This new section of ***eurofenix*** will bring you the most relevant news in the field of insolvency tech and digital assets. To contribute an article to a future edition, please send your proposal to: ***insolvencytech@insol-europe.org*** or the individual Chairs:
Dávid Oršula ***david.orsula@bnt.eu***
José Carles ***j.carles@carlescuesta.es***
Laurent Le Pajolec ***lpa@exco.pl***

Cyber risks, corporate responsibilities and international challenges

LUDOVIC VAN EGROO
Institut d'Etudes Politiques, Lille, France

Cyber risk[1] is increasingly present, with impacts that are not clearly identified, but very real and with potentially heavy consequences for a company's activities.

In the current context, interstate tensions in the cyber space are ever growing and the number of collateral victims – human and industrial – is increasing. As an illustration, the NotPetya malware, which originated from Ukraine and spread around the world, transited via widely used accounting software in Ukraine.

Cyber risks highlight the need to clarify the relationship between the law of war and the law of insurance covering claims and risks.

Potentially very heavy impacts, financially as well as humanely: An act of war?

In 2016, the North Atlantic Treaty Organization (NATO) wrote in article 5 that acts of state-sponsored cyber-attacks are acts of war. The UN characterises such a war as an "attack on computer systems carried out with malicious intent".

The origin and reasons for the attack can also be summed up in the questions who is attacking and why.

"Unfortunately, when you are being attacked in cyber space, the two things you often do not know are exactly who is attacking you and why. It is not that everything can be defined as a cyber-war, it is that we are increasingly seeing war-like tactics used in broader cyber conflicts. This makes defence and the national cyber-defence policy difficult."[2]

On the side of private actors, awareness of the need to cover this risk is real, as is the need to identify the limits and perimeters of coverage. In its annual report for 2020, the World Economic Forum places cyber risk among the five major risks for this year, by decoupling damage to infrastructure and the risk of fraud[3] via cyber space. *Allianz* insurer, in its "2020 barometer", places cyber risk as the number one priority for 2020.[4]

For its part, the Federal Reserve of the United States (FED), in its report of January 2020 on the risks weighing on the American economy, identifies cyber risk as a direct threat on the economy because of the interconnections generated by the interbank loans and other relationships with counterparties.[5]

Consequences can be serious for businesses and the economy of a country as a whole also because of the vagueness of insurance regulations, due to the difficulty to identify and then assess costs and losses with a view to their compensation.

For instance, acts of war[6] are among the exclusions from insurance contracts. Therefore, the non-consideration of this risk and the inability to provide security to guarantee it can be a way to argue that cyber risk is considered as an exclusion from the contract.

Furthermore, if cyber risk is reclassified as an act of war, you still need to know what it covers. The Maritime Insurance Code provides specific rights under the terms of article L172-17: "When it is not possible to establish whether the claim originates from a risk of war or a risk of sea, it is deemed to result from a sea event."[7]

By extension, a cyber-attack whose origin cannot be established will fall under the code of a disaster event, which is covered by insurance.

The legal vagueness associated with cyber-type attacks could generate a conflict between two actors who have no interest to have a conflict, this approach having been theorised as a 'Thucydides' trap[8] by Graham Allison. How can we clarify this problem, which can either be a conflict generator or generate an insurance vacuum for these risks?

Failing to be able to identify the reasons and origins of cyberattacks, the solution is to determine the responsibilities by identifying the breaches, as well as the event giving rise to them.

Professional awareness of a cyber risk

As part of their risk measurement activity, as an act of good management, management teams are responsible for ensuring that these risks do not degenerate into a crisis. The development of cyber risks has the consequence of increasing the responsibilities of companies both in the use of software and in the provision of services by its employees. A company should no longer care exclusively for its interests: it is now called upon to care for others. The conformity of activities gives rise to the concept of "social responsibility".

The *Agence nationale de la sécurité des systèmes d'information* (ANSSI) warns of the responsibility of private actors, a responsibility springing from the lack of security of their Information System (SI) in the same way as the use of company vehicles engages the responsibility of the company.

This warning targets indirect cyber-attacks, also known as bounce computer attacks. These consist in using one or more intermediate systems without the owner's knowledge (IoT / Smartphones, servers, etc.) in order to provide the malicious agent with the possibility:

- to hide the origin of the attack and its identity,
- to saturate the network of the target company and thus to destroy or block its information system (Denial of Service attack. DoS or DDoS), or
- to break into the business by devious means.

The company's ecosystem is of particular interest. Subcontractors, such as service providers connected to the company's IS, or even email correspondence through 'phishing' are at the heart of these vulnerabilities.

Just as a company is legally responsible for the goods and people who serve its activity, it is also responsible for its information systems. Several causes in using digital tools can be described:

- Human error, through negligence or unintentional omission, concerning an update and the maintenance of the IS.
- The attack on the IS, with the consequence of the cessation of activities.
- Loss, theft or leakage of personal or confidential data.
- The security of the IT system of the outsourcing provider.
- The diversion of the means of production and connected objects (IoT) that can serve a larger-scale attack aimed at another company in another sector, or a state service.

The event giving rise to responsibility can thus come from the company's shortcomings in terms of measures to protect it's IS, leading to the diversion of a company's systems and capacities towards another entity.

A regulatory framework to define and manage cyber risk

The GDPR compliance framework imposes the obligation to inform in the event of a data breach, but also the need to improve security devices in order to increase the level of protection and detection (Articles 32, 33, 34 of the GDPR[9]).

Thus, "*companies and organizations are obliged to inform the national supervisory authority without delay in the event of a serious data breach, so that users can take appropriate measures.*"[10]

The NIS Directive notes that the "Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities and in particular to the functioning of the internal market."[11]

This regulatory framework is also reinforced by ISO standards 27001, 27701 **placing responsibilities on the professionals.**

Conclusion

A 'digital law' should lead to changes in the insurance law, as well as in the definitions proper to the law of war, by incorporating the concept of impacts likely to be identified as acts of war. For insurers, the challenge will be, like in the Maritime Law insurance code, to be able to look for compliance framework cyber security responsibilities and breaches.

For insolvency practitioners, the challenge will be "to carry out all acts necessary for the conservation of the rights of the company facing its creditors and the preservation of the production capacities" (L.622-4 of the commercial Code).

At the same time, the regulatory framework proposes the tools to build the jurisprudence and manage a protean risk generating collateral damage. ■

Footnotes:

1 Definition French Government: "attack on computer systems carried out with malicious intent" https://www.gouvernement.fr/risques/risques-cyber

2 Schneier, B. (2013), "Cyber conflicts and national security", *UN Chronicle*, vol. 50/2, https://doi.org/10.18356/5cbca97a-en.

3 World Economic Forum; "*The Global RisksReport 2020: Insight Report 15th Edition*", January 2020

4 Allianz Risk Barometer, Identifying The Major Business Risks For 2020: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf

5 Federal Reserve Bank of New York; "*Reports Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis*", January 2020

6 Légifrance, Code des assurances France; Article L121-8,

7 Légifrance, Code des assurances, Article L172-17: https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006792318&cidTexte=LEGITEXT000006073984&dateTexte=19760721

8 Graham Allison, 2017 "*Destined for War: can America and China escape Thucydides's Trap?*", Broché

9 Ludovic Van Egroo, "*Le cyber risque: nouveau facteur de défaillance pour les entreprises?*", Eurofenix INSOL Europe, printemps 2017.

10 European Parlement, "*New EU data protection rules put citizens in control*", (10-03-2017)

11 European Commission, "*Directive (EU) 2016/1148 of the European Parliament and of the Council*"

> **JUST AS A COMPANY IS LEGALLY RESPONSIBLE FOR THE GOODS AND PEOPLE WHO SERVE ITS ACTIVITY, IT IS ALSO RESPONSIBLE FOR ITS INFORMATION SYSTEMS**