Cyber insurance demand, supply, contracts and cases

M. Martin Boyer¹

Published online: 26 August 2020
© The Author(s) 2020

This special issue of *The Geneva Papers on Risk and Insurance—Issues and Practice* on Cyber Insurance is the second in three years (see volume 43 of *The Geneva Papers* published in 2018) to cover the emerging threat of cyber risks to firms, organisations, individuals and society as a whole. The first special issue published only four papers; the current special issue publishes eight. The increase in the number of articles in this special issue reflects the growing popularity of the topic not only amongst academics, but also amongst corporate researchers. The 2020 World Risk and Insurance Economics Conference, which was held virtually, had a session devoted to cyber risk, something that would have been unimaginable five years ago.¹

What is cyber risk? One definition that can be used is any attack using electronic devices that causes damage to an organisation or an individual, such as denial of service or the theft or destruction of data for organisations, individuals or otherwise. Such attacks take the form of malicious codes, malware, trojans, worms and phishing, to name but a few.² Cyber insurance usually covers only direct losses, even though indirect losses can be much larger. Whatever cyber risk is, it is certainly difficult to define precisely.³

The eight papers included in the current special issue are divided according to three classifications. The first three papers examine the potential demand for cyber risk insurance by assessing the potential loss for firms and organisations that fall victim to a cyber event. The next three papers examine the supply side by presenting issues related to how contracts are written and interpreted by the courts, and how the writing and the interpretation of cyber contract clauses could have an impact on other insurance contracts. Lastly, the special issue concludes with two papers that

¹ <https://www.wriec2020.org/>

² Goode et al. (2017), Culnan and Williams (2009) and Rasoulouian et al. (2017) include information breach, which they define as unauthorised access to personal information of a group of individuals, as a source of cyber risk.

³ See the excellent cyber insurance reviews of Eling and Schnell (2016) and Marotta et al. (2017).

✉ M. Martin Boyer
martin.boyer@hec.ca

¹ Power Corporation of Canada Research Chair, Department of Finance, HEC Montréal (Université de Montréal), 3000, chemin de la Côte-Ste-Catherine, Montréal, QC H3T 2A7, Canada

examine how cyber risk applies to two industries: health insurance and information technology.

Before briefly summarising the papers in this issue, it feels appropriate to remind ourselves that the lack of proper data regarding cyber losses remains problematic in analysing the actual risk of cyber incidents, and to infer what the demand and supply of cyber insurance should be. Eling (2018) writes (p. 177):

Not only is the lack of data a major concern for insurance managers and empirical researchers, but the dynamic nature of cyber risk also carries an immense risk of change. It is thus far from clear whether the little historical data we have is indicative of future outcomes.

It was true in 2018 and it is still true today. Marotta et al. (2017) identified data issues (including the evaluation of frequency, estimation of damages and dependencies across risks) as the main research gap in the literature. That is why some of the papers in this issue use small data sets or rely on a more qualitative analysis of the issue.

This special issue's first three papers examine the cost of cyber risk events, whether from a stock market perspective, as in the article by McShane and Nguyen, or through the development of new loss distribution techniques, as in the articles by Palsson, Gudmundsson and Shetty and Poyraz, Canan, McShane, Pinto and Cotter.

The paper chosen to lead this special issue, coauthored by Palsson, Gudmundsson and Shetty, examines the impact of cyber events on organisations using the Advisen cyber loss data feed. This source of data was used previously by Romanosky (2016). They apply a 'random forest' algorithm approach in order to better quantify the risk of critical cyber losses. They conclude that phishing and malicious breach incidents are associated with much higher losses than cases of cyber extortion.

The approach used in McShane and Nguyen's paper is similar to that in the finance literature in that the authors examine the American stock market's reaction to cyberattacks (mostly data breaches) on publicly traded firms. Contrary to the results presented in Rasoulilian et al. (2017), McShane and Nguyen find no significant stock market reaction to cyberattacks, on average, over the 10 years under examination. The story does not end there, however. Over time, McShane and Nguyen find that the market's reaction to cyberattacks changes, with negative and significant reactions in 2011, 2012 and 2013. This suggests that cyberattacks and cyberattack damages are driven by causes that are outside of any simple frequency-severity model.

The third paper in the first set of papers, by Poyraz, Canan, McShane, Pinto and Cotter, is interested in measuring the monetary impact of large cybersecurity breaches that could lead to the illegal use of personally identifiable information (aka: PII mega data breaches). In the year ending in April 2020, it was reported that 8.5 billion records were compromised in data breaches, of which 80% were theft of customer-related personally identifiable information (PII).⁴ The potential

⁴ www.ibm.com/security/data-breach

for misuse is high. The authors develop an original method to examine the potential loss associated with future breaches.

In the second set of three papers, the reader is drawn into the world of cyber insurance contract wording and the supply of cyber insurance. The contributions of Woods and Weinkle, Wrede, Stegen and Graf von der Schulenburg and Xie, Lee and Eling therefore examine the supply side of cyber insurance, with the first two particularly interested in the wording of contracts.

In their paper, Woods and Weinkle collect data from 56 cyber insurance policies to examine how deliberate cyberattacks on corporations and organisations are viewed with respect to so-called war exclusions in insurance policies (see also Romanosky et al. 2019). We also learn that 'war' is in the eye of the beholder as war exclusions differ by policy type and different market practices, giving rise to ambiguity in payment and the risk of contract non-performance (see Doherty and Schlesinger (1990) and Peter and Ying (forthcoming) for more on this topic) or subperformance (Asmat and Tennyson 2014). Woods and Weinkle conclude that cyber insurance coverage has been converging to a new equilibrium whereby losses due to war, in its traditional sense, are still excluded, but losses due to terrorism are not.

Wrede, Stegen and Graf von der Schulenburg also examine whether cyber insurance is covered in traditional insurance policies but focus exclusively on the German market. Their focus is on whether there is any 'silent coverage' of cyber losses embedded in other insurance contracts. This is important given the difficulty of defining what cyber risks are and, perhaps more importantly, how much reserve capital should be put aside to cover cyber risk incidents (Eling and Schnell 2016). They find that there is indeed some silent coverage of cyber-related losses in the great majority of the contracts they examine, such as business income insurance, liability insurance, fidelity insurance and D&O insurance. They conclude that the importance of silent coverage is such that cyber risk is becoming systemic.

In the paper by Xie, Lee and Eling, we remain with the supply side of cyber insurance, but we learn more about what motivates a property and casualty insurer to start offering cyber risk protection as a standalone (or a packaged) product. Making use of the National Association of Insurance Commissioners (U.S.) supplement on cybersecurity, which is available starting in 2015, the authors are able to use three years of data to study market development of this insurance line in the U.S. (see Pooser et al. (2018) for an earlier assessment). They find that, despite the absence of solid actuarial models, cyber risk insurance is extremely profitable, with industry loss ratios below 50% and more than half the insurers paying no claim in any given year. With an average loss ratio of 50% and a median paid claim ratio of 0, the authors rightly conclude that this is a very volatile line, making it suitable, perhaps, for services by reinsurers.

The last two papers in this special issue consist of studies that focus on two particular cases where cyber risk and cyber insurance could have an important impact. Leong and Chen examine the particular risk for health insurance companies of an attack against health Internet of Things (IoT) devices using a Chinese data set. Along with the examination of PII by Poyraz et al., Leong and Chen's study on

private health information allows us to cover what Greisinger (2016) calls the two most vulnerable types of data breach.⁵

Lastly, Franke develops a questionnaire that can be used to measure the risk perception of risk managers in large corporations when it comes to IT service outages. The author presents three industry cases in detail: transportation, food and government services. IT service outages are a particular case of cyber risk that are not necessarily caused by a malicious act. IT service outages are similar to IT-related supply chain glitches, which Goldstein et al. (2011) attribute to some category of operational risk (see also the references therein). IT-related supply chain glitches cost firms, on average, 0.75% of their market capitalisation in the U.S., whereas Liu et al. (2016) find an abnormal return of −0.61% in Japan. This is not a trivial amount given that Goode et al. (2017) estimate indirect costs of data breaches to be six times the direct cost.

As a final word, there are still many unknowns associated with cyber risk, many of them related to issues dealing with data, but some also from the point of view of modelling the demand for cyber risk insurance using approaches more embedded in economics. Is it a problem of risk aversion? Of ambiguity? Is it a question of trust in the insurance system and in the wording of the insurance contract? Hopefully, the eight papers published in this special issue will provide a springboard for more research on cyber risk and cyber insurance.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Asmat, D.P., and S. Tennyson. 2014. Does the threat of insurer liability for 'bad faith' affect insurance settlements? *Journal of Risk and Insurance* 81 (1): 1–26.
- Culnan, M.J., and C.C. Williams. 2009. How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quarterly* 33 (4): 673–687.
- Doherty, N.A., and H. Schlesinger. 1990. Rational insurance purchasing: Consideration of contract non-performance. *Quarterly Journal of Economics* 105 (1): 243–253.
- Eling, M. 2018. Cyber risk and cyber risk insurance: Status quo and future research. *The Geneva Papers on Risk and Insurance—Issues and Practice* 43: 175–179.
- Eling, M., and W. Schnell. 2016. What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance* 17 (5): 474–491.

⁵ Greisinger (2016) writes (p. 1): 'PII was the most frequently exposed data (28.7% of breaches), followed closely by PHI (27.2% of breaches)'.

- Goldstein, J., A. Chernobai, and M. Benaroch. 2011. An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems* 12 (9): 606–631.
- Goode, S., H. Hoehle, V. Venkatesh, and S.A. Brown. 2017. User compensation as a data breach recovery action: An investigation on the Sony Playstation network breach. *MIS Quarterly* 41: 703–727.
- Greisinger, M. 2016. NetDiligence 2013 cyber liability & data breach insurance claims. <https://www.netdiligence.com/wp-content/uploads/2016/05/CyberClaimsStudy-2013.pdf>.
- Liu, J., S. Sarkar, S. Kumar, and Z. Jin. 2016. An analysis of stock market impact from supply chain disruptions in Japan. *International Journal of Productivity and Performance Management* 67 (1): 192–206.
- Marotta, A., F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin. 2017. Cyber-insurance survey. *Computer Science Review* 24 (2017): 35–61.
- Peter, R. and J. Ying. Do you trust your insurer? Ambiguity about contract nonperformance and optimal insurance demand. *Journal of Economic Behavior and Organization* (forthcoming).
- Pooser, D.M., M.J. Browne, and O. Arkhangelska. 2018. Growth in the perception of cyber risk: Evidence from U.S. P&C insurers. *The Geneva Papers on Risk and Insurance—Issues and Practice* 43: 208–223.
- Rasoulilian, S., Y. Grégoire, R. Legoux, and S. Sénécal. 2017. Service crisis recovery and firm performance: Insights from information breach announcements. *Journal of the Academy of Marketing Science* 45: 789–806.
- Romanosky, S. 2016. Examining the cost and causes of cyber incidents. *Journal of Cybersecurity* 2 (2): 121–135.
- Romanosky, S., A. Kuehn, L. Ablon, and T. Jones. 2019. Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity* 5 (1): 1–19.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

About the author

Professor M. Martin Boyer, Ph.D., holds the Power Corporation of Canada Research Chair in the Department of Finance at HEC Montréal (Université de Montréal). He graduated with a Ph.D. from the Wharton School of the University Pennsylvania and was a visiting scholar at the University of British Columbia, the University of New South Wales, Cornell University and the Rotman School of the University of Toronto. Having published over 70 articles in scientific and professional journals, or as book chapters, Professor Boyer was Acting President of the Northern Finance Association in 2006 and President of the American Risk and Insurance Association in 2018–2019.