Demand side expectations of cyber insurance

Ulrik Franke
RISE Research Institutes of Sweden
Kista, Sweden
ulrik.franke@ri.se

Per Håkon Meland
SINTEF Digital and
Norwegian University of Science and Technology
Trondheim, Norway
per.h.meland@sintef.no

Abstract—Cyber insurance has attracted much attention from both practitioners, policymakers and academics in the past few years. However, it also faces some challenges before it can reach its full potential as a tool for better cyber risk management. One such challenge is the gap between what customers expect and what insurers really offer.

This paper investigates this gap empirically, based on interviews with informant companies in Norway and Sweden considering cyber insurance. The expectations expressed in the interviews are compared to anonymized incident claims reports and claims statistics for 2018 from a global insurance intermediary.

The results show no obvious pattern of discrepancies between different domains. However, informant expectations on business interruption coverage are much greater than one would expect from its share of claims. In this respect, informant expectations on business interruption coverage are more aligned with some recently published scenarios on possible major business interruptions.

Index Terms—cyber insurance, company expectations, cyber claims data, cyber coverage, threats

I. INTRODUCTION

Cyber insurance has reached its age of adolescence, with sporadic growth spurts and a somewhat confusing relationship with more mature siblings such as crime, property and liability insurances. Part of this confusion stems from misaligned expectations. In an analysis of obstacles to more mature cyber insurance, the OECD identified misunderstandings about coverage and unsuitability of the coverage available as two of the main concerns on the demand side [1]. Despite efforts to rectify this, e.g., by Insurance Europe [2], it is safe to assume that misaligned expectations persist. Indeed, this is to be expected, as new products and new players are entering the market, and as companies with little experience of cyber insurance and perhaps cyber risk management as such look for appropriate insurance coverage. Furthermore, the ambiguity in the cyber insurance policy language should not be underestimated [3], even though there are efforts to standardize terminology [4].

The purpose of our research has been to examine the expectations that early and prospective customers have towards cyber insurance, and see if these are in line with contemporary incidents and claims. If there are discrepancies between what the customer needs, what the product offers and what kind of incidents take place in the real world, cyber insurance will struggle reaching adulthood.

Our research approach has been to perform qualitative interviews with companies in Sweden and Norway. These two countries are at the top of the Digital Evolution Index [5], which means that they have an economy that relies strongly on the digital infrastructure, hence constituting a region where cyber insurance should be able to get a foothold. The results from these interviews have been compared with reports describing recent incident claims, claims statistics from 2018, as well as data breach statistics for different industry domains and a few cyber insurance loss scenarios. The use of these disparate data sources reflects a fundamental and well-known problem with cyber insurance: lack of data on cyber incidents [1]. Nevertheless, we believe that the sources used give interesting perspectives on our research, even if definite answers cannot be found.

We have tried to address the following research questions:

1) Are there different expectations in different business domains?

2) Are there discrepancies between coverage expectations and the costs of prevalent incidents as seen in incident data?

3) Are there discrepancies between coverage expectations and the costs of prevalent incidents as seen in scenarios?

The remainder of the paper is structured as follows. Section II gives a brief overview of related work. Section III details our employed method, before Section IV summarizes the results from customer interviews and incident data. A discussion and analysis of these results are presented in Section V. Section VI concludes the paper and also gives some directions for future work.

II. RELATED WORK

Marotta et al. [6] provide a comprehensive review of the available cyber insurance literature up until 2017. They point out that there has been a “slow start and many problematic issues”, and enlist a number of research gaps where many are related to lack of experience. The main body of this literature has been focused on topics related to the provider side, and this has been the trend among the most popular papers in recent years as well, e.g. the cyber insurance assessment process [7], insurance policies analysis [8], insurance claim disputes [9], [10], [11], contract design and pricing [12], [13], [14] and

U. Franke was partially supported by the Swedish Civil Contingencies Agency, MSB (agreement no. 2015-6986). P.H. Meland was supported by the Norwegian Research Council (agreement no. 259869).
characterisation of markets and trends [15], [16], [17], [18], [19], [20], [21], [22] to mention a few.

Our work is mostly concerned with the demand side of cyber insurance. Here, the recent literature is rich on various investment strategies. For instance, Wang [23] proposes analytical models to quantify effects of security spending, including cyber insurance. He also suggests how innovative cyber insurance products should look like. Hoang et al. [24] propose an algorithm that owners of electric vehicles can use to determine whether to use cyber insurance as a risk transfer option. Bodin et al. [25] have created a model for selecting the optimal set of insurance policies. Here, it is pointed out that “cybersecurity insurance premiums are commonly viewed as being poorly aligned with the risks and coverage needs of private sector firms”. Tosh et al. [26] use game theoretic models to study self-defence investment for organisations, optimal attack rate for adversary and optimal coverage level for insurers. Similarly, Massacci et al. [27] use game theory to model firms, attackers, insurers and a public policy coordinator, where their findings show that the aggregated security level of the targets may be eroded. Mukhopadhyay et al. [28] propose a framework that allows organisations to select among cyber insurance, self-insurance or self-protection as a strategy to minimize losses. Meland and Seehusen [29] have suggested a data-driven decision support model for companies considering buying cyber insurance. Shetty et al. [30] propose a tool that allows organisations reduce insurance premiums by optimally chosen mitigation policies. Vakilinia and Sengupta [31] present three models where organisations collaboratively insure a common platform instead of themselves.

Unlike these contributions, our approach has been to empirically investigate the expectations towards cyber insurance. The most closely related paper that we are aware of is by De Smidt and Botzen [32], who have analysed professional decision makers’ perceptions of cyber risks. They found that the “overall awareness of the cyber risks is high, the perceived probability is high, but expected impacts of a cyber-attack may be underestimated”. Another notable finding was that “the low uptake of cyber insurance may be explained by the low expected damage of a cyber-attack”.

III. METHOD

A. Company interviews

In the autumn of 2016, interviews on cyber insurance were performed with 10 Norwegian companies (4 of which had not considered cyber insurance previously, 3 of which had actively decided not to procure, 2 of which were considering, and 1 of which had acquired insurance). These results were first partially reported in [33], but orientated towards what kind of uncertainties existed as seen from the demand side. To complement the initial Norwegian results, a follow-up study was conducted in Sweden in the autumn of 2018. For maximum relevance, only companies who had actively considered cyber insurance were approached. 3 companies were interviewed (2 of which were considering and 1 of which had acquired insurance).

All interviews, in 2016 and 2018, were conducted in a semi-structured form for the duration of an hour at the office of the informant or using teleconferencing. The Norwegian interviews were carried out by two researchers, one of whom asked the questions and one of whom took notes. These interviews were digitally recorded, transcribed and coded, before a draft summary report was presented to the informants so they could give additional comments. The Swedish interviews were carried out by a single researcher. The raw transcription notes of the Swedish interviews were distributed to informants shortly after the interview, to give the opportunity to correct and complement the findings, and also for the informants to confirm that their level of anonymity was sufficient.

All interviews were conducted using the same semi-structured template given in Appendix A. The Swedish translation was created based on the Norwegian original in early 2017 in preparation for the second, Swedish, data-collection phase. All transcriptions were independently analysed by two researchers (the authors) in order to identify opinions about expectations among the informants.

B. Incident data analysis

A set of anonymized incident claims reports were obtained from the global insurance intermediary Willis Towers Watson, along with their aggregated cyber claims data [34] and data breach event statistics for 2018 [35]. The claims reports covered the following business domains and included short narratives about the event, consequences, coverage categories and claims costs:

- **Finance**, with three breach incidents related to loss of sensitive data, malware and insider data theft.
- **Healthcare**, with two incidents related to insider data theft and theft of servers containing sensitive data.
- **Education**, with three incidents related to ransomware/extortion, loss of personal data and malware information theft.
- **Manufacturing**, with two incidents related to unintentional business interruption and information theft.
- **Retail**, with two incidents related to intentional business interruption and information theft.

The claims data showed what kind of claim coverages were implicated and the data breach event statistics were based on 330 breaches and their incident costs related to a broader set of industry/business domains than the claims reports. As a supplement to this, historical data about proportion of breaches per domain had previously been obtained from Advisen, which is a commercial data provider for the insurance market.

IV. RESULTS

We have summarized the interview results in Table I. The first column specifies the identifier of the informant. The second column defines what kind of domain they belong to, using the industries defined in [35]. In the third column we have tried to briefly summarize what kind of expectations the informants have on current products and what they would like to see more of.
TABLE I
SUMMARY OF EXPECTATIONS FROM THE INFORMANTS

<table>
<thead>
<tr>
<th>ID</th>
<th>Domain</th>
<th>Expectations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comp1</td>
<td>IT</td>
<td>Emphasizes business interruption, and in particular related to catastrophic events.</td>
</tr>
<tr>
<td>Comp2</td>
<td>Finance</td>
<td>Expect that the insurance they have bought will cover incident response and costs related to reconstruction of lost data. Motivated to buy insurance if this gives them access to highly skilled expertise.</td>
</tr>
<tr>
<td>Comp3</td>
<td>Process industry</td>
<td>Stresses the width of insurance triggers. Coverage for ransomware attacks and similar would be nice to have, but not the only thing that would make them buy an insurance. They expect that e.g. CEO-phishing attacks would be covered by their extended crime insurance.</td>
</tr>
<tr>
<td>Comp4</td>
<td>Food</td>
<td>Expect the insurance will cover incidents with low probability but high consequence. Stresses the costs of business interruption and motivates not procuring cyber insurance with limits being too small, so that it is more rational to self-insure. Would like transfer short time business interruption risks to an insurance company.</td>
</tr>
<tr>
<td>Comp5</td>
<td>Transport</td>
<td>Stresses business interruption as the most important coverage factor.</td>
</tr>
<tr>
<td>Comp6</td>
<td>Media</td>
<td>Business interruption should be the most important coverage, not so concerned about data breach. Notes that current limits are too small. Insurance should cover the truly catastrophic events, and then some 20 MEUR is not so much.</td>
</tr>
<tr>
<td>Comp7</td>
<td>Finance</td>
<td>Stresses the non-monetary impact to reputation, questioning if insurance can help. Seemingly more interested in SLAs with guarantees than insurance to manage business interruption.</td>
</tr>
<tr>
<td>Comp8</td>
<td>IT</td>
<td>Has not considered cyber insurance, currently has self-insurance for many types of incidents. Data breach might become relevant after 2018 (GDPR implementation).</td>
</tr>
<tr>
<td>Comp9</td>
<td>Energy</td>
<td>Worries mostly about business interruption, but not relevant to insure this. Reasons that in principle, (any) insurance is only relevant if it covers what you cannot cover yourself. For instance, handling reputation loss in case of an incident is something they should take care of themselves.</td>
</tr>
<tr>
<td>Comp10</td>
<td>Retail</td>
<td>Emphasizes business interruption, for instance a virus attack that could take down the whole business.</td>
</tr>
<tr>
<td>Comp11</td>
<td>Retail</td>
<td>Places equal importance on the three components (i) data breach, (ii) business interruption, and (iii) incident response.</td>
</tr>
<tr>
<td>Comp12</td>
<td>Manufacturing</td>
<td>Deems business interruption more important than data breach.</td>
</tr>
<tr>
<td>Comp13</td>
<td>Manufacturing</td>
<td>Notes that the up until now, it has been rational for them to self-insure, as the limits have been too small and the consequences not so severe. Do not possess sensitive data and not too worried about data breach coverage today, but foresee that it may become more relevant in the future.</td>
</tr>
</tbody>
</table>

Fig. 1 shows actual coverages implicated based on the claims data from [34]. The coverage categories were defined by the insurance intermediary. The most interesting finding here is that incident response constitutes the bulk of the coverages (61%), while business interruption has only a mere 4%.

Table II shows informants grouped according to domains, and relates these to incidents described in claims report and breach claims data. Here, we have grouped Comp12 and Comp13 (manufacturing), Comp3 (Process industry) and Comp9 (Energy) within the same group (manufacturing). Similarly, Comp11 (Retail), Comp4 (Food) and Comp10 (Retail) are grouped as retail. We only have relevant claims reports (from [34]) for finance, manufacturing and retail.

The breach claims data, by contrast, is richer and consists of several statistics: The first is the relative frequency of breaches per domain. This data stem from Advisen and is described in [29]. The proportion of claims, average cost and total cost values stems from [35] and encompasses 281 claims worldwide from 2018. Note that retailers have the greatest total breach costs associated with them ($3 473 550), while hospitality and leisure has the highest average cost per claim ($173 908). Healthcare is the domain that has greatest number of claims (27% of the data set). These two latter along with some other minor categories are not displayed in Table II, as we did not interview any informants from those domains.

Fig. 1. Coverages implicated

V. DISCUSSION

A. Expectations from domains

There is no clear pattern in what companies from different domains expect from their cyber insurance policies. In the
<table>
<thead>
<tr>
<th>Domain</th>
<th>Informants</th>
<th>Incident examples from claims reports</th>
<th>Breach claims data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>Comp2, Comp7</td>
<td>• Lost laptop containing data about individuals. Lawsuit defence costs exceeds $700 000.</td>
<td>21% of the breaches. 19.6% of the claims in 2018, average cost $83 242, total cost $2 422 106.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malware infection, expensive forensic investigations and customer credit monitoring.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Insider stole customer information, insurance carrier helped with coordinate legal, forensics, notification, call center &amp; credit monitoring.</td>
<td></td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Comp3, Comp9, Comp12, Comp13</td>
<td>• Failed software upgrade lead to business interruption, $2M insurance pay out.</td>
<td>5.6% of the breaches. 1.8% of the claims in 2018, average cost $152 900, total cost $764 500.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Malicious software scraped customer credit cards, insurance carrier covered legal counselling and forensic assistance. Additional expenses related to customer services.</td>
<td></td>
</tr>
<tr>
<td>Retail</td>
<td>Comp4, Comp10, Comp11</td>
<td>• Stolen login credentials, 50 000 customer credit card numbers stolen. $1M income loss.</td>
<td>9.9% of the breaches. 8.5% of the claims in 2018, average cost $144 731, total cost $3 473 550.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DDoS attack lead to service disruption and a $300 000 income loss.</td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td>Comp5</td>
<td>-</td>
<td>4.6% of the breaches. 1.1% of the claims in 2018, average cost $10 331, total cost $30 994.</td>
</tr>
<tr>
<td>IT</td>
<td>Comp1, Comp8</td>
<td>-</td>
<td>Part of the wider Advisen category services, which has 42.6% of the breaches. 4.6% of the claims in 2018, average cost $6 968, total cost $90 586.</td>
</tr>
<tr>
<td>Media</td>
<td>Comp6</td>
<td>-</td>
<td>Part of the wider Advisen category services, which has 42.6% of the breaches. 1.4% of the claims in 2018, average cost $14 879, total cost $59 516.</td>
</tr>
</tbody>
</table>

In the **retail** domain, there is typically an emphasis on business interruption (Comp4, Comp10) or it is at least deemed as important as other aspects (Comp11). This is somewhat contrary to our expectations of a greater emphasis on data breach, based on retail handling large amounts of personal data and credit card data from customers. One of our incident examples in Table II showed that this had been the case, and that the income loss was much higher than the average cost covered by insurance. As already mentioned, the claims statistics show that retailers have the largest amount of total breach costs.

In the **manufacturing** domain, business interruption is deemed more important than data breach (Comp9 and Comp12). Comp12 motivates this by noting that being in the business-to-business rather than business-to-consumer segment gives less exposure to sensitive personal data and the potential consequences of a breach. This is more in line with expectations. One of the incident examples showed that the business interruption pay-out was much higher (13x) than the average cost covered by insurance, and also larger than the total cost. We assume that this incident must be prior to 2018, but it is a good illustration how one incident can dominate a market when the number of claims is small with variable costs. Another noteworthy finding is that this domain has a much lower proportion of claims compared to the proportion of breaches.

Considering the **finance** domain, Comp2 were concerned about incident response and recovery, while Comp7 stressed that good SLAs were more important than insurance. Expectations on response and recovery are aligned with the two latter incident examples for this domain in Table II. On the other hand, SLAs would not have made a difference for any of the three incident examples. It is also interesting to note that finance is where the largest proportion of breaches and claims occur among the companies we interviewed. This is in accordance with Forbes, claiming that US financial services firms are attacked more than 300 times more frequently than businesses in other industries [36].

For the remaining domains, **transport**, **IT** and **media**, coverage of business interruption is the common expectation. These domains constitute a significant portion of the breaches; however, the claims data show that there are only a few claims, and these are all very low in terms of costs. This is an indication of a discrepancy between coverage expectations, claims and incidents.
Independent of domain, several informants (Comp4, Comp9, Comp13) reason about self-insurance, arguing that this is a more rational option when limits are too small or important consequences such as reputational damage are not covered anyway. Comp13 (manufacturing), however, goes on to say that this may change as their line of business is expected to undergo digital disruption in the coming years, where their exposure both to personal data (covered by cyber insurance) and to cyber risks that might entail physical damage or bodily injuries (not covered by cyber insurance) will increase. Comp13 also stated that even though cyber is a great risk, it is currently not their greatest. If we compare this with the Allianz Risk Barometer from 2019 [37], business interruption and cyber incidents are on the top for Europe considering all domains. However, for manufacturing, natural catastrophes trump cyber incidents, so this is in accordance with the view of Comp13.

B. Expectations and claims paid out

Comparing customer expectations with statistics on the claims paid out, some discrepancies can be identified.

First, it is evident that incident response expenses are by far the most common of the coverages implicated in the claims data [34], as seen in Fig. 1. The coverage for incident response expenses is implicated some 4 times more often than security/privacy liability (roughly the same as data breach) and some 15 times more often than business interruption. This is clearly out of proportion compared to customer expectations. As we saw in the previous section, there are informants who value incident response highly (Comp2) or at least places it on a par with data breach and business interruption (Comp11), but they are a minority.

However, it should also be noted that the incident response coverage is a bit different from the other categories in the sense that the latter count different kinds of incidents (e.g., data breach is one kind of incident and business interruption is another), but incident response counts them all. Hypothetically, for any number of incidents that each implicate (i) a particular category and (ii) the general incident response category, incident response would account for half of the coverages implicated. Furthermore, if some incidents do not reach the thresholds for activation in the particular categories, e.g., the waiting periods always included in business interruption coverage, incident response would account for strictly more than half of the coverages implicated. From this perspective, the apparent over-representation of incident response fully disappears.

Conversely, business interruption coverage was highly valued by informants from retail (Comp4, Comp10) and manufacturing (Comp9 and Comp12) alike, yet accounts for only 4% of the coverages implicated. Here, it is clear that customer expectations are not in line with claims actually paid out. However, business interruption policies have waiting periods before they are activated. These are rarely shorter than some 6 or 8 hours and often significantly longer, e.g., 24, 36, 48, or 72 hours [15]. From this perspective, it is not surprising that business interruption claims are limited. It is also worth observing that many informants emphasize that insurance should cover incidents with low probability but high consequence (Comp1, Comp4, Comp6). Thus, their expectations may not be that business interruption should represent a large proportion of claims in any given year, but rather that if there are interruptions with very long durations, these will be covered. This leads us to the question of how expectations align with business interruption scenarios.

C. Expectations and scenarios

Since it is well-known that statistics on cyber insurance are rare [1], [15], [6], it is reasonable to expect that expectations – both of customers and insurers – are also formed by hypothetical scenarios. Some such scenarios are private, e.g., internal risk analyses carried out before procuring an insurance, or as part of the underwriting. However, other scenarios are made public. It is instructive to compare some recent such published scenarios with the customer expectations expressed in the interviews.

In early 2018, Lloyd’s released a report mapping the impact on US companies of a major cloud service provider outage, i.e. an outage in the order of several days [38]. While the big enterprise public cloud providers – Amazon Web Services, Microsoft Azure, Google Cloud and IBM – are all remarkably reliable, outages do happen and the impact of such downtime is substantial. In the scenarios investigated in the report, where a major cloud service provider is down for 3-6 days, the US manufacturing industry would experience ground up losses of some $4.2-$8.6 billion, and the US wholesale and retail trade industry would experience ground up losses of some $1.4-$3.6 billion. It is noteworthy that these are the industries carrying the greatest losses.

In early 2019, Lloyd’s together with the Cambridge Centre for Risk Studies, and Nanyang Technological University, released a report exploring the consequences of a global infection by contagious malware [39] – not unlike the real cases of WannaCry and NotPetya in 2017. In a less severe version of the scenario, retail suffers the most ($15 billion), followed by healthcare ($10 billion) and manufacturing ($9 billion). In a more severe version, retail and healthcare are on a par ($25 billion each), followed by manufacturing ($24 billion). This report also explores the insurance coverages implicated, showing that business interruption is the main driver of the insured losses (with some 71% of total losses in the less severe scenario and 59% in the more severe one). The second and third largest claims arise in incident response costs and liability, respectively.

In brief, it can be concluded that scenarios such as these are well aligned with the concerns of the many informants, who emphasize business interruption coverage (Comp1, Comp4, Comp5, Comp6, Comp9, Comp10, Comp11 and Comp12).

D. Who is to blame?

An interesting remark by Comp11, which at the time of the interview had just signed their cyber insurance policy, is...
that its existence will not be announced to the employees. The reason given is moral hazard: the risk of more reckless behaviour as a consequence of insurance protection (this also applies to other insurance policies at Comp11). Comp12, which at the time of the interview expected to soon request quotes through an insurance intermediary, reasoned in a similar way.

Such management of human error is prudent, since 66% of the incidents in the claims statistics from Willis Towers Watson were blamed on “employee negligence or malfeasance”. For example, phishing and ransomware is introduced by an employee opening a malicious e-mail attachment is typically considered “human error” by insurers.

E. Validity and reliability

The 13 companies interviewed were selected with a kind of purposive sampling, actively looking for companies considering cyber insurance. Thus, the sample cannot be claimed to be representative of all Norwegian or Swedish companies. However, such broad representativity was never the goal of the research. It is known from previous work that the number of companies with cyber insurance is still low in Norway and Sweden [15], so a random sample of all companies would mostly generate informants oblivious to cyber insurance. Instead, the aim was to investigate attitudes of companies who had considered cyber insurance. From this perspective, the sample is more representative. Among the 13 companies, there is broad representation from different industries, such as finance, media, retail, manufacturing, critical infrastructure and IT.

Most of the informant companies are relatively large and many of them are international companies active on many markets. This means that they represent the large company market segment of cyber insurance. While most insurance companies offering cyber insurance have relatively large customers [15], there is also an SME cyber insurance market segment. Both in Denmark and in Sweden, thousands of small cyber insurance packages have been sold, typically with comparably small indemnity limits and mostly focusing on incident response [15, Table 1, Insurance company 1]. Thus, it is important to bear in mind that the results do not represent this SME segment, but the large company segment of cyber insurance.

The claims data set represents events from all over the world (though mostly North America and Europe). Thus, while the claims data set has a much broader scope than the interviews, it allows to assess the expectations of (would-be) cyber insurance policy holders with the kinds of events for which insurance claims are actually paid out. While it might be argued that it would be more accurate to compare the expectations of Scandinavian policy holders with Scandinavian claims, this is not feasible, as it is known that the number of such claims is still very low [15]. Instead, to have a reasonable frame of comparison, it is necessary to look at claims from a larger area, and the data set used can thus be deemed suitable, though results need to be interpreted with some caution.

VI. CONCLUSIONS AND FUTURE WORK

Revisiting the research questions posed in Section I, first, we can discern no obvious pattern of discrepancies between different domains. What differences there are between of informants do not correspond to their domains, and the coverage that seems to be the most valued among all informants is business interruption.

This naturally leads us to our second research question, because this is not aligned with the incident data. Here, incident response constitutes 61% of coverages implicated, whereas business interruption represents a mere 4%. However, this dominance of incident response is not surprising when accounting for the fact that this is a generic category that applies to all incidents. Similarly, the small fraction of business interruption can to some extent be explained by the fact that this coverage has waiting periods before it is activated. Many informants also reason in a mature way about this: the important thing is not coverage of many small incidents that happen every year, but rather coverage of rare but substantial incidents. From this perspective, the waiting periods are not misaligned with customer expectations.

This leads to the third question, about scenarios. Indeed, some recently published scenarios on possible major business interruptions, due to cloud service outages or rapidly spreading ransomware, are more aligned with informants’ emphasis on business interruption coverage. At the very least, these scenarios show that major business interruption events are not at all implausible, and are in this respect aligned with customer expectations on business interruption coverage as expressed by the informants.

A few avenues for further research suggest themselves. Cyber insurance is still in its development phase and the number of claims paid out in the Nordic region is still very low [15]. Thus, it would be interesting to investigate how expectations on coverage change over time.

Second, the interview guide given in Appendix A can be used to conduct comparative studies in other regions. Are customer expectations uniform all over the world, or do they differ? Based on previous research [15], we hypothesize that customers in Europe still focus more on 1st party costs such as business interruption, whereas customers in the US still focus more on 3rd party liabilities connected to data breaches. However, the advent of the General Data Protection Regulation (GDPR) in Europe might change this, so longitudinal studies, tracking the expectations over time, are interesting.

A third research direction is to look at how emerging threats may change the expectations of what policies should cover. For instance, there is a generally high awareness about ransomware, which has very noticeable consequences and is present in the majority of the policies [6], [33]. However, a more recent trend is that the ransomware threat is being dethroned by cryptojacking or cryptomining malware, which also provides direct revenue to the criminals but with a lower risk of penalty. According to the latest Internet Organised Crime Threat Assessment from Europol [40], this is a type of
threat that only has a small impact on the victim’s system, and it is hard to quantify the damages and difficult to investigate due to the lack of reporting. It is comparable to theft of electricity, which may go unnoticed over a long period of time though the accumulated costs can become significant. How the insurance market will position themselves towards large-scale, low-impact threats is still an open question.

ACKNOWLEDGMENT

The authors would like to thank all the interviewed informants. We would also like to express our gratitude towards Willis Towers Watson and Advisen for sharing their data with us.

APPENDIX

A: INTERVIEW GUIDE

In the following, the interview guide used is outlined, translated from Norwegian/Swedish and somewhat abbreviated.

A. About the research

1) Short introduction of the scope of the research project and the interview.
2) Do you give your informed consent to the use of the material gathered for scientific publication?

B. Background on the informant and the enterprise

1) What is your role, how long have you had it, and what is your background?
2) Is there a CISO in the enterprise?
3) Has the enterprise procured cyber insurance?

C. Evaluation of cyber insurance

For enterprises that have procured cyber insurance.

1) What made you consider cyber insurance?
2) Can you describe the process (roles, intermediary, understanding market offerings)?
3) Can you describe the process of obtaining an insurance quote (relevance of insurer questions, proposal forms, etc.)?
4) What should insurance quotes and insurance policies look like to be attractive (e.g., price, incident response service, claims payment, simplicity, flexibility, coverage of many small incidents, coverage of catastrophic incidents)?
5) Can you describe how the decision was reached on which insurance policy to choose (easy or difficult decision, comfortable with it, the right competence to decide, based on risk-analysis or quantification of security, insurance vs. other measures)?
6) Does the existence of a cyber insurance affect how you work with security?
7) Have you experienced incidents covered by the insurance?

For enterprises that have not procured, but considered cyber insurance.

1) Why have you not considered cyber insurance?
2) Can you describe the process (roles, intermediary, understanding market offerings)?
3) Was there a process of obtaining an insurance quote (relevance of insurer questions, proposal forms, etc.)?
4) What should insurance quotes and insurance policies look like to be attractive (e.g., price, incident response service, claims payment, simplicity, flexibility, coverage of many small incidents, coverage of catastrophic incidents)?
5) Can you describe how the decision was reached on not taking out insurance (easy or difficult decision, comfortable with it, the right competence to decide, based on risk-analysis or quantification of security, insurance vs. other measures)?
6) If you had procured a cyber insurance, do you think it would have affected how you work with security?

For enterprises that have not procured and not considered cyber insurance.

1) Why have you not considered cyber insurance?
2) To what extent are you familiar with cyber insurance products and their meaning?
3) Do you have other kinds of insurance that also cover cyber crime related incidents?
4) What would be important to make cyber insurance relevant for you?
5) How do you make decisions on the kinds of cyber security measures you need to implement (risk-analysis, evaluation of measures against each other, quantification of security, roles involved, easy or difficult decisions, comfortable with them)?

D. Evaluation of enterprise cyber risk

1) How exposed are your enterprise to cyber risk (why, what are the potential consequences)?
2) Have you experienced cyber incidents (and did they affect your future risk management)?

E. Conclusion

1) Thanks and a brief description of the road from interview to scientific publication.
2) Is there anything you would like to add about cyber insurance?
3) Are there any questions related to the interview that future research should address?
4) Do you want information about future research project activities?

REFERENCES
