COMPUTERS & SECURITY 68 (2017) 130–144

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

The cyber insurance market in Sweden

Ulrik Franke *

RISE SICS – Swedish Institute of Computer Science, P.O. Box, 1263 SE-164 29, Kista, Sweden

ARTICLE INFO

Article history:
Received 7 March 2017
Received in revised form 7 April 2017
Accepted 23 April 2017
Available online 26 April 2017

Keywords:
Cyber insurance
Underwriting
Risk management
Business continuity
Business interruption
Data breach
Asymmetry of information

ABSTRACT

This article is a characterization of the cyber insurance market in Sweden. As empirical investigations of cyber insurance are rarely reported in the literature, the results are novel. The investigation is based on semi-structured interviews with 10 insurance companies active on the Swedish market, and additional interviews with 2 re-insurance companies and 3 insurance intermediaries. These informants represent essentially all companies selling cyber insurance on the Swedish market. Findings include descriptions of the coverages offered, including discrepancies between insurers, and the underwriting process used. Typical annual premiums are found to be in the span of some 5–10 kSEK per MSEK indemnity limit, i.e. 0.5–1% of the indemnity limit. For business interruption coverage, waiting periods are found to be relatively long compared to many outages. Furthermore, insurance companies impose information and IT security requirements on their customers, and do not insure customers that are too immature or have too poor security. Thus cyber insurance, in practice, is not merely an instrument of risk transfer, but also contains aspects of avoidance and mitigation. Based on the findings, market segmentation, pricing, business continuity, and asymmetry of information are discussed, and some future work is suggested.

1. Introduction

Modern society is becoming increasingly dependent on IT services. Functioning IT services now underpin aspects of all human endeavors, from work to leisure, from private to public sector, and from Andorra to Zanzibar. When these services stop functioning, whether by non-malicious mistakes or by malicious attacks, consequences are immediately felt and effects ripple through interconnected IT service orchestrations, integrated supply chains, and interdependent businesses processes across the globe. In this sense, IT services are becoming a critical infrastructure, much like roads, electricity, tap water, and financial services.

As a result, there is much research dedicated to preventing IT outages and ensuring business continuity. Whereas in the early years of computing hardware outages were the main culprit behind downtime, since the 1980s, IT administration and software errors have become predominant causes of outages (Gray, 1990) along with human errors (Pertet and Narasimhan, 2005). With the advent of service oriented and cloud computing, much effort has gone into the investigation of how to optimize quality of service in these settings (Casalicchio et al., 2013), including how to learn from past incidents in order to offer better future services (Kieninger et al., 2013). From a traditional reliability engineering perspective, risk management of IT outages have been endowed with studies of statistical distributions of IT outages and the importance

* *E-mail address:* ulrik.franke@ri.se.
http://dx.doi.org/10.1016/j.cose.2017.04.010

of knowing them (Franke et al., 2014; Snow and Weckman, 2007; Snow et al., 2010). To prevent or mitigate malicious attacks, research is constantly ongoing in areas like intrusion detection systems (Liao et al., 2013), threat detection (Virvilis and Gritzalis, 2013), and cyber security in industrial control systems (Knapp and Langill, 2014).

However, with the realization that all threats, security breaches and IT outages cannot be prevented by technical means alone, financial risk management through so called *cyber insurance* has become an increasingly discussed complement. Its relevance has been further increased by the trends of outsourcing and cloud computing: whenever IT is not operated in-house, it is difficult to manage risk through technical or organizational measures, further underscoring the role of making financial risk management. This has traditionally been solved by requiring external IT service providers to maintain an errors and omissions insurance. However, many large service providers have strict service level agreements (SLA) that limit their liability. Therefore, cyber insurance is often used to cover the gap between the insurance coverage and contract limitations of the service provider and the full loss of the client.

This growing interest in cyber insurance is reflected in many ways. IT strategy consultancies like Gartner provide guidelines for how to use it effectively (Wheeler et al., 2015). Insurance industry forecasts predict expected growth in premiums from around 2 billion USD in 2015 to some 20 billion USD or more by 2025 (Wells and Jones, 2016). International organizations like the EU (ENISA, 2016) and the OECD (OECD, 2016) are conducting studies aiming to better understand the potential of cyber insurance. National governments like the British are supporting the growth of the cyber insurance market to improve cyber security risk management (Cabinet Office, 2014).

It is against this background that the research reported in this article was conducted. Its focus is the cyber insurance market in Sweden. This may seem like a provincial concern, but there are reasons why this is interesting beyond Swedish borders as well. First, most of insurance companies active on the Swedish market are global companies. Even though their products are adapted to local markets, they are also bound to have much in common across the globe. Second, Sweden regularly scores top results when countries are evaluated in terms of digital and ICT maturity. For example, Sweden was ranked 3rd in the World Economic Forum's Networked Readiness Index 2016 (World Economic Forum, 2016), 3rd in the EU Digital Economy & Society Index 2017 (European Commission, 2017), and 3rd in the International Telecommunication Union's ICT Development Index 2013 (ITU, 2014). It is reasonable to assume that the cyber insurance experience of mature countries such as Sweden might offer valuable and relevant insights for other countries as well. Third, the findings include results concerning pricing and premiums that are unique in the literature and thus merit attention in this respect.

The general research question addressed in this article is: What does the cyber insurance market in Sweden look like? This broad question is broken down into a few more specific research questions:

- What coverage do typical cyber insurance products offer?
- How many cyber customers and claims do insurance companies have?
- How is the market segmented?
- How does the underwriting process look?
- How are premiums determined?
- Are business interruptions treated with mathematical availability modeling tools?
- How does cyber insurance fit into a bigger risk management tool box?

These research questions were investigated using semi-structured interviews with the insurance companies offering cyber insurance products on the Swedish market. At this stage, no demand side investigation, i.e. data collection from buyers of cyber insurance, was conducted. Nevertheless, the findings offer an interesting picture of the cyber insurance market in Sweden.

The remainder of this article is structured as follows. Section 2 reviews the literature for related work. The methodology used is described in Section 3, followed by a report of findings in Section 4. Results and implications are then discussed in Section 5, which together with the findings is the main contribution. Section 6 concludes the article with some final remarks and thoughts on future work.

2. Related work

The concept of cyber insurance has received much academic attention over the past decade and a half. From a conceptual point of view, insurance is an interesting approach to problems of IT security, as it allows risk management of low-probability–high-impact events by sharing the risks over many actors, each of whom individually would be severely affected by an event, but who collectively can afford to save enough to cope with it. It is also possible for insurance companies to impose mandatory requirements on their customers, thus improving security for everyone. However, there is a large difficulty: *cyber risks are not independent*, the way they are in many other lines of insurance (Böhme and Kataria, 2006). First, a non-malicious outage or a malicious attack can suddenly affect "everyone" using a certain kind of technology, whether this is a shared data center or a software with a newly discovered vulnerability. Second, both the business continuity and the information security of any one actor are highly dependent on the efforts of *other actors* with whom the first actor somehow interacts. Anderson and Moore, in a review article published in *Science* over a decade ago, concluded that these difficulties, unfortunately, have hampered both the development and use of cyber insurance products (Anderson and Moore, 2006).

These difficulties are mirrored in the negative results that pervade the literature: cyber insurance markets cannot exist when the cyber risks facing individual clients are too correlated (Böhme and Kataria, 2006) or when insurers cannot observe their customers' security levels (Shetty et al., 2010) and furthermore, policies tend to be overpriced because insurers are unable to anticipate customers' secondary losses such as reputational damage (Bandyopadhyay et al., 2009). Other models give more encouraging results: cyber insurance can create powerful incentives to invest in security (Bolot and Lelarge, 2009), partial cyber insurance coverage can motivate non-cooperative insurance customers to invest more efficiently in self-defense

(Pal and Golubchik, 2010), and cyber insurance premiums can be estimated in robust ways (Herath and Herath, 2011). Böhme and Schwartz offer a good but now slightly dated literature review, and also introduce a framework to make sense of all the different models and assumptions found in the literature (Böhme and Schwartz, 2010).

Concluding their literature review, Böhme and Schwartz note an oddity of cyber insurance research: while economic research on insurance is typically concerned with the existing products and markets, the study of cyber insurance has been more concerned with developing theoretical models than with empirical research (Böhme and Schwartz, 2010). Therefore, it is encouraging that some empirical work has been published in recent years. For example, Biener et al. use data on cyber-related losses from an operational risk database to empirically analyze whether these losses are insurable, according to standard criteria (Biener et al., 2015). Though they identify difficulties known from the literature – (i) correlation between losses, (ii) lack of data, and (iii) severe information asymmetries – the authors nevertheless conclude on a positive note, observing that growing and developing markets will offer important opportunities for improvement, including better data collection. The newer literature also includes various empirical studies of data breaches (Edwards et al., 2015; Sinanaj and Muntermann, 2013) relevant not least in pricing cyber insurance.

A more recent comprehensive literature review of cyber insurance was compiled in late 2016 by Eling and Schnell, available both as a condensed academic journal article (Eling and Schnell, 2016b) and as an extended working paper including supplemental material, available from the Geneva Association (Eling and Schnell, 2016a). It is organized along seven core topics, the last of which is what the cyber insurance market looks like and what the main insurability challenges are. To summarize their main findings about the cyber insurance market, it is still small but expected to grow significantly in the next years, and the US is far ahead of Europe.

Despite some progress in recent years, Eling and Schnell also conclude that more empirical research is needed, both on the demand and the supply sides. This is a key motivation for the research reported in the present article. By making an empirical characterization of the cyber insurance market in Sweden today, a contribution is made to the state of knowledge about actual market practices, complementing the theoretical understanding abundantly found in the literature.

Two existing pieces in the literature are particularly closely related to the present article: First, a short monograph about the cyber insurance market in Germany, written by a freelance journalist commissioned by an insurance company (Choudhry, 2014). It is similar in its systematic approach to analyze a particular market, but obviously different in which market that is, as well as in being more of a popular science work. Second, a recent study on cyber insurance by European Union Agency for Network and Information Security (ENISA, 2016). While this study is more policy-oriented, making recommendations to policy makers, insurance companies, and customers, it also has some empirical contents based on questions posed to a cyber insurance stakeholders group including representatives from cyber insurance companies. There is some overlap in scope, e.g. the underwriting process and the coverage offered, but the present article differs both in its systematic approach to analyze the market in a single country, and more importantly, in reporting novel results on pricing and premiums.

3. Method

In order to answer the research questions about the Swedish cyber insurance market, it was decided to approach the supply side, i.e. the insurance companies, first. To do so, the industry association Insurance Sweden was first contacted. Insurance Sweden works to promote good business conditions for the insurance industry, and also maintains publicly available statistics about the Swedish insurance industry. However, as it turned out, Insurance Sweden does not collect any statistics on cyber insurance. Nevertheless, Insurance Sweden did provide contact details to a number of relevant actors on the Swedish insurance market who were known to be working in the cyber area.

3.1. *Interview questions*

In preparation for the interviews with the insurance companies, interview questions were developed. It was decided to conduct semi-structured interviews with a mix of open questions that would allow the informant to comment and expand on the subject more freely, and more specific questions that would require more precise answers. The questions, somewhat compressed for conciseness, were as follows:

- Do you offer insurance against IT incidents? This could be cyber insurance, or it could be other kinds of insurance, e.g. business interruption insurance that covers outages in IT services. If so, expand on what is covered, e.g. in terms of data theft, data manipulation and business interruption.
- How big is the market and your market share? For example, how many customers do you have for the cyber insurance product? What is the turnover of a typical customer?
- How many cyber claims do you have?
- Can you reveal anything about your pricing? For example, is the pricing based on historical claims data, other kinds of data, or some kind of best guess? Can you say anything about premiums and indemnity limits?
- Is pricing affected by the particular situation and maturity of customers? Do you use particular methods to assess customers, e.g. ITIL, IT audits etc.? Do you work proactively with customers to increase security?
- If you cover business interruption, do you do any modeling in terms of Mean Time to Failure (MTTF) and Mean Time to Restore (MTTR) for customer IT services?

This set of questions was initially developed based on the research questions. In order to get second opinions on the applicability and relevance of the questions, they were also subjected to review by two experts. The first expert was a colleague of the author with a PhD in mathematics and several years of professional experience as an actuary in the insurance business. The second expert was a representative from Insurance Sweden. Based on their comments and suggestions, the questions were refined and revised. One particular

concern was how much "hard data" the insurance companies would be willing to reveal about the market and their pricing. Therefore, an important insight from this review phase was the need to clearly communicate to the informants that their anonymity would be preserved, that they would have the opportunity to review the results before publications, and that the research effort is impartial in relation to the competing companies on the market.

3.2. *Data collection*

Data were collected through semi-structured interviews with market actors in the period of September to November 2016. The primary informants were representatives from 10 insurance companies active on the Swedish market. Out of these, 5 were on the original contact list provided by Insurance Sweden, and the other 5 were recruited through additional contacts made in the interview phase. These 10 are anonymously referred to as Insurance company 1–10 (or I1–I10 for short) in the following. Whereas Insurance companies 1–9 offer dedicated cyber insurance products, Insurance company 10 does not. Still, the interview with I10 plays an important role in providing a contrasting perspective, and I10 was deliberately included precisely for this reason. I2, I3, I4, I5, I6, I7, and I9 are global companies. I1, I8, and I10 are regional actors on the Nordic and Swedish markets.

Additionally, interviews were conducted with 2 re-insurance companies (RE1-2 for short) and 3 insurance intermediaries (II1-3 for short). These interviews with secondary informants were conducted following recommendations from other informants, or from Insurance Sweden. The rationale for including these interviews in the investigation was to collect additional perspectives from market actors that do not sell cyber insurance directly, but nevertheless are knowledgeable in the area, and more impartial regarding the offers of particular insurance companies. While these interviews also focused on the research questions and were loosely based on the questions listed in Section 3.1, they should be regarded as unstructured, rather than semi-structured, interviews carried out to collect background data and contrasting perspectives.

All interviews were carried out face to face in Scandinavia, most often at an office of the insurance company. Most interviews were conducted in Swedish or in Swedish and mutually understandable Scandinavian languages, but two interviews were conducted in English. At 8 of the primary informant companies, a single representative was interviewed, while 2 primary informant companies elected to have two representatives present at the interview. All interviews were conducted by the author. In two cases (I5 and I6), the author was accompanied by a colleague. A typical interview lasted for about one hour. In addition to the answers given in the interview, I1, I2, I3, I4, I5, and I6 all provided additional materials ranging from marketing flyers to example policy schedules.

3.3. *Verification of interview results*

Following each of the 10 interviews with primary informants, interview notes of 1–2 regular pages of written text were sent to the company representative(s) interviewed. Additionally, preliminary versions of Table 1 below were distributed for review. The representatives were requested to review the notes and the table for accuracy and also to identify any information that they would like to have removed or made less precise in order to preserve informant anonymity. It was explained that the notes distributed were "raw" notes and as such verbose, whereas the final text, as reflected mostly in Sections 4–5, would be more condensed. All 10 primary informants gave relevant feedback on the interview notes and the table, thus ensuring that the documentation of the interviews reflects the beliefs of the informants.

Once all interviews had been conducted, and a preliminary analysis of the data was ready, all primary and secondary informants were invited to a seminar held in late November 2016, where the findings were presented and the informants were given the opportunity to comment and reflect upon them. While not all informants participated, the seminar was attended by some ten informant representatives, and the discussions at the seminar served as additional verification of the results, as well as further informing the analysis detailed in Section 5.

As a final measure to verify the results, a draft of this article was sent to all primary and secondary informants in February 2017, giving them the opportunity both to correct factual errors and to offer reflections on the analysis. All informants responded, most often just a confirmation that results were accurate, but also some corrections to factual details and relevant reflections.

4. Results

In the following subsections, the main results are presented. A summary of findings is given in Table 1. Implications are further analyzed in Section 5.

4.1. *Coverage*

Originally, the term "cyber insurance" – sometimes "cyber liability insurance" – comes from the US, and the corresponding product focuses on the 3rd party liabilities connected with *data and privacy breaches*, including notification costs. This emphasis is due to breach notification laws, enacted in most US states, that mandate companies subject to data breaches to notify customers and other parties about the breach, and to take measures to limit the damage caused to such 3rd parties. Historically, this differs from Europe, where the 1st party costs of *business interruption* have instead been in focus. This discrepancy, however, has been decreasing in the past few years, and the European General Data Protection Regulation (GDPR) is widely expected to make liabilities connected with data and privacy breaches a top concern in Europe.

As a result of this convergence, all the dedicated cyber insurance products investigated (i.e. the products of Insurance companies 1–9) offer coverage of both 1st party costs and 3rd party liabilities. A typical cyber insurance product on the Swedish market covers 1st party costs such as lost revenue from business interruption, cost of cyber extortion (though actually paying a ransom is only a very last resort), costs for forensic

Table 1 – Summary of findings from interviews with I1-9. SEK is the Swedish currency, krona, prefixed with M, and G to denote millions and billions, respectively. The ~ sign denotes approximate figures. N/A is used for I8, who at the time of the interview was just launching its cyber insurance product, and thus did not give any customer figures.

Insurance company	Data breach	Business interruption from attack	Business interruption not from attack	One-stop-shop incident telephone support	# customers in Sweden	# annual cyber claims in Sweden	Typical customer turnover	Typical indemnity limit
1	Yes	Yes	No	Yes	~1 000	~1	1 MSEK (typical), up to 300–400 MSEK	1 MSEK (typical), up to max 25 MSEK
2	Yes	Yes	Yes	Yes	~50	3–5	5 GSEK	100–200 MSEK
3	Yes	Yes	Yes	Yes		~1	15 MSEK to 10 GSEK	50 MSEK
4	Yes	Yes	Yes, optional	Yes	~5	~0	3 GSEK	100 MSEK
5	Yes	Yes	No	Yes		~0	500 MSEK to 3 GSEK	50–100 MSEK
6	Yes	Yes	Yes, optional	Yes, optional	~10	~0	1–10 GSEK	250 MSEK
7	Yes	Yes	Yes, optional	Yes	~10	0	100 MSEK to 10 GSEK	50–100 MSEK
8	Yes	Yes	Yes	Yes	N/A	N/A	Aiming for 5 MSEK till 5 GSEK	Aiming for 2–50 MSEK
9	Yes	Yes	Yes	Yes	< < 100	~1	100 MSEK to 10 GSEK	10 MSEK (typical), 2–100 MSEK

investigations and system restoration, as well as legal and PR costs related to cyber incidents. Products also cover 3rd party liabilities resulting from e.g. data and privacy breaches (including notification costs), malware spread from the insured, fines (if legal to insure by law), costs to comply with investigations and regulatory requirements, and internet or cyber media liabilities (e.g. copyright infringements, libel, etc.).

At the coarse level of detail described above, all the cyber insurance products investigated are similar in their offerings. However, there are also key discrepancy areas, which can be very important to customers. This is interesting, as lack of clarity on coverage in cyber insurance has been identified as a reason for its limited adoption (ENISA, 2012).

The first important discrepancy is whether non-malicious events (e.g. mistakes, omissions) are covered at all, and if so, which such events are covered (e.g. power outages). Here, companies have different policies. Some are very strict in not covering non-malicious events at all. I5, for example, describes such coverage as opening a potential Pandora's box, where it is difficult to know what kind of risk is accepted. This also conforms to I5's overall strategy, which is to offer a conservative "standard" cyber insurance product that does not differ much from competitors. Others offer optional coverage. I4, for example, does not include 1st party errors in the standard package, but offers coverage for errors or omissions committed by the insured as an add-on for an extra fee. I6, similarly, covers (i) attacks only in the standard coverage, but sells separate extensions also covering to (ii) human errors, (iii) technical failures, and also (iv) legal or regulatory requirements (e.g. when the police orders a system to remain shut down for the sake of a crime scene investigation). I7 also offers business interruption protection in three versions: (i) business interruption costs due to security events (attacks), (ii) costs due to attacks and system failures not due to attacks (any unplanned, unintended interruption is covered), both of which are triggered by the interruption, and (iii) additional protection against the effects of reputational harm triggered by data loss. Some offer coverage of non-malicious events as part of the standard package, for example I2, I8 and I9, but do not cover power outages or other physical damage that is outside of the insured party's control and that is typically covered by property insurance. These exceptions apply to the market in general – physical damage or bodily injuries caused by cyber incidents are not covered by cyber insurance. I8, however, remarks that there is scope for future product development where an add-on product covering physical damage from cyber events would be sold. The insurance intermediaries paint a similar picture. II1 and II2 both report that there is an ongoing development toward increased coverage of non-malicious events, but that current offerings differ in exactly what is covered.

A second discrepancy concerns the extent to which events at sub-contractors or external service providers are covered. Clearly, in the age of outsourcing and cloud computing, these differences can be very important to the insured. Again, insurance companies take different approaches. I6, for example, offers to cover outages at external service providers either unnamed (with an increase in the premium of some 20–25% and the indemnity limit cut in half) or a specific list of some 3–5 named providers. Others, such as I7 and I8, make no distinction between internal outages and outages at external

service providers. Indeed, I7 believes that most companies are actually better off, from a business interruption perspective, trusting providers like Microsoft, Google, or Amazon rather than trying to build equally reliable in-house IT environments. These big service providers, however, typically have terms and conditions where they do not accept responsibility for business interruptions caused by service outages, meaning that it is prudent for their customers to buy insurance coverage instead.

A third discrepancy, pointed out by II3, relates to the coverage offered for subsidiaries and corporate entities in different jurisdictions. For example, I3, I5, and I6 all automatically cover new subsidiaries created during the policy period, subject to some exceptions regarding size, line of business, and jurisdictions. However, their exceptions differ. For example, I3 allows a new subsidiary to have assets worth up to 20% of the total assets of the insured (parent company and all subsidiaries together), I5 sets the same limit to 25%, and I6 instead imposes a limit at 10% of the total turnover. Similarly, exclusions on jurisdictions vary. I3 covers wrongful acts committed and claims made anywhere in the world, but excludes claims and regulatory proceedings brought or originating in the US and Canada. I5 per default imposes territorial and claim jurisdiction limits that exclude the US and Canada. I6 per default covers losses incurred and claims made in the entire world.

A final observation regarding coverage relates to the division of labor between cyber insurance on the one hand and traditional property and liability insurance on the other hand. For example, I1, which does not cover non-malicious events in its cyber insurance, remarked that a cyber business interruption caused by non-malicious outages might still be covered by a traditional business interruption insurance, though this would not be explicitly clear from the policies. Then again, as remarked by I2, a traditional business interruption insurance might *not* cover a cyber business interruption. I8 remarked that they might have undesired coverage of cyber business interruption in their non-cyber portfolio, i.e. traditional business interruption insurance where cyber incidents are not explicitly excluded, and a customer thus reasonably could make a claim. If in such a case an agreement cannot be reached, the interpretation of the policy would have to be settled in court. I1, I2, and I8 all agreed that this situation is undesirable, and that it is mostly due to old policies written for stand-alone machinery (e.g. a business interruption insurance designed to cover losses resulting from outages in manufacturing machines) not having been updated to reflect today's realities (e.g. integrated supply chains, Industry 4.0, and industrial Internet of Things). From the re-insurance perspective, RE2 also remarked that uncertainty about what is covered in existing policies also can have a profound effect on re-insurance companies, exposing them to large and unexpected losses.

The question of how much coverage for cyber events is included in traditional insurance was at the heart of the interview with I10, which does not offer any pure cyber insurance product today. I10 identified two products in their portfolio that might cover cyber events: (i) a computer breach clause in the crime insurance policy (a liability insurance designed to cover financial losses caused by employee dishonesty), and (ii) the business interruption insurance essentially designed to cover fire, flooding, and machinery breakdown. According to I10, the computer breach clause in the crime insurance policy would probably be difficult for the insured to use, as the insured has the burden of proof that a breach has occurred, and as there is a sweeping exception for "computer viruses", making the policy difficult to interpret unambiguously. As for the business interruption insurance, I10 largely agrees with the comments from I1, I2, and I8, that policies are not as clear and explicit as would be desirable. Interruptions without physical damage are explicitly excluded, disqualifying many cyber incidents, but not all. For example, a Stuxnet like incident where a production facility is hacked and machinery is run outside specifications until it breaks would not be excluded by the physical damage criterion, since physical damage indisputably occurred. To summarize, I10 finds itself in a position where it has unquantified and uncertain exposure to cyber risk in traditional non-cyber insurance products. In the long run, this is not desirable. However, the exposure remains largely potential, as of now, since the representatives of I10 did not know of any cyber-related claims under either of the two relevant policies. I10, being an insurance company with mostly small and medium sized customers, many of whom traditionally have not been very dependent on information technology, reports that it and its European peers are a bit hesitant about development of cyber products.

The ambiguity of coverage – customers might think that cyber incidents are covered, the insurer thinks they are not – is familiar from the literature (Eling and Schnell, 2016b).

4.2. *Incident first response services*

An essentialist view of cyber insurance might be that it is only a product where a policyholder pays a premium to receive financial compensation in case of certain IT related adverse events. However, the investigated cyber insurance products are not pure financial risk transfer instruments in this sense. Rather, all informants affirm the importance of first response incident management as an integrated part of their products and an important sales driver. As pointed out by II1, these services also give insurance companies a degree of control of the quality of incident management, making it easier to predict and manage the costs of incidents.

This service typically takes the form of a one-stop-shop incident telephone service which the insured calls when an incident occurs. The insurance companies do not provide this service in-house, but rather partner with IT consultancies, law firms, PR consultants etc. who deliver the actual first response services. Typically, the first response is coordinated by a law firm or a dedicated claims management firm, that calls upon other consultancies as needed.

The exception to this rule is I6, which at the time of the interview did not offer this kind of all-consultancy-costs-covered initial response. The reason was the risk to act on false alarms, i.e. events that are not triggers specified in the policy. I6 did not want to allow the client to self-initiate a potentially expensive all expenses paid initial response. At the time of the final verification, however, I6 had started to offer first response incident management as an optional service depending on the client's maturity, in particular with regard to having a well-established in-house IT incident management function. Other companies take similar steps to mitigate the risk of false alarms. For example, I8 emphasizes that the in-

cident response service is not a general helpdesk, but only covers the triggers specified in the policy.

4.3. *Market composition*

All informants agree that the Swedish market for cyber insurance still is small, but also that it has grown quickly in the past 18 months (i.e. from spring 2015 until fall 2016) and that it is expected to grow more in the future. Compared to the other Nordic countries, Sweden and Denmark are typically assessed to be the more mature markets in terms of cyber insurance adoption, with Finland somewhere in the middle and Norway somewhat trailing.

Cyber insurance in Sweden is currently mostly bought by relatively large companies, or by smaller companies with exposure to the US market where cyber insurance is often regarded as a hygiene factor, i.e. a *sine qua non* for doing business. This is reflected in the customer turnover column of Table 1. According to the informants, there are two main reasons for the dominance of larger customers. First, as pointed out by II1, large companies are often the customers of large global insurance companies, who have ventured into the cyber insurance market. Smaller companies are more often customers of smaller domestic or regional insurance companies that may not offer cyber products (this is the case of I10). Not being able to procure cyber insurance from one's regular insurance company should raise the threshold for buying cyber insurance. Second, larger companies are accustomed to commissioning insurance intermediaries, who are a key actor and almost always facilitate the sales of cyber insurance. Intermediaries can also have a contractual obligation to keep their customers informed about emerging threats and emerging insurance products, meaning that smaller companies without commissioned intermediaries will not be exposed to the idea of cyber insurance products as early as larger ones. (While the insurance companies often emphasize the role of the intermediary in sales, some intermediaries also point to other factors. II2 maintains that cyber insurance sales are very incident driven, i.e. that companies react to incidents happening to themselves and news stories of incidents happening to others. According to II2, cyber insurance is more difficult to manage for the intermediaries compared to other kinds of insurance, due to the complicated underwriting process. See also the discussion in Section 4.5).

Looking at the customer turnover column of Table 1, it is also evident that I1 has a different customer base compared to the rest. I1 has relatively many customers, but also relatively small ones, as measured by their turnover and indemnity limits. The only competitor to I1 in the small business segment is I8, which at the time of the interview was just launching its cyber insurance product. Thus, I8 did not give any actual number of customers, but stated its aims for customers with a mere 5 MSEK in turnover.

4.4. *Pricing, premiums and competition*

As seen in Table 1, the number of claims handled by the insurance companies is very low: the typical insurance provider handles zero, or at most a handful of claims in Sweden annually.

As a result, pricing is more based on expert models than on historical data, though every informant aims to move in a more data-driven direction. Typically, pricing and price differentiation is based on the following factors:

- Company size/turnover
- Indemnity limits, deductibles
- Industry, as a proxy for risk exposure
- Market exposure to others jurisdictions (especially the US)
- Assessment of IT and information security maturity, based on forms, interviews, IT audits etc.

Many informants mention that they, as long-standing international players in cyber insurance, have substantial amounts of historical claims data. For example, I2 has data since 1995 and I4 has 20 years of data. However, while all the big insurance companies have many years' worth of historical data, this has limited relevance and applicability to a customer in a particular industry in a particular (non-US) country in the particular kind of IT environment of today. Thus, I2 admits that its data are not very fine grained in terms of countries or industries, and I3 remarks that claims data in the cyber area are something that everyone wants, but no one really has, at least not as much as they want. I5 confesses to being outside the comfort zone when it comes to pricing, because there is not enough data to build an accurate statistics-based model. I5 attributes the variability in premiums seen on the market to this fundamental uncertainty – no one knows the right price. I6 agrees that there is not enough data to create a pricing model based on historical claims data – a decade or so is not enough. I6 also highlights the differences between markets. For example, the deductibles on the US market can be of the same size as the indemnity limits in Europe, so applying US data in the Swedish or broader European context is not reasonable. I7 agrees that even though the company has proprietary data on claims from the US and the UK, it is difficult to translate that to the circumstances on the Nordic market. Cyber claims at I7 are treated as catastrophic events that happen maybe once per hundred years, not like everyday events where detailed actuarial models can be built. Only now is I7 starting to be able to compare prospective customers to similar existing ones in terms of being in the same industry, of the same size, and in the same geographical location. I9 also tells the same story: Pricing is currently not actuarial in the sense that it is based on historical claims data – the number of claims is far too small.

However, I6 and I9 also remark that in the future, pricing will probably become more based on historical data, as markets grow and laws become more harmonized across jurisdictions. Thus, in the longer run, market prices will probably converge.

This lack of actuarial, statistics-based, pricing is a cause for concern for re-insurance companies. RE1 perceives that many products are based on historical data that may be irrelevant in two ways: (i) being based on simple DDoS and script kiddie attacks, and (ii) being based on US data breach notification laws. For customers facing more advanced threats in other jurisdictions, there is no way to know if the pricing is right. RE2 adds that pricing probably is more based on rules of thumb like industry than on the individual risk profiles of the customers, and that proper understanding of risk aggregation poses

a significant challenge when it comes to cyber insurance products. The price convergence scenario suggested by I6 and I9 can also be contrasted with a more sinister scenario that RE1 warns for: that a large and unforeseen event (a "cyber 9–11") causes a backlash for the entire cyber insurance market, suddenly making (some kinds of) cyber risks very difficult to insure on the market.

As outlined above, the actual premiums paid depend on several factors, such as the size, risk profile, industry etc. of the insured. Therefore, average or typical premiums for cyber insurance are useful only as first indications. Nevertheless, the question was asked, and some characterization of premiums can be made.

A typical annual premium span is some 5–10 kSEK per MSEK indemnity limit, i.e. 0.5–1% of the indemnity limit. Some informants give a wider span of 5–15 kSEK per MSEK, some give figures somewhere in the middle, i.e. 7 or 8 kSEK per MSEK, some give slightly higher figures like 12 kSEK per MSEK. (For anonymity reasons, these sensitive figures are not associated even with the I1–9 pseudonyms.) According to II1, it is possible to get premiums even below 5 kSEK per MSEK.

There is a common perception that increased competition has put pressure on premiums. Thus, I3 perceives itself as more conservative than some competitors that are trying to get into the market by dumping prices, I5 remarks that competition might in the end turn cyber insurance into a commodity, and I6 holds that premiums are down a few kSEK per MSEK compared to a few years ago. I9 agrees that premiums have decreased over the past few years due to competition, but also predicts that premiums might stabilize or even climb again in the face of more incidents and claims.

It should be pointed out that there is no necessary contradiction in the diverse premium figures given by different companies. First, there is a perception that prices differ between insurance companies, so it stands to reason that different insurance companies will state different typical premiums. Second, the number of customers of each insurance company is so small that outliers (in terms of size, indemnity limits, risk exposure, etc.) would be expected to lead to different observed average premiums even if everyone was using the same pricing model. Third, there is a time lag by which some premium figures might be based on an earlier, less competitive market situation, while others are based on the present, more competitive market. As remarked by I3, there has been a considerable increase in competition over the past six months (i.e. the second and third quarters of 2016), with the number of companies offering cyber insurance growing from some six to some ten.

4.5. *The underwriting process*

The informants all use questionnaires to determine the situation and maturity of their potential customers. This is also the basis of the pricing model described in Section 4.4 above. I1 *prima facie* appears to be an exception in that such a questionnaire is only used for higher indemnity limits, but as is evident from Table 1, a high indemnity limit from the perspective of I1 is a low indemnity limit from the perspective of the other companies.

In addition to self-assessment questionnaires, additional reports are typically developed in-house by cyber risk engineers, or procured externally from specialized consultancies such as auditors and IT security consultants, who may perform e.g. penetration tests. Some informants explicitly let the procedure depend on the customer, e.g. I3 always conducts additional interviews and risk assessment by a cyber risk engineer for customers with a turnover above 3 GSEK. Most informants place a high value on personal interviews with stakeholders such as CIO, CFO, CEO to assess risks.

As a result, the cyber insurance underwriting process is relatively complicated and takes relatively long time before signing, compared to other, more standardized insurance products. Thus, II2 points to the information gathering requirements as a complicating factor from the intermediary perspective. II3 emphasizes that cyber insurance coverage and conditions are not as standardized as other insurance products: some insurers offer standard policy terms with a broad coverage of cyber events, others offer a narrower standard package where additional protection is optional. Still, informants generally agree that intermediaries play an important role in the underwriting process.

One factor that drives the complexity of the underwriting process is that cyber insurance is not a bulk product, but is highly tailored to each customer, as is also evident from the coverage discussion in Section 4.1. Another complication is that clients are first time buyers of cyber insurance. In other words, cyber risks are a kind of business risk that has not previously been quantified by the insured. Doing so, and determining how much of it to transfer by buying insurance, is quite difficult for companies as a first-time exercise. On a future, more mature, market where insurance providers have begun losing cyber insurance customers to each other, underwriting might become less complicated.

4.6. *Business interruption*

An important aspect of the coverage of lost revenue from business interruption is the *waiting period* applied. A waiting period is a mechanism similar to a deductible, but based on time rather than money. Under a policy with a waiting period, compensation for lost revenue from business interruption is only paid when the duration of the business interruption exceeds the waiting period.

The shortest waiting periods offered by the insurance companies interviewed are 6 hours (I2, I5, I7, I9) or 8 hours (I3, I4, I8). However, just like deductibles, waiting periods are tailored as a matter of pricing and negotiation, and most actual policies sold have significantly longer waiting periods than these minimums, such as 24, 36, 48, or 72 hours. Though uncommon, it is also possible to negotiate shorter waiting periods – II1 reports that they have brokered a contract with a waiting period as short as 2 hours, however only applicable to outages causing losses over a threshold amount.

The compensation paid for a business interruption that exceeds the waiting period is calculated according to standard accounting and auditing principles, similar to how lost revenue from fires, floods etc. are calculated under a regular property insurance policy. However, as pointed out by II3, the details of these calculations still differ between insurance com-

panies, particularly the period of historical data (e.g. a quarter, a year or several years) that is eligible when determining the amount of lost revenue.

One way to assess the impact of business interruptions is to build models based on Mean Time to Failure and Mean Time to Restore for customer IT services (or even to use full distributions rather than means). However, the insurance companies typically do not build such models of IT service availability. I2 sometimes buys this kind of service from specialized consultancies. I3 explains that historically, when business interruption was the exclusive realm of property insurance, such models were built. However, for business interruption as part of a wider cyber insurance, I3 does not use such models. I4 is the only company that conducts detailed availability calculations using MTTF and MTTR in-house, but only on a client by client basis.

I5, I6, I7, I8 and I9 do not conduct detailed availability calculations of client IT services. I8 remarks that such detailed modeling would be interesting for very large risks only, thus implicitly making a cost/benefit analysis of the modeling effort. II1 remarks that MTTF and MTTR will be different in different systems, meaning that such models are difficult to accurately apply at the enterprise level, which may span hundreds or even thousands of systems.

It is interesting to contrast these findings with the practices in traditional business interruption insurance. I10, which does not have any cyber insurance products, is similar to the other companies in not conducting any detailed availability calculations using MTTF and MTTR – neither for cyber events nor for traditional events (e.g. fires or floods). The adjustment of the premium offered to the client is instead industry dependent, thus differentiating e.g. manufacturing from professional services or transportation. However, one interesting observation is that the traditional business interruption insurance offered by I10 does not have an indemnity limit (as all the cyber insurances do), but rather compensates actual loss all the way up to the full turnover of the client, with the deduction of a 24-hour waiting period. This is probably due to the small size of most of I10's customers.

4.7. *Requirements on the insured*

If cyber insurance is regarded as a pure financial risk transfer instrument, it might be thought that insurance companies are willing to insure any risks, provided that the premium paid is high enough. However, none of the investigated insurance companies work this way. I2 reports that depending on the outcome of the customer assessment, sometimes no offering is made, and sometimes only partial protection is offered. I4 has a number of "red flags" in the policies, i.e. certain parts of the policy cannot be offered unless the customer meets certain requirements. For example, a customer without an incident response process cannot be insured at all. Similarly, I7 explicitly says that it is preferred to turn a bad customer down over accepting risky clients at a higher price. I9 also has some basic criteria which must be met by the customer to even get an offer, but this minimum baseline varies with industry and risk exposure.

If turning customers down is the stick, there is also a carrot in the form of lower premiums for more secure and less risky customers. I2 reports that the outcome of the underwriting process is a list of actions to be taken, allowing the customer to improve its IT environment in order to get a lower premium. Similarly, I3 and I4 both use pricing models where improvements in the security parameters lead to lower premiums, though I4 adds that its pricing model always defines a minimum price. I5 also rewards improved security with lower premiums, and at least on the US market also offers customers assistance from so called breach coaches, who demonstrate exploits and offer help in finding vulnerabilities that should be mitigated. I6 remarks that customer maturity in terms of e.g. network segregation, endpoint protection etc. "has a huge impact on customer premiums". I9, as part of the underwriting process, has a dialog with the customer about the road ahead, including possible future security improvements that have an impact on insurance premiums.

I1 and I8 differ a bit from this pattern. Both report a greater reliance on static security guidelines that must be fulfilled by the customer for the insurance policy to be valid, rather than thorough individual risk assessment. Both also say that improved security in principle could lead to lower premiums, but have not actually put this into practice. As remarked by I8, such practices probably suit bigger clients better. This also seems to be the best explanation for I1 and I8 breaking the pattern: they operate (or aim to operate) with smaller customers and thus offer more of a bulk product.

5. Discussion

In the following, reliability and validity of the findings are first discussed, followed by some substantive implications of the results.

5.1. *Reliability and validity*

The reliability of the findings should be assessed as good. First, there is virtually no risk of sampling distortion, as the informants do not represent a sample, but essentially all companies selling cyber insurance on the Swedish market have been interviewed.

Second, the iterative measures taken to verify the interview results – collecting informant comments on interview notes, at a seminar, and on the manuscript – should have eliminated most inaccuracies and misunderstandings from the data collection.

Third, the high degree of unanimity among the informants about the basic characteristics of the Swedish cyber insurance market suggests that the results are reliable in the sense that they would not change much if, somehow, an additional informant company were interviewed. This could be contrasted to a hypothetical low-reliability situation where only I1 and one of the other primary informants had been interviewed, resulting in lack of unanimity among informants.

As for validity, the situation is a bit more complicated. The main threat to validity is inherent in the method chosen. The interview situation allows informants to answer in ways that – consciously or unconsciously – distort the facts. In particular, the numerical answers elicited may be subject to well-

known psychological biases and heuristics (Tversky and Kahneman, 1975). For example, informants may exhibit an *availability bias* e.g. by equating a "typical" indemnity limit or premium with that of the first customer that comes to mind, regardless of its representativeness. They may also exhibit *anchoring* e.g. by being influenced by a recently stated figure of customer turnover when assessing an indemnity limit. Anchoring effects in particular cannot be disregarded, as the author sometimes gave examples of responses from other informants in order to gain trust in the interview situation, especially to obtain the sensitive information about premiums. Results should be interpreted with some caution in the light of this. Nevertheless, it should also be remembered that the informants are experts in the field of cyber insurance, who earn their living working with these figures. In the light of the previous lack of numerical figures in the literature, the findings of Section 4 should still be regarded as progress.

To some extent, these threats to validity are also mitigated by the use of the secondary informants. Since reinsurance companies and insurance intermediaries are knowledgeable about cyber insurance, but not biased or partial in the same ways as the insurance companies, the inclusion of their perspectives and the relative unanimity of these with those of the primary informants strengthens validity.

To further strengthen validity, additional data collection using different methods would be needed. Perhaps most obvious is a demand side investigation, using buyers of cyber insurance as informants. This remains future work.

5.2. *Generalization to markets beyond Sweden*

Connected to issue of validity is the possibility to generalize the results to other markets, beyond Sweden. This question can be asked in several consecutive versions.

First, generalization to the Nordic region is relatively straightforward. None of the cyber insurances investigated is sold in Sweden only, and most of the informants do underwriting in the entire region. This is also evident from the comments on market composition, where informants often spontaneously contrasted Sweden with the other Nordic countries, as seen in Section 4.3. In terms of Table 1, everything but the number of customers and claims in Sweden should be valid in the whole Nordic region.

Second, generalization to other countries that are mature in IT in general, but where the cyber insurance market is still growing fast, is also possible. In these cases, the numerical figures cannot be transferred, but qualitative features such as the dynamics of the interplay between global and regional insurance companies probably still hold true.

Third, generalization to cyber insurance anywhere in the world should be made with more caution. As noted above, I6 highlights the differences between markets, e.g. that deductibles and indemnity limits can vary by orders of magnitude, so simplistic generalizations are discouraged. However, since I2, I3, I4, I5, I6, I7, and I9 are all global companies, many aspects of the coverage and incident first response services they offer, the underwriting process they follow, the waiting periods they apply, and the requirements they pose on the insured should be true in all markets, i.e. substantial information about product offerings anywhere in the world can be inferred from this study. Clearly, though, the effects of different jurisdictions are important to consider here.

5.3. *Market segmentation*

Based on the findings reported in Sections 4.3 and 4.5, there seems to exist a market niche not yet fully occupied for more standardized cyber insurance, using a simpler underwriting process, and aiming at small and medium sized enterprises. Currently, only I1 and to some extent I8 occupy this niche in Sweden. Indeed, the fact that I8 launched their cyber insurance product during the interview period provides some evidence that this niche is now increasingly being filled, as does a comment from II1 that the underwriting process is increasingly being segmented, with background checks ranging from simple evaluation forms to exhaustive IT audits.

5.4. *Pricing*

In line with the literature (Bandyopadhyay et al., 2009; ENISA, 2016; Shetty et al., 2010; Wheeler et al., 2015), the findings reported in Section 4.4 suggest that accurate pricing of cyber insurance is very difficult and that in practice, it is based on expert models rather than on historical data.

An *actuarially fair premium* means that the cost of an insurance policy is precisely its expected value. On an idealized theoretical market where (i) competition drives the profit of insurance companies to zero, and (ii) the probability of losses is not affected by customer behavior, full insurance for losses will be sold at market prices corresponding to actuarially fair premiums (Varian, 1992). In other words, if the probability of losing 1 MSEK a given year is 1%, the annual insurance premium would be 10 kSEK.

Real markets, of course, do not correspond to this neat model. First, competition is not perfect, and insurance companies do make profits. Second, the probability of losses is affected by customer behavior, and thus insurance policies contain deductibles, waiting periods, and various proactive activities to limit risk.

Nevertheless, the mechanism of competition is real, and according to all informants, it is driving premiums down. On the ideal market, competition would never drive premiums below the actuarially fair premium, because the probability of loss is known, and insurance companies would knowingly incur expected losses by such pricing. However, on the Swedish cyber insurance market, the probability of loss is *not* known, because there is not enough historical data of the right kind to estimate it accurately.

The theoretical concept of the actuarially fair premium is useful in that the concerns of some informants can now be phrased more clearly: RE1 and RE2 are worried that market prices might be below the actuarially fair premium. Thus, in the longer run, insurance companies would incur losses, even though they have not done so in the short period lived through so far. RE1 worries that the correction (a "cyber 9–11") would be akin to any pricing bubble bursting, impeding the functioning of the market in the aftermath. The prediction of I9 that premiums might stabilize or even climb again in the face of more incidents and claims can be interpreted as a more mod-

erate worry that current market prices might be below the actuarially fair premium. Finally, as I6 and I9 remark that future pricing based on historical data will probably cause market prices to converge, this means that the market will have a better understanding of what the actuarially fair premium is.

Contrary to the concerns of RE1 and RE2, II1 argues that current market prices are well above actuarially fair premiums. This argument is backed up by statistics on cyber insurance, covering 2013–2016, from the Lloyd's Market Association, showing gross loss ratios, i.e. ratios of paid and outstanding claims to premiums, that are comfortably below 70%. (Note that gross loss ratios correspond to *gross* margins – to assess the *net* profits of insurance companies, all operating costs must also be accounted for. Thus, actuarially fair premiums would correspond to *net* loss ratios of 100%, i.e. no profit made.) However, as discussed in Section 4.4, a few years' worth of statistics is not enough to be considered conclusive evidence.

Finally, it should be noted that the concerns recapitulated above correspond to the interests of the respective informants. The re-insurers worry that premiums are too low, so that they will incur losses. The insurance intermediaries worry that premiums are too high, so that their clients will pay too much. Pricing is a notoriously difficult area, and the findings reported here in no way settle the question of how current premiums relate to actuarially fair prices. It does, however, shed some light on the current practices of pricing, including their limitations.

5.5. *Business continuity and waiting periods*

From the perspective of business continuity, the waiting periods applied in cyber insurance policies are interesting to discuss. For decades, it has been acknowledged that even short IT service outages can have significant impacts (IBM Global Services, 1998), and more recent practitioner reports estimate average hourly costs of downtime for large companies in the hundreds of thousands of US dollars (Rapoza, 2014). The availability of IT services is often characterized by the number of "nines", i.e. 99.9% availability is three nines, 99.99% is four nines, etc. Service level agreements with three nines or better are very common. Some argue that enterprises typically require four nines or more (Durkee, 2010). Three nines correspond to just below 9 hours of downtime for *all* outages in a 24-7 operating year (even less if scheduled downtime and maintenance are subtracted from the operating year). Still, the waiting periods found in the standard cyber insurance policies are never shorter than 6 or 8 hours for a *single* outage (though these are negotiable), and often in practice one or several days. Thus, waiting periods *prima facie* appear very long compared to many IT service outages, including severe ones that receive much media coverage.

To give a concrete example, Fig. 1 illustrates the cumulative distribution functions for the time to recovery of 1876 incidents, corresponding to 672,272 minutes, or just over 11,000 hours of downtime recorded from January 2009 to May 2011 at a large Nordic bank (Franke et al., 2014). The diagram illustrates the durations of these IT service outages on a logarithmic scale. The five different distributions shown correspond to *channels*, a business side categorization of IT services into categories such as automated teller machines (ATMs), Internet banking,

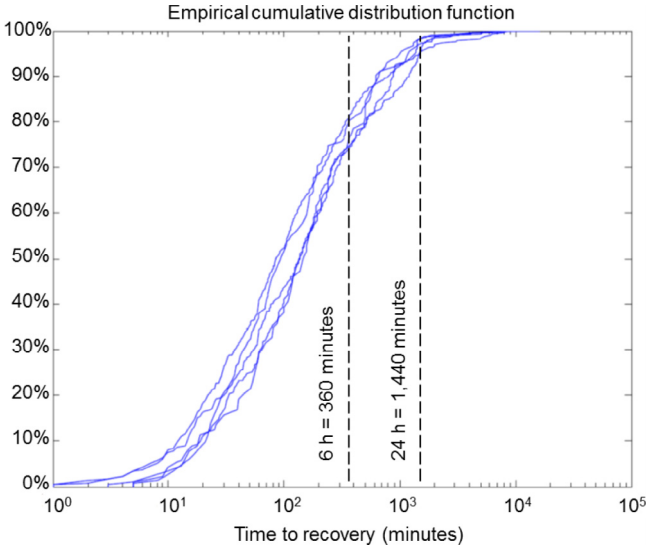


Fig. 1 – Cumulative distribution functions for the time to recovery of 1876 incidents at a large Nordic bank (Franke et al., 2014) with waiting periods approximately superimposed.

credit card payments, etc. Of course, it is not certain that all IT service outages are similarly distributed, but Fig. 1 is from one of the few examples in the scientific literature where IT outage distributions have been investigated empirically, and it also happens to be an example from the geographical area investigated here.

Approximately superimposed onto Fig. 1 are two waiting periods: 6 hours (the very minimum found on the Swedish cyber insurance market), and 24 hours (a more typical waiting period). As clearly seen in the diagram, only a tiny fraction of outages last long enough to exceed a typical 24 hours waiting period.

At first, it might seem counterintuitive that waiting periods disqualify some 95–99% of IT service outages. However, insurance is typically not about managing small everyday risks, but rather about managing large but uncommon risks, that might be very expensive if they occur. Thus, it makes sense, both from the perspective of the insurance company and the insured, that a large number of mundane outages are indeed managed internally by the insured, without any need to involve the insurance company for doing loss adjustment. The example is instructive: the data in the diagram correspond to some two incidents per day in the period studied. Clearly, involving the insurance company should only happen for a fraction of those.

However, it might also be the case that different customers in different market segments have different preferences. For example, the bank in the example has a competent in-house IT department that manages IT service outages on a daily basis, and it thus makes sense to have a long waiting period and self-insure the short outages. For a smaller enterprise that does not have the same in-house capacity, it might make sense to pay a higher premium to have a shorter waiting period. On the other hand, another small company might have its entire IT outsourced, and so not need to bother with in-house outage management at all. It remains to be seen if increasing market segmentation with more offers tailored to smaller customers

(as discussed in Section 5.3) will also have an impact on waiting periods. In addition, it should be noted that the first response services included in cyber insurances are offered to all customers, and are activated immediately, not being subject to waiting periods.

5.6. *Cyber insurance, risk management, and asymmetry of information*

In the field of risk management, responses to risks are often classified by the fourfold categorization of (i) avoid, (ii) transfer, (iii) mitigate, and (iv) accept (Hillson, 2002). In this paradigm, insurance is the archetypal example of risk transfer. Therefore, it is interesting to note that the cyber insurance products studied are *not* pure mechanisms of risk transfer.

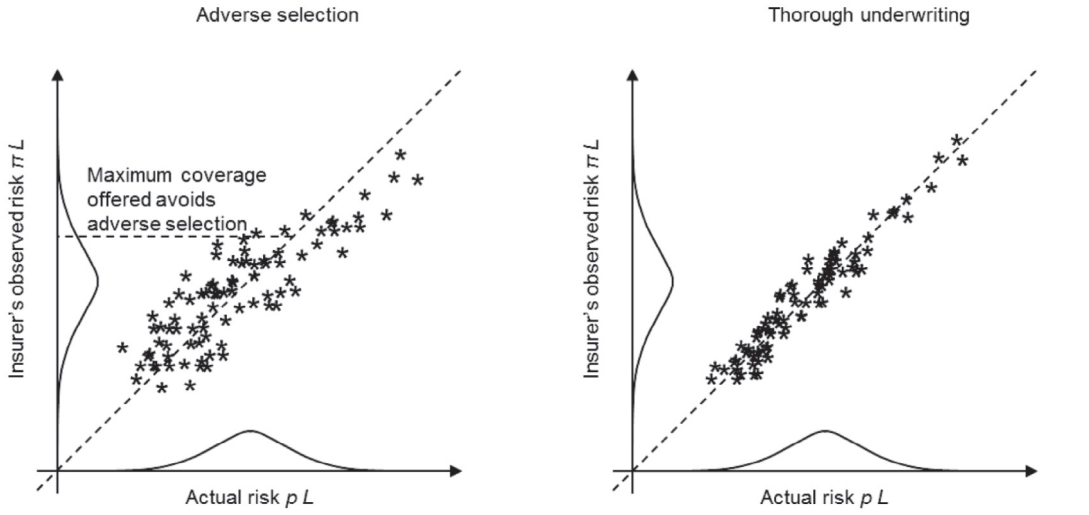
Two features are noteworthy: First is the fact that incident first response services are not only included in cyber insurance packages, but actually central to customers, as related in Section 4.2. Customers "want to know whom to call when incidents occur", as noted by I2. Such risk response services add aspects of accept (incidents will occur) and mitigate (a well-managed incident will have less severe consequences) to the basic transfer mechanism of the insurance.

Second is the fact that insurance companies pose information and IT security requirements on their customers, and use pricing and underwriting to nudge customers in a more secure direction. This adds aspects of avoid (with better practices, some incidents will not occur) and mitigate (with better practices, consequences are less severe). Furthermore, the extent of transfer is rationed, in that customers that are too immature or have too poor security are turned down.

It is worth commenting on the fact that cyber insurance is not available on the market for those customers perceived to be the riskiest. This is expected on a standard insurance market, where *asymmetry of information* may destroy the market: if insurance policies for high risk customers were offered, they would be very expensive, and thus attract only customers who perceive themselves to be at very high risk. This principle is illustrated in Fig. 2 (a), where the high risk customers are actually even more risky than observed by the insurer. When risk is not fully observable to the insurance company, such *adverse selection* can be dealt with by introducing a maximum coverage offered, refusing coverage for the most risky clients (Akerlof, 1970; Anderson and Moore, 2006).

However, this standard explanation of why prices do not just rise to match risks is not as convincing on the Swedish cyber insurance market as on insurance markets in general, because on this market, the risks are thoroughly evaluated as part of the underwriting process (as related in Section 4.5). In Akerlof's classic example of asymmetric quality information, the market for used cars, supply and demand become zero because quality is known only to the seller, but not the buyer. Thorough and competent inspection of the car would alleviate this. The effect is illustrated in Fig. 2 (b), where thorough underwriting improves the observability of customer risk. Here, the insurer's risk observations of high risk customers are, on average, correct. Thorough underwriting would thus *prima facie* be expected to lead to the insurability also of high risk customers.

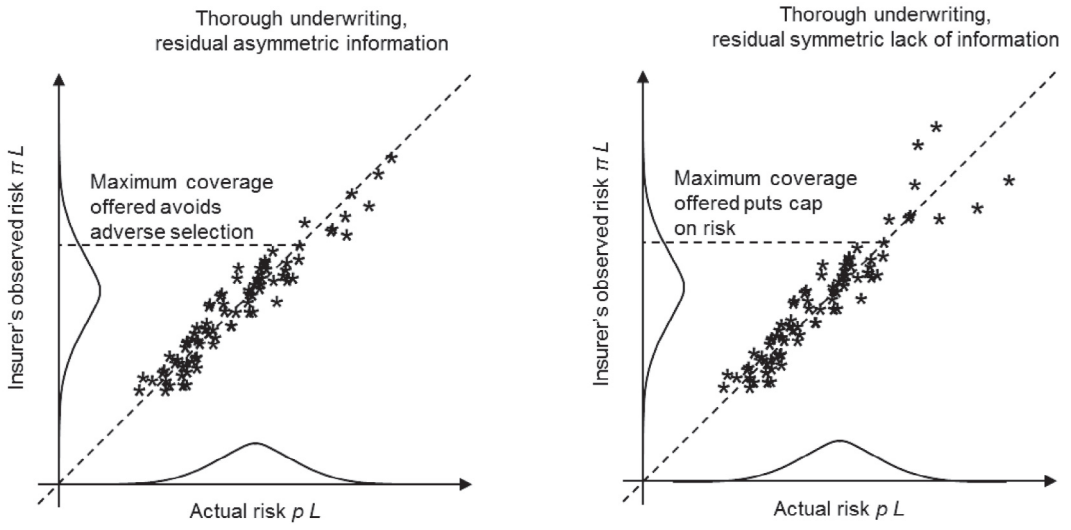
Then again, insurance companies may not believe that their thorough underwriting leads to the situation depicted in Fig. 2 (b), and they may be correct. First, it may be that there is *residual asymmetric information*, even after the underwriting process, so that although some risks are known and understood by the insurance company, other residual risks are still known and understood by the customer only. Then adverse selection would still occur, as illustrated in Fig. 3 (a), and refusing coverage to the riskiest customers still makes sense. This is



(a) Asymmetric information leads to adverse selection. A maximum coverage can avoid the problem.

(b) Sufficiently thorough underwriting might do away with asymmetric information.

Fig. 2 – Sketches illustrating asymmetric information and adverse selection. There is an actual probability distribution p for an insured party to suffer loss L, but the insurer only knows the observed distribution π. The more accurately the observed risk matches the actual, the closer any sold policy * will be to the 45° line.



(a) Residual asymmetric information despite thorough underwriting.

(b) Large residual symmetric lack of information despite thorough underwriting.

Fig. 3 – Sketches illustrating asymmetric information and adverse selection.

surely true to some extent. Second, it may be that there is a large *residual symmetric lack of information* about the risk level, even after the underwriting process, i.e. both parties know equally much, but uncertainty is still large. This is illustrated in Fig. 3 (b), where the number of high risk customers over- and underpriced is the same (no adverse selection), but observations are still not very accurate. This is certainly the case in some instances. For example, I5 is explicit in having as a strategy not to assume too much risk, even though building volume – making sure to have enough customers that risk is meaningfully spread among them – would be a different strategy to manage the risk of the customer portfolio.

A more practical perspective, as noted by I2, is that insurers work in a similar way to fund managers at banks, deciding what type of companies are wanted in the portfolio and then trying to manage and evaluate these as thoroughly as possible, within a set risk appetite that determines who is desirable to insure. I4 similarly presented a rank ordering of industries in terms of risk (retail being the best, pornography the worst). From this perspective, underwriting and risk management is not the abstract exercise in economics illustrated above, but rather an evolving enterprise with several contributing control mechanisms, not all of which are necessarily captured by Figs. 2 and 3.

6. Summary and conclusions

The results reported in this article offer an interesting picture of the cyber insurance market in Sweden. Market offerings are quite similar in covering both 1st party costs e.g. from business interruption, and 3rd party liabilities e.g. from data breaches. However, there are important discrepancies in the coverage of non-malicious events, the extent to which events at sub-contractors/service providers are covered, and the coverage for subsidiaries and corporate entities in different jurisdictions. The cyber insurance policies offered are not pure instruments of risk transfer, but typically also contain first response incident management, which is an important sales driver.

The Swedish cyber insurance market is rapidly growing, but cyber insurance in Sweden is currently mostly bought by large companies. This reflects a market segmentation where the standard products come with a complicated underwriting process tailoring offers to large customers, but some niche players are increasingly offering simpler policies aimed at smaller customers. Accurate pricing of cyber insurance is difficult and is based on expert models rather than on historical data. Lack of actuarial pricing is a cause for concern, at least among re-insurers who fear that pricing is wrong. In the long run, there is a belief among market actors that prices will become more accurate and converge, but there is some disagreement on whether this correction will mean lower or higher premiums, and whether it will be benign or a bubble bursting. Anyhow, increased competition has put pressure on premiums on the Swedish market. As a rough indication, the typical annual premium span is some 5–10 kSEK per MSEK indemnity limit, i.e. 0.5–1% of the indemnity limit.

Waiting periods when business interruption occurs are long (6–8–24–36–48–72 hours) compared to many outages. This probably reflects the principle that insurance is about managing large but uncommon risks, rather than small and mundane ones. However, preferences for waiting periods may vary over different customer segments.

Insurance companies are not willing to insure customers that are too immature or have too poor security. To some extent, this can be understood from standard reasoning about adverse selection, but particularities to the cyber market also make for

additional complications. Insurance companies impose information and IT security requirements on their customers, and insurance pricing and underwriting nudge customers in a more secure direction, though practices vary between insurance companies.

While the study is limited to the Swedish market, the results are of broader interest, as some aspects can be generalized to the global arena. While absolute numbers such as deductibles, indemnity limits, number of customers and number of claims cannot be transferred from the Swedish setting, many important qualitative features can be expected to apply worldwide. This includes the dynamics of the interplay between global and regional insurance companies in other countries that are mature in IT in general, but where the cyber insurance market is still growing fast. It also includes coverage and incident first response services, underwriting processes, waiting periods, and requirements posed on the insured, at the very least with respect to I2, I3, I4, I5, I6, I7, and I9, which are all global companies.

Though the picture summarized above is interesting, it is by no means complete. A few avenues for future work suggest themselves. First, an obvious road ahead is to complement the supply-side investigation reported here with a similar demand-side one, i.e. to conduct a study with cyber insurance customers. Such a study could corroborate findings regarding e.g. premiums, underwriting, and security requirements imposed, as well as answer new questions regarding e.g. insurance as part of wider risk management practices, rationales for procuring cyber insurance, and the role of the insurance intermediary. A second interesting undertaking would be to combine the mathematical cyber insurance models found in the literature with findings from qualitative empirical research such as that reported in the article. A third area concerns cyber insurance decision-making and the preferences of decision-makers. This could be studied e.g. with an experimental economics approach, as has previously been applied to availability service level agreements (Franke and Buschle, 2016). A fourth area deals with different markets and would include more detailed investigations of how cyber insurance markets are (i) similar and (ii) different across different countries.

Acknowledgments

This research was supported by the Swedish Civil Contingencies Agency, MSB, agreement no. 2015-6986. The author would like to thank all the company representatives that agreed to be interviewed, and Dr Niclas Petersson of Research Institutes of Sweden and Staffan Moberg of Insurance Sweden for their support.

REFERENCES

Akerlof GA. The market for 'lemons': quality uncertainty and the market mechanism. Quarterly Journal of Economics 1970;84(3):488–500. http://www.jstor.org/stable/1879431. Insurance is discussed on pp. 492–494.

Anderson R, Moore T. The economics of information security. Science 2006;314(5799):610–13. http://dx.doi.org/10.1126/science.1130992.

Bandyopadhyay T, Mookerjee VS, Rao RC. Why IT managers don't go for cyber-insurance products. Commun ACM 2009;52(11):68–73. http://dx.doi.org/10.1145/1592761.1592780.

Biener C, Eling M, Wirfs JH. Insurability of cyber risk: an empirical analysis. Geneva Pap Risk Insur Issues Pract 2015;40(1):131–58. http://dx.doi.org/10.1057/gpp.2014.19.

Bolot J, Lelarge M. Cyber insurance as an incentive for internet security, in Managing information risk and the economics of security, Springer, pp. 269–290, 2009. http://dx.doi.org/10.1007/978-0-387-09762-6_13.

Böhme R, Kataria G. Models and measures for correlation in cyber-insurance, in Workshop on Economics of Information Security – WEIS, 2006.

Böhme R, Schwartz G. Modeling cyber-insurance: towards a unifying framework, in Workshop on Economics of Information Security – WEIS, 2010.

Cabinet Office, Cyber insurance market: joint government and industry statement; 2014. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/371036/Cyber_Insurance_Joint_Statement_5_November_2014.pdf. [Accessed 9 January 2017].

Casalicchio E, Menascé DA, Aldhalaan A. 2013, Autonomic resource provisioning in cloud systems with availability goals, in "Proceedings of the 2013 ACM Cloud and Autonomic Computing Conference, ACM. http://dx.doi.org/10.1145/2494621.2494623.

Choudhry U. Der Cyber-Versicherungsmarkt in Deutschland: Eine Einführung, Springer-Verlag; 2014. Available from: http://dx.doi.org/10.1007/978-3-658-07098-4.

Durkee D. Why cloud computing will never be free. Queue 2010;8(4):20. http://dx.doi.org/10.1145/1755884.1772130.

Edwards B, Hofmeyr S, Forrest S. Hype and heavy tails: a closer look at data breaches, in The Workshop on the Economics of Information Security (WEIS), 2015.

Eling M, Schnell W. Ten key questions on cyber risk and cyber risk insurance, Technical report, The Geneva Association (the International Association for the Study of Insurance Economics). Edited by Fabian Sommerrock; 2016a. Available from: https://www.genevaassociation.org/media/954708/cyber-risk-10-key-questions.pdf.

Eling M, Schnell W. What do we know about cyber risk and cyber risk insurance? J Risk Financ 2016b;17(5):474–91. http://dx.doi.org/10.1108/JRF-09-2016-0122.

ENISA, Incentives and barriers of the cyber insurance market in Europe, Technical report, European Union Agency for Network and Information Security; 2012. Available from: https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe.

ENISA, Cyber insurance: recent advances, good practices and challenges, Technical report, European Union Agency for Network and Information Security; 2016. Available from: http://dx.doi.org/10.2824/065381.

European Commission, The Digital Economy & Society Index (DESI); 2017. Available from: https://ec.europa.eu/digital-single-market/en/desi. [Accessed 3 March 2017].

Franke U, Buschle M. Experimental evidence on decision-making in availability service level agreements. IEEE T Netw Serv Manage 2016;13(1):58–70. http://dx.doi.org/10.1109/TNSM.2015.2510080.

Franke U, Holm H, König J. The distribution of time to recovery of enterprise IT services. IEEE T Reliab 2014;63(4):858–67. http://dx.doi.org/10.1109/TR.2014.2336051.

Gray J. A census of tandem system availability between 1985 and 1990. IEEE T Reliab 1990;39(4):409–18. http://dx.doi.org/10.1109/24.58719.
Herath H, Herath T. Copula-based actuarial model for pricing cyber-insurance policies. Ins Markets & Comps: Analyses & Actuar Comp 2011;2(1):7–20.
Hillson D. Extending the risk process to manage opportunities. Int J Project Manage 2002;20(3):235–40. http://dx.doi.org/10.1016/S0263-7863(01)00074-6.
IBM Global Services. 1998, Improving systems availability, Technical report, IBM Global Services.
ITU. Measuring the information society report 2014. Geneva, Switzerland: International Telecommunication Union; 2014.
Kieninger A, Straeten D, Kimbrough SO, Schmitz B, Satzger G. Leveraging service incident analytics to determine cost-optimal service offers, in 11th International Conference on Wirtschaftsinformatik, pp. 1015–1029, 2013.
Knapp ED, Langill JT. Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems. 2nd ed. MA, USA: Syngress Publishing; 2014.
Liao H-J, Lin C-HR, Lin Y-C, Tung K-Y. Intrusion detection system: a comprehensive review. J Netw Comput Appl 2013;36(1):16–24. http://dx.doi.org/10.1016/j.jnca.2012.09.004.
OECD, Cyber risk insurance; 2016. Available from: http://www.oecd.org/finance/insurance/cyber-risk-insurance.htm. [Accessed 9 January 2017].
Pal R, Golubchik L. Analyzing self-defense investments in internet security under cyber-insurance coverage, in Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on, IEEE, pp. 339–347, 2010. http://dx.doi.org/10.1109/ICDCS.2010.79.
Pertet S, Narasimhan P. Causes of failure in web applications, Technical report, Parallel Data Laboratory, Carnegie Mellon University, CMU-PDL-05-109, 2005.
Rapoza J. Preventing virtual application downtime, Technical report, Aberdeen Group, 2014.
Shetty N, Schwartz G, Felegyhazi M, Walrand J. Competitive cyber-insurance and internet security, in Economics of information security and privacy, Springer, pp. 229–247, 2010. http://dx.doi.org/10.1007/978-1-4419-6967-5_12.
Sinanaj G, Muntermann J. Assessing corporate reputational damage of data breaches: an empirical analysis, Proceedings of the 26th International Bled eConference pp. 78–89, 2013.
Snow A, Weckman G. What are the chances an availability SLA will be violated?, in "Networking, 2007. ICN'07. Sixth International Conference on, IEEE, pp. 35–35, 2007. http://dx.doi.org/10.1109/ICN.2007.106.
Snow A, Weckman G, Gupta V. Meeting SLA availability guarantees through engineering margin, in Networks (ICN), 2010 Ninth International Conference on, pp. 331–336, 2010. http://dx.doi.org/10.1109/ICN.2010.59.
Tversky A, Kahneman D. Judgment under uncertainty: heuristics and biases, in Utility, probability, and human decision making, Springer, pp. 141–162, 1975.
Varian HR. Microeconomic analysis. 3rd ed. New York: W.W. Norton & Company, Inc.; 1992 Insurance is discussed on pp. 180–181 and 455–457.
Virvilis N, Gritzalis D. The big four-what we did wrong in advanced persistent threat detection?, in "Availability, Reliability and Security (ARES), 2013 Eighth International Conference on, IEEE, pp. 248–254, 2013. http://dx.doi.org/10.1109/ARES.2013.32.
Wells A, Jones SK. Growth in cyber coverage expected as underwriting evolves, Insurance Journal 2016. Available from: http://www.insurancejournal.com/magazines/features/2016/04/04/403439.htm. [Accessed 9 January 2017].
Wheeler JA, Akshay L, Proctor PE. Understanding when and how to use cyberinsurance effectively, Technical report, Gartner, Inc. G00274770, 2015.
World Economic Forum, The 10 countries best prepared for the new digital economy; 2016. Available from: https://www.weforum.org/agenda/2016/07/countries-best-prepared-for-the-new-digital-economy/. [Accessed 9 January 2017].

Dr. Ulrik Franke is a senior researcher at the Swedish Institute of Computer Science (RISE SICS). He received his MSc and PhD in 2007 and 2012, respectively, both from the Royal Institute of Technology (KTH) in Stockholm, Sweden. His research interests include cyber security, IT service availability, enterprise architecture, and decision-making. He has recently published in journals such as Computers & Security, IEEE Transactions on Dependable and Secure Computing, and IEEE Transactions on Reliability.