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.

© 2017 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

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
0167-4048/© 2017 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

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

Download English Version:

https://daneshyari.com/en/article/4955474

Download Persian Version:

https://daneshyari.com/article/4955474

Daneshyari.com