
Efi Tziva,
Professor Faculty of Law,
Department Economic and Commercial Law,
Aristotle University Thessaloniki

1. INTRODUCTION

The cyber insurance is one of the most growing but at the same time one of the most complex sectors of the private insurance. The explanation of this phenomenon is mainly due to the cyber risk which remains an undefined, high, large, an international risk that makes the insurance providers sceptical about its coverage.

Although the cyber insurance has made its appearance the late 1970s¹, even today has still a form of a niche and very specialized insurance market². The main open question about this relatively “new” risk is its coordination with the fight and sometimes with the defense of the persons, of the entities, of the organizations, even of the states against the cyber-attacks, that are becoming more frequent and serious.

The development of the cyber insurance is not the expected one, because many “victims” of cyber-attacks have given much more attention to adopt technical means instead of being insured.

Other reasons for the difficulties in this sector are already mentioned by the scarce up to now literature, such as the absence of the calculation of loses due to cyber-attacks, the cover of small loses, the uncertainty about the cover itself. Even the used terminology does not give the necessary information to people and to entities who seek for the suitable policies.

The whole situation has become much more complex during the last two years of pandemic which have multiplied the applications of IT in every sector of professional and personal life and as a result the cyber risks have reached unexpectable numbers. Beside the numbers the frequency and the variety of the risks in many sectors have made urgent the development of the cyber insurance.

In many sectors such as the financial sector the exposure to the cyber-attacks or incidents is very high, as it is given by a bulletin published by the BIS (Bank of International Settlements)³, that refers to the continuity of the treat because of the pandemic and the efforts of the entities to work together in order to be protected by the cyber risks using, besides other protection measures⁴, the solution of the cyber insurance.

⁴ As it is said protection from harm on any networked computer system can not reach 100%, see R. Majuca/W. Yurcik/J.P.Kesan, The evolution of cyberinsurance.
Also, the EIOPA recently (15.10.2021) has published a report on the cyber-risks and their impact on the insurance industry\(^5\) declaring October as the European cyber security month and calling the insurance groups to insure and prevent cyber risks by offering at the same time the suitable coverage against these risks, which human beings and entities face in the era of Covid-19. In this direction EIOPA gives the necessary means to the insurance companies for the innovation and cooperation to each other to face these new risks and to offer to their clients an effective coverage.

2. THE BASIC LEGAL TERMINOLOGY

Since the cyber insurance constitutes a relatively “new” branch of the insurance market it is necessary to focus on some basic elements and try to clarify the content and the legal meaning of these elements.

First, even the item of “cyber” needs some clarifications. An interesting research in 2016 by Eling and Schnell\(^6\) in more than 209 papers for definitions of cyber risk by an insurance perspective has shown that as far as the item cyber it mainly relates to electronic communication networks and virtual reality. Especially networks are connected to the term cyberspace often used synonymously with the Internet, which means that internet has become the main source of cyber threats of any kind.

Problematic is also the definition of the several threats or attacks on the internet. Some of the main categories (criminal and non-criminal), according to a report of the UNODC (=United Nations Office on Drugs and Crime) with the title “Covid-19: Cyber Threat Analysis (May 2020)” are: phishing e-mails, impersonating an official website from different criminals, spreading malware which can steal credentials of any kind, fake campaigns, disinformation, attacks to banks and government infrastructures e.t.c.

Unfortunately, this is an indicative catalog which every day, especially during the huge spreading of users of Internet and of the social media\(^7\) is increased by the variety and the numbers of the attacks worldwide.

The cyber insurance is the insurance which covers the liability, or the damages created by the cyber risks to persons, entities and organizations, liable or “victims” because of the risks.

3. COVID-19 AND ITS IMPACT ON INSURANCE GENERALLY AND MAINLY ON CYBER INSURANCE

A comment by a VMware cybersecurity strategist, Tom Kellermann\(^8\), declares with emphasis on the connection of Covid-19 to the cyber security: “there is a digitally historic event occurring in the background of this pandemic, and that is there is a cybercrime pandemic that is occurring.”

The pandemic itself and its consequences have transformed the cyber risks in a “nightmare” for people, for the governments, for the entire community. The unbelievable increase of teleworking, education by distance, e-commerce, data interchange, the circulation

\(^{5}\) https://www.eiopa.europa.eu/topics/cyber-risks_en EIOPA
\(^{6}\) See the full text at www.emeraldinsight.com/1526-5943.htm
\(^{8}\) Quoted by Menn (2020) and H.J. Hejace et al. Cyber Security .. see f.n. 5.
of the informations, the whole change of the daily life of millions persons all over the world has given the possibility also to the criminals to take advantage of the situation.

In front of this situation a new horizon has emerged for the so-called cyber insurance, which is called, besides to the necessary technical measures, to develop a sector which, up to now, had a specific and primitive content.

That means, inter alia, that the insurance and reinsurance sector have in front of them a real challenge not only to create profits, but at the same time to distribute, with their one capacities and technical knowledge to the effectiveness of the cyber security.

4. MAIN LEGAL ASPECTS AND PROPOSALS

The enormous increase of the cyber-attacks during the two years of the pandemic have proved the fragility of some systems and the risk for people safety, because of the global transformation of the physical and vital activities to online. As Internet connectivity has increased, the vulnerability of people but at the same time of companies and of other entities has proportionally increased.

It is obvious that the main sectors of the cyber - attacks have to do with data breaches due to the daily use of internet and the lack -sometimes- of the information of the users and of the invention of ransomware. But even the big organizations, hospitals, ministries, public services all over the world have faced serious hacking attacks and they were suffered huge damages of any kind, especially they had to pay “ransoms” to the cyber criminals that reached amazing amounts.

Among the possible means of defense in front of the various cyber - attacks the private insurance could give a solution. Of course, what is also needed is the development of a deeply education of people about the cyber - attacks and the cybersecurity which would be designed by the governments, the businesses, the educational institutions, the technical experts in order to be protected by an existed big threat.

The cyber insurance although the risks are present and serious has not been enough developed and the reasons are not only the difficulties in planning the suitable terms of condition but also the weakness of the entities to buy this kind of insurance due to big losses, they suffered because of Covid-19. This situation has also influenced both insurers and reinsurers to create relevant insurance products and to undertake high value coverage by forming the respective insurance premiums and find the necessary balance between cost and risks.

The sector of private insurance indeed was also a “victim” of pandemic, because it faced a lot of claims especially in the frame of BI (=Business Interruption) policies since many insured companies have closed due to the public health measures against Covid-19 and for this reason they asked to be paid, facing the deny of the insurance companies that the policies have n’t covered effects or certain effects of a pandemic (lockdown measures).

It is important to mention that the UK Supreme Court in a decision The Financial Conduct Authority v Arch Insurance (UK) Ltd & others [2021] UKSC 1 decided in favor for the claimants, saying that, according to the spirit and intent of the relevant provisions of the policies it is clear from the use of the definition of a 'notifiable disease' in most of the relevant clauses that Covid-19 belong to the indicative list of diseases for which all the relevant disease

---

9 See H.J. Hejace et al. Cyber Security . p.10
10 See T. Johansmeyer, in https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem
11 See https://www.supremecourt.uk/cases/docs/uksc-2020-0177-judgment.pdf
© 2022 by Author(s). This is an open-access article distributed under the terms and conditions of the CreativeCommons Attribution-NonCommercial-NoDerivatives International 4.0 License (CC BY-NC-ND 4.0) https://creativecommons.org/licenses/by-nc-nd/4.0/
and hybrid clauses provided cover. This decision has brought an end to legal arguments of six insurers and could have a positive result for other insured to claim successfully in the frame of their similar policies.\footnote{See more details in https://www.fca.org.uk/news/press-releases/supreme-court-judgment-business-interruption-insurance-test-case}

As the situation is critical for insureds and insurers as well, the coverage against the specific “new” cyber risks caused by the Covid-19 and the measures taken all over the world in order to stop the unexpected consequences of this disease, is for the time being, underestimated.

Of course, it is absolutely urgent everyone who suffers from various cyber-attacks to protect the privacy as well as the other rights by using technical means, but also is necessary to try to find a suitable insurance cover that would limit the exposure to such inevitable risks.

Experts of the insurance market have pointed out the difficulties for the improvement of the cyber insurance given the necessary directions but at the same time a very important sector is to form the relative policies according to the needs of the insured. In this direction is useful to distinguish the so called “large risks” according to the Art. 13 (27) of the Dir. 2009/138/EC (Solvency II) because some of these risks refer to attacks against organizations or important service providers which could cost amazing damages. In this category belong also state – sponsored or terrorist attackers whose scope is to provoke damages to national infrastructure and economies with huge and catastrophic loses\footnote{See M. Camillo (2017), Cyber risk and the changing role of insurance, Journal of Cyber Policy, 2:1, p. 56.}

By the other hand the insurers should focus on the different types of policies such as policies suitable for damages of persons or damages of companies, although the typical insurance products (First Party Insurance, Liability Insurance, BI policies, Errors and Omissions insurance) are not considered suitable to cover the damages provoked by cyber-attacks\footnote{See R. Majuca/W. Yurcik/J.P.Kesan, The evolution of cyberinsurance p. 4.}, unless if these traditional policies would include cyber wordings. Also, the insurers should clarify the meaning of the damage that in most of the cases is not physical and of course the meaning of the “accident”, that has also a specific content in the cyberspace. An accident (=event) remains in the frame of insurance law unexpected and unintended\footnote{See Bird’s Modern Insurance Law (2007), p. 240.}, but as far as the “cyber accidents” the insurers must describe precisely their content in order to avoid misunderstandings about the coverage.

Especially regarding the controllers and processors of personal data is quite important to cover their liability according to the Regulation EU 2016/679 (GDPR), Art. 82, by a specific insurance of liability that could cover the compensation paid to any person who has suffered material or non-material damage as a result of any infringement of the Regulation. That means a great responsibility for the insurance industry to regulate this important and new risk, according to the legal and technical requirements in order to give to their insureds the necessary confidence about the coverage.

The protection of the policyholders is generally a very important issue as a part of the legal supervision according to the Directive Solvency II, to the Insurance Distribution Directive (IDD, Dir. EU 2016/97) and to the POG (=Product Oversight and Governance) requirements. These requirements mean that the providers of the insurance must demonstrate the value for the customers of their products and all the providers and distributors must take care of their
customers\(^\text{16}\). This legal obligation means especially in the cyber insurance that the producers and the distributors of the new sophisticated insurance products should be very careful and very clear in describing the covered risk, the damage, the exceptions of the coverage, the rights of the contracting parties.

Finally, an important issue that insurers are called upon to address is the “moral hazard” problem\(^\text{17}\), that means when someone is covered by insurance may intentionally cause the loss or take fewer measures to prevent the losses from occurring e.g. don’t give the necessary attention to phishing-mail. A realistic and effective solution for this problem is the coverage exception (legal or as a general contract term) in the case when the insured don’t take the necessary measures to avoid the risk and the general duty for policyholders to act in good faith and in a spirit of cooperation with their insurers.

5. CONCLUSION

The pandemic, in addition to all the serious human and economic problems it has created around the world, significantly affects to the private insurance. Especially the big size businesses and organizations have to take effective measures in order to keep their continuity through the pandemic, with few resources and less expertise available\(^\text{18}\) and try also to find a suitable insurance program with reasonable costs.

The cyber insurance sector, however, must face, in addition to the risk management, also the serious problems that the pandemic has brought to their finances, as well as the fact that new risks or variants of old ones are constantly being created in the cyberspace.

For an effective function of this sector, the following factors had to be taken into account:

- a) careful design or redesign of suitable insurance products
- b) examination of the unfairness of general contract terms
- c) setting premiums at reasonable levels
- d) information of the insured
- e) necessary and technically justified insurance exemptions
- f) the evasion of conflict of interests e.g. being intermediaries and working at the same time for companies in the field of the security of information systems
- g) taking into account the global nature of the phenomenon the seeking of solutions with the cooperation of insurers, reinsurers and all the others market’s actors
- h) recovering the costs of R&G and achievement of profits for the insurance companies

The new conditions due to the Covid-19 can provide opportunities for large or even small sized insurance companies to operate in this sector\(^\text{19}\). This will benefit not only themselves but also companies and individuals who will share with their insurers the significant financial consequences of these “new” risks.


\(^{17}\) See Eling et al. p.482


\(^{19}\) In cyber insurance some predicting the market could grow to $20 billion or more by 2025, see M. Camilo, Cyber risk and the changing role of insurance, Journal of Cyber Policy, pp 53-63 (59).

\(©\) 2022 by Author(s). This is an open-access article distributed under the terms and conditions of the CreativeCommons Attribution-NonCommercial-NoDerivatives International 4.0 License (CC BY-NC-ND 4.0) https://creativecommons.org/licenses/by-nc-nd/4.0/