The Geneva Papers, **2018**, **43**, (175–179)

www.genevaassociation.org

Editorial

Cyber Risk and Cyber Risk Insurance: Status Quo and Future Research

Martin Eling
Institute of Insurance Economics, University of St. Gallen, Girtannerstr. 6, St. Gallen 9010, Switzerland.
E-mail: martin.eling@unisg.ch

The Geneva Papers (2018) **43,** 175–179. https://doi.org/10.1057/s41288-018-0083-6;
published online 15 March 2018

The *Geneva Papers on Risk and Insurance—Issues and Practice* has a long tradition of publishing special issues on emerging topics in the insurance industry. Recent topics include extreme events and climate risk, microinsurance and longevity. There have also been several special issues devoted to the fields of pensions, health, and regulation. Currently, the growing economic and social importance of cyber risk is seen in the media on a daily basis. In addition, businesses are facing cyber risks that can lead to considerable corporate losses. Although first studies on cyber risk have been published, there is still an enormous lack of information on its empirical properties.

The goal of this special issue is not only to present some interesting articles on one of the timeliest topics in insurance research and practice but also to stimulate future research on cyber risk and cyber risk insurance. This editorial summarises the papers included in this special issue and highlights some of the potential avenues for future research.

It is not surprising that the number of submissions and accepted papers for this special issue was low compared to other special issues of *The Geneva Papers*. Although cyber risk—or information security in general—is a classic topic in IT research, only relatively few researchers are currently analysing this topic from a business or an economics perspective. The few articles that do exist come from very different methodological backgrounds and focus on different industries.

The four articles presented in this special issue reflect the current state of research by covering numerous disciplines and industries. Three articles look at cyber risk management in general and one considers cyber risk insurance in detail. One of the four articles focuses on banking (Ashby *et al.*, 2018) and one on insurance (Pooser *et al.*, 2018); the remaining two have no specific industry focus (Shetty *et al.*, 2018; de Smidt and Botzen, 2018). On the methodological side, the articles range from semi-structured interviews (Ashby *et al.*, 2018) to a smaller empirical analysis with z-tests (de Smidt and Botzen, 2018), from a broader empirical analysis with probit regressions (Pooser *et al.*, 2018) to the presentation of a conceptual framework for cyber risk scoring and mitigation (Shetty *et al.*, 2018).

The first paper in this special issue is "Emerging IT risks: Insights from German Banking" by Ashby *et al.* (2018). The authors collect interview data from 10 German banks participating in the 2014 ECB stress test to analyse how banks manage IT risks. The authors identify a gap between Enterprise Risk Management (ERM) as a general approach to risks threatening firms' objectives on the one hand and Cyber Risk Management on the other hand. The results suggest that Enterprise Risk Management needs to better

understand and describe emerging IT risks. The article also discusses who needs to be involved in the management of emerging risks from IT innovations.

The second paper, "Growth in the Perception of Cyber Risk: Evidence from U.S. P&C Insurers" by Pooser *et al.* (2018), considers 10-K reports for 50 publicly traded U.S. property-casualty (P&C) insurers to examine trends in cyber risk identification and cyber risk perception from 2006 to 2015. While only 25 per cent of all firms identified cyber risk as a material risk factor in 2006, almost 100 per cent did so by 2013. The authors compare "early adopters" of cyber risk identification to "late adopters" and find that the former tend to be smaller, more leveraged and faster growing. Early identifiers were thus more sensitive to cyber risk because of their size and firm risk (higher leverage and growth rate). One particularly useful element of this paper that also links very well with the preceding analysis by Ashby *et al.* (2018) is the analysis of similarities and differences between Enterprise Risk Management and Cyber Risk Management.

The third paper, "Reducing Informational Disadvantages to Improve Cyber Risk Management" by Shetty *et al.* (2018), analyses the role of insurance in cyber risk management. The use of insurance should not only include the transfer of cyber risk but also provide incentives for insured enterprises to invest in cyber self-protection. Research indicates that asymmetric information, correlated loss, and interdependent security issues significantly reduce insurability, especially if insurers cannot continuously monitor the cyber security efforts of the insured enterprises. In response to this problem, this manuscript proposes a cyber risk scoring and mitigation tool that estimates cyberattack probabilities; the premise is to directly monitor and score cyber risk based on assets at risk and software vulnerabilities that are continuously updated. The tool produces risk scores that encourage organisations to choose mitigation policies that can reduce insurance premiums.

The final article, "Perceptions of Corporate Cyber Risks and Insurance Decision-Making" by de Smidt and Botzen (2018), analyses professional decision makers' perceptions of cyber risks with a special emphasis on behavioural factors. The authors document that the availability heuristic, threshold level of concern, degree of worry and trust in one's own organisational capabilities all have a significant influence on the perceived probability and impact of cyberattacks. They also discuss one potential explanation for the low demand for cyber risk insurance: the probability of a successful cyberattack tends to be overestimated, whereas its financial impact is underestimated. The paper includes an overview of hypotheses about perceptions of cyber risk that could form a fruitful basis for future research. De Smidt and Botzen (2018) also note that the development of a predictive model for assessing total financial impacts and the likelihood of a cyberattack on specific organisations may be useful. This point connects to the preceding paper with the scoring approach developed by Shetty *et al.* (2018) that might provide a starting point for more future development in this predictive direction.

Understanding the properties and nature of cyber risk is vital for the provision of cyber insurance and the estimation of risk capital. The papers in this special issue could make a contribution to this understanding by offering insights for cyber risk management and the insurability of cyber risks. The findings are relevant for risk managers, policymakers and regulators who need to develop sound policies for the treatment of this new and dynamic risk category. For academic readers, the special issue presents mainly empirical results,

which reach beyond the first empirical papers for this novel application area of risk management.

We are not only aware of the limitations of empirical research, but we also note the opportunities for future research. On the most general level, insurance research can be categorised according to insurance mathematics, management and economics, and we use these categories to organise the following discussion on future research opportunities.

From the *mathematical/actuarial perspective,* it is striking that for this new and dynamic type of risk both the frequency and severity of potential losses from cyber events are unclear. 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. Cyber loss data are limited and the risk itself is very dynamic. It is therefore not surprising that there is no set of models that sufficiently captures the properties of this new class of risk. Developing cyber risk models would not only help companies to improve their cyber risk management but would also foster the emergence of an insurance market for cyber risk. For insurance purposes, the data on losses related to cyber risks are not yet sufficient to calculate premiums, risk capital, or reserves. In such cases, predictive models and scenario analyses might also provide useful starting points.

Two problems that are often discussed are (i) what extreme cyber scenarios might look like and (ii) what the dependence structure is between cyber losses. Many experts fear that in some cases cyber losses are heavy-tailed and highly correlated, for example because all companies use the same software. If cyber losses are heavy-tailed, there is the question of the extent to which the diversification of cyber risks is possible or whether a non-diversification trap exists (as documented for other catastrophic risks). We also note that the focus of databases today is on data breaches and U.S. data; information for other types of risk or other countries is scarce. This situation may improve in the coming years with the introduction of the new data protection rules in the European Union, which also include mandatory notification requirements for some cyber incidents. These notification requirements will not only generate interesting data for actuaries and researchers but could also encourage decision makers in firms to invest in cyber self-protection and cyber insurance.

The global cyber insurance business is therefore expected to grow in the coming years, partly as a result of the new data protection rules. When it comes to the *management* or *business perspective*, however, it is striking that the cyber insurance market is still very small and far removed from what many experts expected. The research presented in this special issue illustrates that the misperceptions of cyber risk might be one explanation. One interesting behavioural element in this context is the latent fatalism many people express when discussing cyber risk (‘it will not happen to me’; ‘my data are not interesting enough’). Identifying the drivers of this perception and increasing awareness (research on de-biasing) might help to increase the demand for cyber risk insurance. The effectiveness of communication strategies to improve awareness and perceptions of cyber risks has also been questioned. Furthermore, it might be interesting to compare risk perception and risk aversion in the field of cyber risk insurance with other types of insurances or other types of risks (e.g., from the capital market).

This special issue illustrates the need to close the gap between Enterprise Risk Management, which has seen enormous developments over the last decade or two, and

Cyber Risk Management, which is still in its infancy in many organisations. Companies need to invest in people, processes and systems; in particular, there is a need for employees who can help to bridge the gap between business managers and IT specialists. Given the current insurability limitations, cyber insurance product design and innovative ways to transfer cyber risks (including alternative risk transfer (ART) instruments such as cat bonds) might be interesting fields for business research. In the future, new and innovative business models that reduce and transfer cyber risks could arise, for example via the blockchain. When it comes to cyber risk management, the lack of data on the cost of cyber risks makes it difficult to assess the right level of investment in self-protective measures and insurance. Another important aspect from the business perspective is the existence of "silent covers," which are cyber covers in traditional policies. While in new policies the cyber risks will be named and either included or excluded, it is not clear how far cyber covers are given in older policies, for example, in the field of business interruption or directors and officers (D&O). Identifying and measuring such risks from a regulatory point of view poses an interesting, unexplored question.

Finally, regarding the *economics perspective,* the link between insurance economics and cyber risk needs to be explored more thoroughly to better understand the economic foundation of cybersecurity investments. What is the optimal mix of prevention, insurance and other risk management activities from an economic point of view? What risk characteristics (e.g. correlation) determine whether insurance or self-protection is economically a more efficient risk management tool for cyber risk? In this context, one important open discussion is the extent to which minimum standards for cyber self-protection should be introduced to support the development of cyber insurance and to enhance economic welfare. The latter discussion is also very relevant in light of the inherent incentive problems in cyber security investments: for both individual users and companies, the interconnectedness and dependencies of their IT systems mean that they remain vulnerable even if they invest substantially in cyber risk self-protective measures. Investments in cyber security thus exhibit a 'public good' character with positive externalities. In such a situation, the coordination problem that arises is that the utility of cyber security investment by one firm depends on the investment in cybersecurity by all other firms. These incentive problems are a direct consequence of cyberspace as a dense and complex network of information systems and users. What strategies can be used to resolve this inherent incentive problem in cyber security investments? When it comes to government intervention, information sharing and pooling of insurance in public or private partnerships are often discussed.

Another critical aspect that also needs consideration in the macroeconomic context is the extent to which an extensive writing of cyber risk insurance could give rise to systemic risk, especially if IT systems are increasingly connected. The systemic risk might also depend on the type of cyber risk covered in cyber insurance policies. Some risks, such as viruses or phishing, might show a high correlation between different firms, while for other types of risks such as insider attacks or hardware failures the correlation between different firms might be rather low. Risk pooling is clearly expected to work better in the latter case, while the former case of high correlation might show undesirable accumulation risks at least in extreme scenarios. We also note that insurance companies are affected by cyber risk in two distinct ways: first, in their underwriting when new cyber insurance policies are

sold; but second, in their critical consideration of the operational cyber risk stemming from their own IT systems in an industry that is built on trust, reputation and sensible data.

In considering this special issue, it is striking that all contributions are empirical and that there is no established theoretical framework to analyse cyber risk. Obviously, one might ask whether a separate theoretical framework for cyber risk is needed or whether cyber risk is just another new type of risk that should be analysed using classical models. The above discussion, however, illustrates the special nature and complex features of cyber risk (e.g. asymmetric information, potential correlations, 'public good' character) so that distinct papers that analyse cyber risk from a theoretical point of view might be needed.

In conclusion, I feel privileged to benefit from the research of the contributing authors. I hope you will enjoy reading their articles as much as I have enjoyed editing this special issue of The *Geneva Papers on Risk and Insurance—Issues and Practice*.