Cyber risk management: a new challenge for actuarial mathematics.

Maria Francesca Carfora, Fabio Martinelli, Francesco Mercaldo, Albina Orlando and Artsiom Yautsiukhin

Abstract A specific kind of insurance that is emerging within the domain of cyber-systems is that of cyber-insurance. Cyber-insurance is the transfer of financial risk associated with network and computer incidents to a third party. Insurance companies are increasingly offering such policies, in particular in the USA, but also in Europe. The emerging trends in cyber insurance raise a number of unique challenges and force actuaries to reconsider how to think about underwriting, pricing and aggregation risk. Aim of this contribution is to offer a review of the recent literature on cyber risk management in the actuarial field. Moreover, basing on the most significant results in IT domain, we outline possible synergies between the two lines of research.

Keywords: **Risk management**, **Cyber risk**, **Cyber Insurance**

1 Introduction

The Internet evolution is one of the greatest innovations of the twentieth century and has changed lives of individuals and business organizations. As a consequence, cyber risk has emerged as one of the top challenges faced by companies worldwide. Executives and security professionals are accepting that it is not a matter of if but a matter of when their organization will be hit by a cyber-attack. Compa-

Maria Francesca Carfora and Albina Orlando
Istituto per le Applicazioni del calcolo "M. Picone" - Consiglio Nazionale delle Ricerche, Via P. Castellino, 111 Napoli, Italy e-mail: mfcarfora@na.iac.cnr.it, a.orlando@na.iac.cnr.it

Fabio Martinelli, Francesco Mercaldo and Artsiom Yautsiukhin
Istituto di Informatica e Telematica - Consiglio Nazionale delle Ricerche, Via Moruzzi, 1 Pisa, Italy e-mail: fabio.martinelli@iit.cnr.it, francesco.mercaldo@iit.cnr.it, artsiom.yautsiukhin@iit.cnr.it

nies have to include cyber risk in their risk management framework, depicting their risk profile, assessing their risk appetite and looking for corresponding risk transfer solutions.Cyber-security insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, data theft, business interruption and network damage. In general, immense difficulties emerge to insure cyber risk, especially due to a lack of data and modelling approaches, the risk of changes and the accumulation risks. Scientific interest on this topic is growing, but despite the increasing relevance for businesses, at present research on cyber risk is still limited. Many papers can be found in the IT domain, but relatively little research has been done in the actuarial, business and economic literature. Considering that it is expected that cyber crime damage costs to hit 6 trillion annually by 2021[1], it is plausible that there is an increasing demand for methodologies with the aim to quantify the risk of cyber attacks exposure by industrial and public companies: this new scenario calls for bridging the gap between actuarial, economic and IT domain in order to address this increasing demand. Aim of the paper is to outline the peculiarities of cyber insurance and to show the main recent results in actuarial literature. Finally the interdisciplinarity of the topic is stressed togheter with the suggestion to look at the results in IT domain.

2 Peculiarities of cyber insurance

The main issues related to cyber insurance can be summarized as follows[6]:

- *Evolution of information system*: The system of an organisation may easily change and new technologies appear, changing the landscape of cyber risks;
- *Information asimmetry*: There are many obstacles for an insurer to get reliable information about the risk exposure of an insured and it is difficult to know if this exposure will be mantained during the whole period of policy operation;
- *Evolution of attacks*: It is very hard to determine the rate of occurrencies and, as a consequence, the assessment of risk exposure;
- *Interdependence of security*: Security level of an information system may depend on security of others;
- *Impact determination*: Damage for cyber risks is very hard to estimate in advance because of the intangible nature of information assets. Moreover reputation cost, which accounts for a large portion of the whole damage, is very difficult to estimate;
- *Lack of statistical data*: Data lie at the center of any actuarial project, but data are very limited in this field. Companies often do not want to reveal breaches, since they cause secondary damage , e.g. to reputation.

[1] https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

- *Premium estimation*: Unlike traditional insurance policies, however, cybersecurity insurance has no standard scoring systems or actuarial tables for rate making. Moreover geographical similarities and monocolture make the task very hard.

.

2.1 Some recent results in economic and actuarial literature

A very interesting contribution is given in [2] where the authors aim to provide an overview of the main research topics in the emerging fields of cyber risk and cyber risk insurance. The results illustrate the immense difficulties to insure cyber risk and various ways to overcome the insurability limitations are discussed. The authors illustrate where research stands currently and outline directions for the future.

Regarding modelling and pricing cybersecurity risk, in [5] the authors propose a model consisting of three components: epidemic models, loss functions and premium strategies. A simulation approach is proposed to compute the premium for the cybersecurity risk for practical use. [3] develop a cyber-insurance model using the emerging copula methodology. This approach is the first in the information security literature to integrate standard elements of insurance risk, with the robust copula methodology to determine cyber insurance premiums.

As far as it concerns the lack of data, [1] link what has been done in information technology field with the current discussion on goodness of fit, pricing and risk measurement in actuarial domain. They analyze the data breach information taken from "chronology of Data Breaches" provided by the Privacy Rights Clearing house and use multidimensional scaling and goodness-of-fit tests, to analyze the distribution of data breach information. They illustrate the usefulness of their results in two applications on risk measurement and pricing.

3 Information Technology for Cyber Insurance

Considering the cyber nature of the attacks that are targeting cyber physical or network infrastructure, a normal consequence is that the computer science community started to develop methodologies in order to provide defense mechanism to IT systems. A recent paper in computer science literature [6] summarizes the basic knowledge about cyber insurance so far from both market and scientific perspectives. The survey discusses the issues which make this type of insurance unique and show how different technologies are affected by these issues.

As a matter of fact, while computer scientist in last years proposed techniques in order to mitigate cyber attacks, there a is lack of knowledge about the quantification of these attacks in terms of relapse from a money perspective. Cyber-insurance is currently considered just an option for industrial and public companies but it represents the increasingly important way for businesses of all sizes to manage the

threat of cybercrime. However, less than 10% of UK companies actually take out specific protection. Incredibly, cyber-insurance cover has been around 10 years but, it seems, that companies do not have confidence in the types of products or services currently being offered [4]. Among the peculiarities of cyber-insurance there is coverage specification. It is hard to specify what an insured wants to be covered from and an insurer is willing to cover precisely.

For many insurers and brokers, the technicalities of information security and the details of how to deal with a data breach remain a mystery. We think that a good starting point is to determine the costs or expenses the company needs covering and the types of incidents that cyber-insurance wants cover for. Instead of a general insurance able to cover all cyber attacks, considering the peculiarity and the repercussions behind different attacks, we think that each kind of threat can be managed by different insurance policies and we think furthermore that different companies can exhibit a different risk between these kinds of threats. In few words, we are proposing to insurance companies to create ad hoc policies in order to support the real spread of cyber insurance policies. The insurer should gain the trust of the company discussing the possible threats to which the company is exposed to, being able to propose ad-hoc policies for different companies, basing on a preliminary analysis on the current company infrastructure highlighting the vulnerabilities.

We aim to create a virtuous circle between companies that benefit from cyber insurance ad-hoc policies, insurers that will stipulate policies against cyber attacks and computer scientist, that will be able to adopt their proposed methodologies in the real-world.

Acknowledgments

This work has been partially supported by H2020 EU-funded projects NeCS and C3ISP and EIT-Digital Project HII and PRIN “Governing Adaptive and Unplanned Systems of Systems” and the EU project CyberSure 734815.

References

1. M. Eling and N. Loperfido. Data breaches: Goodness of fit, pricing, and risk measurement. *Insurance: Mathematics and Economics*, 75:126–136, 2017.
2. M. Eling and W. Schnell. What we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(4):474–491, 2016.
3. H. S. B. Herath and T. C. Herath. Copula based actuarial model for pricing cyber insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations*, 2(1), 2011.
4. P. Low. Insuring against cyber-attacks. *Computer Fraud & Security*, 2017(4):18–20, 2017.
5. X. Maochao and H. Lei. Cybersecurity insurance: Modelling and pricing. *Society of Actuaries*, 2017.
6. A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin. Cyber-insurance survey. *Computer Science Review*, 2017.