The Geneva Papers on Risk and Insurance - Issues and Practice (2023) 48:267–274
https://doi.org/10.1057/s41288-023-00294-w

EDITORIAL

New advances on cyber risk and cyber insurance

Martin Boyer[1] · **Martin Eling**[2]

This is the third special issue of *The Geneva Papers on Risk and Insurance—Issues and Practice* devoted to cyber risk and cyber insurance (previous issues were published in April 2018 and October 2020). Interest in the topic of cyber risk and cyber risk insurance has been increasing over the last years, both in industry and academia. We document a steady growth of academic research on cyber risk and cyber risk insurance (see Fig. 1 in "Appendix 1"), not only in computer science but also increasingly in business and economics (see Fig. 2 in "Appendix 2"). There have also been top publications in finance, economics and management journals focussing on market reactions to cyber risk events (Kamiya et al. 2021; Foerderer and Schuetz 2022; Florackis et al. 2023) and potential systemic risks arising from such events (August et al. 2022; Eisenbach et al. 2022; Crosignani et al. 2023). Yet, insurance is not a major component of this research.

With this special issue, we contribute to this emerging field of literature with seven articles. Two of them focus on ransomware insurance, while three consider cyber loss modelling. The remaining two consider cyber risk management in general, with one paper looking at the coordination of cybersecurity management and the other at risk mitigation and optimal contract design for cyber insurance As in the two previous special issues, the articles come from different methodological backgrounds and focus on different industries. This editorial summarises the papers included in this special issue and then highlights some potential avenues for future research. The goal of the issue is to not only present new contributions on one of the timeliest topics in research and practice but also to stimulate future research on cyber risk and cyber risk insurance.

The first paper by Tom Baker and Anja Shortland collects interview data from 25 insurance, legal, security and policy professionals to study how insurers address the problems of moral hazard, uncertainty and correlated losses when selling and

✉ Martin Eling
martin.eling@unisg.ch

Martin Boyer
martin.boyer@hec.ca

[1] HEC Montréal (Université de Montréal), Montréal, Canada

[2] University of St. Gallen, St. Gallen, Switzerland

managing insurance for ransomware. They describe the origins of cyber insurance and different generations of ransomware-as-a-service, emphasising the industrialisation of cybercrime that insurers are facing. They also illustrate the evolutionary dynamic of insurance markets and how insurers shape and respond to changes in the risk environment in which they operate. The conceptual foundation of the paper is the 'insurance-as-governance' literature, which demonstrates that insurers often make insurance conditional on ex ante risk reduction or mitigation. One important conclusion of the paper is that although businesses improved their resilience, cybercriminals adapted, so that ransom demands escalated. Insurability is questionable and insurers are pushing governments to better contain criminal threats and cushion catastrophic losses.

The second paper by Anna Cartwright and coauthors. uses semi-structured interviews with 64 cybersecurity professionals to analyse how cyber insurance influences the cost–benefit decision-making process of a ransomware victim. One important question, related to classical moral hazard, is whether organisations with cyber insurance are more likely to pay a ransom than non-insureds. The authors consider this question in a game-theoretical framework that, among other aspects, models the channels through which insurance may influence victim decision-making. The results show that the decision to pay ransom is dependent on the severity of the attack or whether sensitive data are affected. Perceptions of whether victims with insurance are more or less likely to pay ransom are very divided.

The third paper by Paul Klumpes evaluates the efforts by both U.K. government and regulatory authorities to coordinate cybersecurity risk management. After providing an overview of efforts taken over the last decade, their effectiveness is evaluated by studying exposure information (data breaches, investment in computer systems) and performing a content analysis of annual reports for U.K. regulators and insurers. The study finds that although the costs of data breaches have increased, the engagement with cyber as a reporting issue by both cyber insurers and financial regulators has not. The author concludes that there are significant gaps and overlaps in the system of cyber regulatory oversight. For example, there is no single regulatory authority that has responsibility for the supervision of insurance firms.

The article by Gareth W. Peters and coauthors. addresses the insurability of cyber risk by enhancing the standard statistical approaches to assessment of insurability and potential mispricing, especially with respect to model risk. The authors use the *Advisen cyber loss* dataset and various robust estimators for key model parameter estimates to show the large quantity of model risk, e.g. on tail index estimation for heavy-tailed loss models or on dependence analysis. The paper's results complement existing studies on the insurability of cyber losses.

Using a more general setting, Daniel Zängerle and Dirk Schierek introduce the ÖffSchOR operational risk database, which includes cyber risk events. In addition to introducing a new database, the paper makes a methodological contribution by using copula theory (see also the paper by Zeller and Scherer in this issue) to help us cope with data scarcity. Copula theory uses the marginal distribution of an event rather than the entire distribution of the same event. This allows the modelling of non-linear dependencies between types of risk or across time, assuming risk distributions evolve dynamically through time. Building on Eling and Wirfs (2019) and

Eling (2020), the authors show that cyber risks are different from operational risks in general. The one important takeaway for modelling purposes is that cyber risk seems less heavy tailed than first thought.

The paper by Bennet Simon von Skarczinski Mathias Raschke and FrankTeuteberg examines the distribution of cyber risk, using a survey of 5000 German organisations (see also von Skarczinski et al. 2022). The goal of the survey was to examine the security measures adopted by organisations that face cyberattacks, to map the vectors through which cyberattacks occur, and to ascertain the organisations' reaction to such attacks, including reporting (or not) to the police. The results suggest that the most appropriate statistical approach to model cyber risk would be to apply extreme value theory to losses, especially when it comes to tail behaviour.

The special issue concludes with the paper by Gabriela Zeller and Matthias Scherer. The article, more technical than the others in this special issue, addresses the important point of risk mitigation and investment in prevention by policyholders. As the authors write in the conclusion, "There is mutual benefit (for all stakeholders) in the combination of risk transfer and risk reduction measures, leading to the (prospective) ubiquitous offering of pre-incident and post-incident services". No one in the cyber risk and insurance industry could argue the opposite.

As we see the incidence of cyber risk changing over time, the modelling of it must also change. One potential area of future research will be modelling how organisations purchase protection against the direct losses associated with cyber events, while at the same time knowing that the impact of such events on their stock price (through a loss of consumer confidence, say) is much greater than what insurers are willing to cover. In other words, the background reputational risk associated with cyber events may dwarf the direct losses that organisations are able or willing to insure. The modelling of this background risk (whether in a multiplicative or additive way) will become more and more important as cyber risk becomes more integrated with other types of operational, financial or market risks.

It seems that cyber risk is a major concern for organisations.[1] It has become clear that cyber threats, data breaches, IT outages and other cyber risk events cannot be prevented by technical means alone (Solms 2000; Liao et al. 2013; Knapp and Langill 2014; Falco et al. 2019). That is why the financial risk management of cyber losses, and particularly cyber insurance, has become a needed complementary tool for informational assets (Biener et al. 2015).

The idea of seeking protection against ransomware[2] raises interesting public policy questions that have been examined in the context of the kidnapping of company executives. The general structure used in many kidnapping settings is that of a *war-of-attrition* game between a criminal asking for a ransom and the victim, in which the information is incomplete. The presence of an insurer (or a third party

[1] For the specific case of the U.S. insurance and banking industries, see Gatzert and Schubert (2022) and Pooser et al. (2018). Also see Allianz (2022) for a global survey of 2650 risk managers.

[2] Note that ransomware attacks are dwarfed by losses due to data breaches, such as at Target in December 2013, Sony in May 2011 and Equifax in 2017, which resulted in direct losses of USD 200 million, USD 171 million and USD 90 million, respectively (Solove and Hartzog 2021; Goode et al. 2017). Eling and Wirfs (2019) tell us that data breaches account for one quarter of all cyber events.

that increases the chance that the ransom is paid) drastically changes the structure of the game and the strategic interactions.[3] The presence of a cyber insurer is conditional on the potential victim choosing to be insured. In that sense, buying insurance is an endogenous decision, and so is the level of protection. The purchase of insurance provides a signal to cyber criminals that the potential victim is more likely to pay the ransom. As a result, having insurance (and making it known) changes the players' beliefs.

Another way that the presence of an insurance company can change the war-of-attrition game is by changing the belief that a ransom will be paid by increasing the likelihood that ransoms will never be paid. How can an organisation commit to not paying a ransom? Of course, committing credibly to not paying a ransom is difficult unless it is a repeated game. Nonetheless, a well-designed insurance contract can help mitigate the likelihood that an organisation falls victim to a ransomware attack by giving protection for business interruption losses associated with the attack, but never for ransom payment. Whether such a contract would reduce the incidence of ransomware attacks and be implementable from a public policy point of view could be a topic of future research.

With respect to the modelling of cyber risk, regarding both the frequency and severity of events, researchers are (unfortunately) likely to gain access to databases that will be increasingly populated with such events. There will come a time where the databases that we are currently using will become outdated with respect to the dynamics and the mechanisms through which cyber events are revealed to policyholders and their insurers. The time series property of cyber risk and insurance citations in Google Scholar (see "Appendix 1") is a delayed measure of the interest among the business community. There were already slightly over 40 mentions of 'Cyber Risk' outside of Google Scholar in 2000, according to Google. In 2021, that number had increased fivefold. In addition, many more insurers are willing to underwrite cyber risk today than 20 years ago.

The papers in this special issue also raise questions on the potential role of coordination in developing databases and risk mitigation tools that could be profitable, not only to the entire cyber insurance industry but even more importantly to organisations that may fall prey to cyber risk events. As some cyber events include attacks by cyber criminals, whether individuals, criminal organisations or terrorist organisations (or even hostile countries preparing for a cyber war), there is necessarily a role for governments and governmental organisations. The misfortune of Colonial Pipeline, which caused gas shortages in much of the eastern seaboard of the U.S. in May 2021, shows that there are systemically important organisations that could benefit from a more systematic approach to cyber risk. Whether there is an appetite for policymakers to venture into this arena is still very much unclear. What is certain, however, is that the potential for large correlated losses in cyber risk requires coordination far beyond the simple

[3] For instance, in May 2021 Colonial Pipeline fell victim to a ransomware attack whereby a computer virus caused firm operations to cease until the company paid 75 bitcoin in ransom—the equivalent then of USD 4.4 million—for which the firm sought reimbursement from its cyber insurer (Menn and Kelly 2021). In addition, Banham (2021) reports that other ransomware attacks in early 2021 cost USD 40 million to CNA Financial, an insurer, USD 11 million to JB3, a meat supplier, and USD 4.4 million to Brenntaj, a chemical company based in Germany.

diversifiable policyholder–insurer relationship, to the national insurance industry, and perhaps even across political boundaries, as viruses, worms and Trojan horses do not necessarily have a clear and definite political agenda.

We thank all the authors and referees and feel privileged to benefit from their research and the feedback for improvement. We hope you enjoy reading the articles as much as we have enjoyed editing this special issue of *The Geneva Papers on Risk and Insurance—Issues and Practice*.

Appendix 1: Google Scholar citations

See Table 1 and Fig. 1.

Table 1 Google Scholar citations as of 1 February 2023

	Cyber risk	Cyber insurance
2000	10	6
2001	22	13
2002	19	9
2003	39	32
2004	42	23
2005	68	51
2006	74	54
2007	86	36
2008	94	41
2009	100	59
2010	135	67
2011	181	68
2012	210	82
2013	329	134
2014	509	189
2015	769	301
2016	1100	403
2017	1390	503
2018	1790	665
2019	2120	634
2020	2770	832
2021	3460	903
2022	3500	889

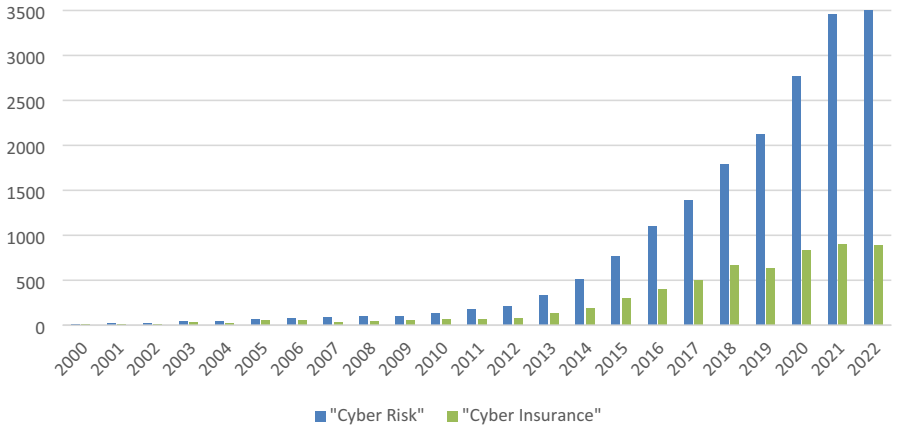

Fig. 1 Google Scholar citations as of 1 February 2023

Appendix 2: Visualisation treemap for 'cyber risk' and 'cyber insurance'

See Figs. 2 and 3.

Fig. 2 Visualisation treemap for 663 Web of Science hits on 'cyber risk' (1 February 2023)

Fig. 3 Visualisation treemap for 226 Web of Science hits on 'cyber insurance' (1 February 2023)

References

Allianz. 2022. *Allianz risk barometer 2022*. Allianz. https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html. Accessed 16 Feb 2023.

August, T., D. Dao, and M.F. Niculescu. 2022. Economics of Ransomware: Risk interdependence and large-scale attacks. *Management Science* 68 (12): 8979–9002.

Banham, R. 2021. Cyber insurance collaboration. *Risk Management* 68 (9): 26–29.

Biener, C., M. Eling, and J. Wirfs (2015). Insurability of Cyber Risk: An Empirical Analysis. Geneva Papers on Risk and Insurance: *Issues and Practice* 40: 131–158. https://doi.org/10.1057/gpp.2014.19

Crosignani, M., M. Macchiavelli, and A.F. Silva. 2023. Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics* 147 (2): 432–448.

Eling, M., and J. Wirfs. 2019. What are the actual costs of cyber risk events? *European Journal of Operational Research* 272 (3): 1109–1119.

Eling, M. (2020). Cyber risk research in business and actuarial science. *European Actuarial Journal,* 10(2): 303–333.

Eisenbach, T.M., A. Kovner, and M.J. Lee. 2022. Cyber risk and the US financial system: A pre-mortem analysis. *Journal of Financial Economics* 145 (3): 802–826.

Falco, G., et al. 2019. Cyber risk research impeded by disciplinary barriers. *Science* 366 (6469): 1066–1069.

Foerderer, J., and S.W. Schuetz. 2022. Data breach announcements and stock market reactions: A matter of timing? *Management Science* 68 (10): 7298–7322.

Florackis, C., C. Louca, R. Michaely, and M. Weber. 2023. Cybersecurity risk. *The Review of Financial Studies* 36 (1): 351–407.

Gatzert, N., and M. Schubert. 2022. Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance* 89 (3): 725–763.

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 (3): 703–727.

Kamiya, S., J.K. Kang, J. Kim, A. Milidonis, and R.M. Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139 (3): 719–749.

Knapp, E.D., and J. Langill. 2014. *Industrial network security: Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems*. Oxford: Syngress.

Liao, H.J., C.H.R. Lin, Y.C. Lin, and K.Y. Tung. 2013. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications* 36 (1): 16–24.

Menn, J., and S. Kelly. 2021. Colonial pipeline slowly restarts as southeast U.S. scrambles for fuel. www.reuters.com/business/energy/colonial-pipeline-has-cyber-insurance-policy-sources-2021-05-13/. Accessed 16 Feb 2023.

Pooser, D.M., M.J. Browne, and O. Arkhangelska. 2018. Growth in the perception of cyber risk: Evidence from US P&C insurers. *The Geneva Papers on Risk and Insurance— Issues and Practice* 43: 208–223.

Solms, B.V. 2000. Information security—The third wave? *Computers and Security* 19 (7): 615.

von Skarczinski, B.S., A. Dreißigacker, and F. Teuteberg. 2022. Toward enhancing the information base on costs of cyber incidents: Implications from literature and a large-scale survey conducted in Germany. *Organizational Cybersecurity Journal*. https://doi.org/10.1108/OCJ-08-2021-0020.

Solove, D.J., and W. Hartzog. 2021. *Breached!: Why data security law fails and how to improve it*. Oxford: Oxford University Press.