or English. Two of the interviewees were brokers, four were underwriters, the rest being, e.g., product manager, practice leader or deputy head of cyber and technology branch. With informant permission, all interviews were recorded for subsequent transcription.
4.3. Analysis

Each interview was transcribed using the software MAXQDA 2018, which allows for text segments to be tagged with codes, e.g., identifying question and informant, but also topics such as NIS, GDPR, information sharing. This encoding was a key enabler for subsequent analysis, as the codes, once set, allow convenient searching of the material. Thus, when 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.

4.4. Ethics

All informants were anonymised in the final text, with no individuals or companies mentioned. As Norway is a small market, this was seen as a prerequisite for the informants to agree to participate. After the interviews, all informants were given an opportunity to correct the interview transcripts. Once the research project is completed, the audio recordings will be deleted according to NIST guidelines (Kissel et al., 2014, pp. 36,39).

5. Results

[Table 1 near here]

5.1. Characterisation of the market

Table 1 characterises informants’ cyber-insurance offers, including 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. Some clarifications are appropriate here: First, the number of claims refers to all claims that have been received in Norway since the launch of the product. Second, IC1 confirms that they have had claims, but will not disclose how many. Third, since brokers do not underwrite policies themselves but only serve
as intermediaries, several columns are not applicable to them. The number of customers is the
number of Norwegian customers that have taken up cyber insurance from the company in
question. MIC1 does not have a dedicated cyber-insurance product on the market, so several
columns are not applicable to them. There is no lower bound for the size of SMEs.

5.1.1. Coverage

The insurance companies offer standard cyber-insurance package solutions, and tailor-made
coverage can be offered. An overview of standard packages is given in Table 2. Of the six
general insurance companies with a dedicated cyber-insurance product, only one lacks
cooperation with a consultancy to offer IT expertise first response crisis management (in the
standard product).

The coverage offered by IC5 and MIC1 differ from the other informants’. The former
in that their standard product is limited to covering first-party data restoration and system
clean-up costs following a cyber-attack, though more comprehensive coverage can be—and
has been—offered upon the broker’s request. The latter in that they as a marine insurance
company do not currently offer a standalone cyber-insurance product.

5.1.2. Underwriting

Generally, the underwriting process is led by questionnaires on implemented technical and
organisational cyber security measures. The answers constitute an essential source of
information for insurers to assess the risk and decide whether to offer insurance. In many
cases both management and technicians need to be involved to answer satisfactorily.

Automated online underwriting, enabling a potential customer to identify the profile of
their organisation and then immediately receive a quote from the insurer, is employed by two
insurers whose main market segment is SMEs (IC1, IC2). Additionally, two companies (IC3, IC6) are developing similar solutions aimed at smaller-sized organisations. More complex organisations—operating in specific high-risk industries, exceeding an absolute limit in turnover, requiring tailor-made coverage, etc.—follow a traditional approach by being individually assessed by an underwriter. When assessing more complex organisations, underwriters occasionally ask the market at Lloyd’s of London for a quotation.

5.1.3. Claims

Insurers report relatively few received claims from customers, as can be seen from Table 1. In the case of informant IC2, it is noteworthy that of approximately 30 Nordic claims, 50% are said to have come in Norway, even though Norwegian organisations account for a mere 900 out of 6000 policies held in the Nordics. Other informants do not report a similar disproportion. Malware attacks are reported as the predominant cyber-incident type: IC3 says that the two ransomware incidents reported triggered first response IT assistance, and that the cases were successfully resolved by decrypting the customer organisations’ files without paying the ransom or even needing to resort to backups. Some informants (IC1, IC4) report that customers might file a claim after falling victim to CEO fraud, and this can be problematic, as it is not covered by their policies.

5.1.4. Market challenges

Insurers whose primary market segment is smaller organisations describe similar market challenges. It is frequently mentioned that many customers do not seem to understand why they should invest in a cyber-insurance product, especially if they are not aware of any incidents having affected themselves, and that many do not see how cyber-risks pose a real threat to their organisation. The attitude that serious cyber-incidents ‘will not happen to us’ is widespread, according to IC2, IC4, and IC5. The insurers whose main market segment is
larger enterprises (IC3, IC6) both remark that the cyber-insurance concept is met with a
certain degree of opposition from organisations’ IT staff. This opposition, despite having
diminished recently, is also mentioned as a complicating factor in supplying insurance by IC4
and B2.

From a broker’s point of view, it can be difficult to explain the variance in the
premium the customer will have to pay, as quotes are procured from several insurers. The
various products available on the market are often communicated differently from the
insurers, and that is a complicating factor, B1 says. B1 also voices uncertainty concerning
systemic risk: that possible major incidents in the future might strike several organisations
simultaneously.

5.1.5. Differences from other markets

Insurance companies active on several Nordic markets say that qualitatively there are minor,
if any, differences (e.g. pricing) between the products they offer on these markets. On the
formal side, one informant (IC4) informs that their cyber-insurance product is categorized as a
property product in Norway, but a liability product in Sweden and Denmark. Norway is
consistently perceived as the least mature Nordic market, in the sense of companies’ uptake of
cyber-insurance.

One informant (IC6) that mainly deals with larger companies 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. IC2 does
not immediately recognize the brokers’ part in preparing the Finnish market for cyber-
insurance as a concept but adds that there have existed limited cyber aspects in insurance
products in Finland for many years, if not standalone products. The same informant is of the
impression that the Norwegian demand-side, in general, does not seem particularly worried
about cyber-risks, as uptake has been considerably lower than in Sweden.
5.2. GDPR

5.2.1. Effect on the adoption rate

In the spring of 2018, prior to GDPR implementation in Norway, when the data collection of this study took place, the insurance-side was split on whether the forthcoming regulation had affected the adoption rate of cyber-insurance: opinions differed from having already played a significant role, to being less important.

Most insurers (IC1, IC2, IC4, IC5, B1) were aligned in downplaying the GDPR’s effect on the uptake of cyber-insurance. Instead, it was believed (IC1) that any cyber-insurance adoption effect would appear only after the implementation date. Media coverage of the very first companies that will be investigated or punished for GDPR non-compliance was thought to lead more companies to look for cyber-insurance (IC1, IC5). However, GDPR is mentioned as functioning well as an ‘icebreaker’ or the starting point in conversations about cyber-insurance with a customer (IC2, IC3, IC4). The GDPR is hardly any prominent reason for considering cyber-insurance among B1’s customer base, shipping companies.

Two informants assess that the regulation indeed has affected uptake: one of them (IC3) stressing the GDPR as the principal reason why organisations are considering cyber-insurance. The other informant (IC6) remarks that even though the regulation is a factor for increased adoption, it is not as critical as one might think. This is primarily because organisations are still focused on getting ready for the GDPR in its own right, and because of the nature of insurance: it covers the residual remaining despite other precautions.

One informant (IC2) brings the perspective that cyber-insurance policies do not intend to give complete coverage for the regulation, and that many organisations do not seem to adequately understand the regulation’s implications. The informant maintains that essentially the GDPR is about how to deal with personal information which belongs to the scope of liability insurance.
5.2.2. Fear of personal data breach as a reason to insure

None of the informants assess that a primary reason for customers’ uptake of cyber-insurance is that they fear a data breach of personal data. It is commented (IC1) that many customers have been preoccupied with the question of punitive fines. Customers have realised that the first-party costs—on which European cyber-insurance traditionally has focused—are more important, according to IC2 and IC4.

5.2.3. GDPR’s influence on the product

Two insurance companies (IC1, IC2) assess that GDPR implementation will change parts of their policies on third-party liabilities, i.e. covering for notification costs; the four remaining says that it does not affect their policies as such. Two insurers (IC1, IC6) highlight that their risk assessment of customers is affected by the GDPR’s implementation in Norway; in IC6’s case this is the case in customer meetings, where companies showing signs of being insufficiently prepared will be considered riskier to cover.

The two insurers (IC3, IC6) whose main market segment is larger organisations are used to regulations similar to the GDPR from other parts of the world, and their cyber policies have considered regulatory fines from the outset.

5.3. The NIS Directive

From the interviews, it appears that the Directive has not yet impacted the supply-side. No informant believes the prospective directive has affected cyber-insurance uptake. It has not been a topic of conversation with customers, nor has it been used to e.g. communicate with customers about cyber-insurance. The informants are not 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 this regulation had changed their product policies. However, one informant (IC1) remarks that more generally, customers who take new regulations that aim to
enhance cybersecurity into account, will be regarded as ‘more secure’ than those who do not, and it will be easier as an insurer to take on their risk. This is also implied by others (IC6), who comments that the directive has not been implemented in their underwriting process yet.

5.4. Cyber risk awareness and cyber-insurance uptake among the general demand-side

The supply-side assesses that organisations’ understanding of both cyber risk and how cyber-insurance can address it varies considerably, with larger organisations generally being at a more sophisticated level than smaller. This is the impression across all industry sectors, including maritime, though the number of informants from the maritime sector is small. Financial institutions are designated as having been the prime movers in terms of taking up cyber-insurance coverage (IC3). Larger companies in retail, production, and technology are also mentioned as having shown interest in the product (IC6). IT industry companies are mentioned as being the most cyber risk-aware (IC2).

The Norwegian demand-side has recently shown more interest in, if not taken up, cyber-insurance. One informant characterises the general customer as having been in large part ‘unconscious’ of cyber risk until 2017 (IC4), and describes the sale of cyber-insurance policies as having progressed from ‘low’ to still ‘low, medium’, adding that despite heightened interest there is little acceptance and action. This can be contrasted with descriptions of a market that has seen an increased uptake of cyber-insurance in 2017, and continued positively so far in 2018 (IC3). Especially, ransomware attacks and their media coverage are mentioned as factors that have led many organisations to begin the process of considering cyber-insurance coverage (IC2, IC3, IC4). Other factors mentioned (IC4) include that there are now more insurers on the market offering a cyber-insurance product, and that brokers are more active. More companies’ board members and executive managers have realised that they have a duty to uncover cyber risk by conducting risk analyses, and
subsequently take some measure to mitigate that risk. The informants have different experiences with SMEs’ interest in cyber risk and relevant insurance solutions; while one informant (IC2) reports of increased attention from this group, others (IC4) find that the typical SME still do not seem to identify with such topics.

6. Discussion

The discussion is divided according to the topics of the results section.

6.1. Characterisation of the market

On a general level, the Norwegian cyber-insurance market is similar to others, especially the Swedish one. Similarities include small uptake relative to the size of the population of all companies, few claims received by insurers, and rapid growth with many recent product launches. However, there are also differences. All interviewees share the understanding that cyber-insurance uptake has been lower in Norway than in the other Nordic countries. This confirms the finding in (Franke, 2017, p. 136).

The low claims-rates illustrate a pervasive cyber-insurance challenge: lack of reliable and comparable data. Not only does this make it more difficult for insurers to price their products correctly, it also makes policy-makers, researchers and the general public less informed about the state of cyber-insurance. Various data exchange and incident reporting schemes are often discussed in the policy debate, and we will revisit this in section 6.4.

In section 5.1, several interviewees (IC3, IC4, IC6, B2) mention scepticism about cyber-insurance in IT departments—the perception that taking up cyber-insurance represents a lack of confidence in them. Schneier argued already in 2001 that many ‘computer science professionals’ would have a hard time understanding risk management through insurance. Nevertheless, findings in section 5.4 suggest that IT and technology companies, especially larger ones, are among the more risk-aware and that the internal power struggle has recently
become less of a problem. Possibly, increased media-reporting of cyber-incidents, an increased cyber-insurance market offering, and increasing numbers of individuals with technology backgrounds in executive management have contributed to convincing IT staff about the virtues of cyber-insurance to manage residual risk. To pre-empt unwarranted scepticism, both academic and more professional training institutions may wish to consider including cyber-insurance in their curricula, to demystify it and explain how it can be used in concert with other tools to enhance security.

6.2. Ambiguity of coverage

It is a well-known challenge that the terms and conditions of cyber-insurance policies are not always clear (ENISA, 2017; Franke, 2017) and this is also a common explanation of low global cyber-insurance uptake (OECD, 2017, p. 192).

Our study confirms this ambiguity in Norway. From the GDPR perspective, many customers misperceive cyber-insurance products to cover any GDPR related costs (IC2), whereas the typical actual coverage mostly relates to breach notification costs, though legal costs and damages from claims could potentially be covered as well.

From a policy perspective, it is interesting to note that this challenge is currently being addressed both by public institutions such as the ENISA (2017) and market actors. In October 2018, a group of European industry bodies including Insurance Europe published a guide to help potential customers better understand cyber-insurance coverage (BIPAR et al., 2018).

The Norwegian experience confirms the need for such initiatives. National insurance industry organisations may wish to consider complementing international initiatives with addenda reflecting local legal and market conditions.

6.3. GDPR

As seen in section 5.2, the informants agree that the GDPR influences the cyber-insurance
market by functioning as a topic to start cyber-insurance conversations with customers, but there is some disagreement as to what degree the regulation has been driving new customers so far. The informants that deal mainly with larger customers assign greater importance to GDPR as a contributing factor than the informants that deal more with SME customers. This is reasonable, considering that larger, more sophisticated companies are generally more prepared for the regulation, having spent more time getting ready. Additionally, brokers are mentioned as being especially preoccupied with the GDPR, and intermediaries are more often involved when insurers deal with larger companies. However, it is still early to evaluate the impact of the GDPR.

6.4. The NIS Directive

The findings consistently show that the NIS Directive has not yet influenced the cyber-insurance supply-side in Norway, though insurers and brokers have a favourable view of organisations that generally strive to be compliant with regulations. Such a lack of influence makes sense, considering that the directive is still under evaluation in the EEA/EFTA countries, even though Norwegian authorities have found it EEA relevant and acceptable.

It is somewhat more surprising that insurers do not express 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. While industry organisations such as Insurance Europe have articulated a desire for both GDPR and NIS incident data to be shared with insurers, at least in Norway, insurers seem oblivious to this aspect of NIS. From a policy perspective, national insurance industry organisations may wish to further bring this to their members’ attention.

Germany took important steps towards securing critical infrastructures earlier than the other EU states in the enactment of its IT Security Act in 2015, before the adoption of the NIS
Directive. However, the German cyber-insurance market for critical infrastructures has been described as non-existent (Baban et al., 2017). Although this analysis supports that market improvement may be possible with appropriate incentives, it refers to more structural weaknesses such as uncertainty about cyber threats, a wide spectrum of potential losses and liability issues for damages. Even if critical infrastructure owners develop a deeper understanding of the NIS Directive, the characteristics of cyber threats in critical infrastructures may impose more demanding obstacles to cyber-insurance underwriting. In this respect, sharing of incident data, researching critical infrastructure cyber threats and clarifying the roles of infrastructure companies and government, respectively, in major incidents become much more important.

6.5. Reliability

Reliability is strengthened by the participation of a reasonable number of fairly diverse companies. Seven insurance companies were interviewed; two companies mainly dealing with larger enterprises through brokers, four having mostly SME customers, and one being a marine insurer. As such, the informants represent several different kinds of insurers.

Nevertheless, the investigation is not a census: At least one company launched its product in February 2018 and was not included in the study. At least three relevant insurers on the market did not participate, but they cannot be said to represent significantly different kinds of actors. All in all, six out of the seven insurers included currently have a cyber-insurance product on the Norwegian market, and it is reasonable to consider them as making up a representative sample of the full population of insurance companies with a presence in Norway offering cyber-insurance coverage. Thus, there is no reason to believe that a different sampling strategy or a bigger sample would have significantly affected the conclusions.

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 is also strengthened by the fact that the interviews were audio-recorded and subsequently transcribed, reducing the risk that relevant information is missed.

6.6. Validity

Validity is threatened by using interviews as the research method. One threat to 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 rationalise a narrative of events that have happened (Andersen, 2006, pp. 288,292). Nevertheless, all informants—underwriters, analysts, product managers—are qualified interviewees with knowledge of cyber-insurance, strengthening validity.

7. Conclusion & Future Work

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. The study confirms other studies’ assertions that despite growth, the Norwegian cyber-insurance market is the least mature of the Nordic markets, though this should be interpreted with some caution as it is not backed by statistical evidence.

Insurers and brokers perceive that there are demand-side actors across the entire 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.

Earlier studies and commentators have anticipated the implementation of the GDPR to increase in the uptake of cyber-insurance. This study shows that most suppliers find the effect so far modest, and that the regulation first and foremost functions as an icebreaker when
talking to customers about cyber risk and introducing cyber-insurance. Although larger enterprises are more prone to use cyber insurance as a risk transfer option for GDPR-related compliance risks, it is reasonable to expect a rise in demand from SMEs in the future, due to their growing compliance concerns.

Some suppliers that are not used to similar legislation from outside the EEA have had to make minor changes to their policies regarding covering for notification costs in case of a privacy breach. However, the general ambiguity problem regarding terms and conditions of policy coverage in cyber insurance still persists in GDPR related issues. With GDPR recently coming into force, future studies will have to further assess its impact on market size and other implementation details of insurance life-cycle.

The study also shows that the NIS Directive has had little or no impact on the Norwegian cyber-insurance market so far, based on the response from the interviewees. High margins of uncertainty in the probability and impact of cyber threats in critical infrastructures pose an important challenge for insurers. However, incident reporting addressed by the directive could help the relevant decision-makers and researchers in providing data for comprehending this uncertainty.

The results of this study provide a valuable outcome for national/EU level decision-makers, the insurance sector and researchers in this field. Some specific policy lessons for different stakeholders have been identified. Insurance industry organisations may wish to continue their work on explaining and clarifying cyber-insurance coverage in light of GDPR and NIS, possibly complementing existing international guidelines with national addenda, and further bring the incident-reporting requirements of NIS to their members’ attention. Cyber-security educators and trainers may wish to add cyber-insurance to their curricula, to prevent IT staff bias against it. National governments should both study best practices from abroad
and encourage innovation at home in order to find the best role of cyber-insurance in
promoting a more secure society.

A few avenues for future work can also be identified. First, it would be interesting to
further investigate the risk perceptions of various stakeholders. For example, could low
insurance uptake be explained by the fatalism identified by Eling & Schnell (2016) (e.g., “it
will not happen to me” or “my data is not interesting enough”)? Second, given the relatively
small impact of GDPR and NIS observed so far, it is worth further exploring the roles of
(trans-)national legislators, e.g., understanding their perspectives and the expected impact of
legislation related to cyber insurance. Third, as the implementation of GDPR is ongoing and
the first infringement cases have just been publicized (e.g., the case of British Airways), the
continuing impact of GDPR on cyber insurance take-up (in Norway and elsewhere) could be
re-evaluated periodically in a longitudinal study. Fourth, as cyber insurance up-take grows,
accumulation risk becomes ever more important to manage. Thus, following the
recommendations of Falco et al. (2019), it would be highly interesting to conduct further
interviews with cyber insurance providers, reinsurers and actuaries to gain insight into the
kinds of accumulation risk scenarios they envision.

Acknowledgments

The authors would like to thank all informants for agreeing to be interviewed and for
generously sharing their insights. U. Franke was supported by the Swedish Civil
Contingencies Agency, MSB, agreement no. 2015-6986.

8. References

Andersen, S. S. (2006) 'Aktiv informantintervjuing', Norsk statsvitenskapelig tidsskrift,
22(03), pp. 278-298. Available at: https://www.idunn.no/nst/2006/03/aktiv_informantintervjuing
314(5799), pp. 610-613. doi:10.1126/science.1130992


Small *Firms Opting Out of Otherwise Soaring Cyber Insurance Market*: A.M. Best (2018): Carrier Management. Available at:


Table 1. Overview of informants.

<table>
<thead>
<tr>
<th>Informant</th>
<th>Org. type</th>
<th># customers</th>
<th># claims</th>
<th>Coverage launch</th>
<th>Main market segment</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC1</td>
<td>Insurance</td>
<td>N/A</td>
<td>YES</td>
<td>2016</td>
<td>SME</td>
</tr>
<tr>
<td></td>
<td>company</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IC2</td>
<td>Insurance</td>
<td>~several hundred</td>
<td>~15</td>
<td>2015</td>
<td>SME</td>
</tr>
<tr>
<td></td>
<td>company</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IC3</td>
<td>Insurance</td>
<td>~50</td>
<td>2</td>
<td>2012</td>
<td>Large enterprises</td>
</tr>
<tr>
<td></td>
<td>company</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IC4</td>
<td>Insurance</td>
<td>~250</td>
<td>0</td>
<td>2017</td>
<td>SME</td>
</tr>
<tr>
<td></td>
<td>company</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IC5</td>
<td>Insurance</td>
<td>~5</td>
<td>0</td>
<td>2017</td>
<td>SME</td>
</tr>
<tr>
<td></td>
<td>company</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IC6</td>
<td>Insurance</td>
<td>~10</td>
<td>0</td>
<td>2014</td>
<td>Large enterprises</td>
</tr>
<tr>
<td></td>
<td>company</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B1</td>
<td>Marine broker</td>
<td>~5</td>
<td>N/A</td>
<td>2016</td>
<td>Marine</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B2</td>
<td>Broker</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIC1</td>
<td>Marine</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Marine</td>
</tr>
<tr>
<td></td>
<td>insurance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>company</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Informant</td>
<td>Restoration of data, software and systems</td>
<td>Business interruption</td>
<td>Business interruption at external service provider</td>
<td>Communication costs</td>
<td>Ransom payment for cyber extortion</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------</td>
<td>-----------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>IC1</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IC2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IC3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IC4</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IC5</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IC6</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>