Cyber-risk:
A new factor for corporate insolvency?

Ludovic Van Egroo examines the rise of cyber-crime, the regulatory impact and the consequences for insolvency professionals

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

Digital is now prevalent in all sectors of economic activity. The European Commission[1] has identified it as a strong vector of growth with the potential to create hundreds of thousands of jobs and about 415 billion euros in revenues.

According to the French E-Commerce Professional Federation (FEVAL), quoted by the "Journal du net", e-commerce websites in France generated a turnover of 72 billion euros in 2016. A figure that is constantly increasing[2].

While it is a great source of wealth and value, this economy is also creating new risks for companies.

The French Government[3] defines Cyber-risks as "*An attack on information systems carried out for malicious purposes. [A cyber-attack] targets different computing devices: computers or servers, isolated or in a network, linked or not to the web, peripheral equipment such as printers, or communicating devices such as mobile phones, smartphones or tablets. There are four types of cyber-risks with various consequences, directly or indirectly affecting individuals, administrations and companies: cyber-crime, damage to the image (reputation?), industrial spying, sabotage*".

These four types of cyber-risks can have an impact on businesses that can be immediate or of medium to long term. These consequences can be classified as in diagram 1 below[4].

According to the Global *Economic Crime Survey* by PWC[5]: "*The emergence of cyber-crime is one of the main risks for companies in the world*". Indeed, according to PWC, cyber-crime increased by 25 points between 2014 and 2016, from 28% to 53%.

> THE EMERGENCE OF CYBER-CRIME IS ONE OF THE MAIN RISKS FOR COMPANIES IN THE WORLD

1. Cyber-risks and their impact

Type of Impact	Management	Economic and Financial	Reputation	Juridicial
Immediate consequences	Governance challenged	Loss of clients Failure / Bankruptcy Destruction of intangible assets / depreciation of assets Decommissioning of production tools, investment for the restoration of assets	Theft of customer / corporate data	Increase in insurance premiums Prosecution for Non-compliance
Medium / long term consequences			Degradation of E-reputation and corporate image	Prosecution for theft and / or data destruction

What are the regulatory developments in the sector? To what extent are insolvency professionals concerned by this risk? What are the consequences for insolvency professionals?

Regulatory developments in the sector: Towards a division of responsibilities between Internet operators

Faced with these new challenges, the Council of Europe and the European Parliament adopted in 2016 a Directive on the security of networks and information systems[6] aimed at protecting digital and digital economy activities in the single market. This Directive is based on the principle of protection and assistance of the European Union for consumers[7].

Once the Directive has been transposed into each Member State's legal system, companies will be required to disclose "*the major IT security incidents of which they are victims*"[8]. The measures adopted aim to:

- strengthen cybersecurity capacities in each country and the national strategy for digital security;
- establish a framework for voluntary cooperation to facilitate the sharing of technical information on risks; and
- define at national level cybersecurity rules for the companies responsible for networks.

The Council and the European Parliament have defined two levels of corporate responsibility between:

- on the one hand, network and infrastructure operators qualified as "*Operators of essential services*". These include search engines, social networks, cloud operators but also the administrations responsible for networks that are used for data transfer;
- on the other hand, companies that collect and use consumer data through Internet. Companies in charge of this data will have to guarantee the security of data and justify it.

The European directive will have to be transposed to Member States by 2018 and applied to companies as part of the digital economy.

What are the new obligations of the regulatory framework?

The European Directive opens up the possibility of:

- Class actions in order to protect consumers' rights and personal data; and
- the right to ask for compensation for material or moral damage by the "contractor" or "subcontractor" who has not met the conformity requirements and who has not protected users' data.

The second part of the Directive concerns businesses using personal data and company data. Any company that processes and stores personal data is required to comply with the General Data Protection Regulation (GDPR). Member States have two years, until 2018, to implement and define the bodies in charge of the implementation.

In concrete terms, this translates into:

- obligation for companies collecting and using data to ensure that users explicitly

"THE EUROPEAN DIRECTIVE WILL HAVE TO BE TRANSPOSED TO MEMBER STATES BY 2018 AND APPLIED TO COMPANIES AS PART OF THE DIGITAL ECONOMY"

> FROM THE MOMENT FIRMS ARE ABLE TO IDENTIFY CYBER-ATTACKS AND THEIR CONSEQUENCES, THIS COULD BECOME A CAUSE OF THEIR FAILURE

2. Issues and consequences of cyber-risks

Consequences of cyber-risks	Issues
Damage to intangible assets	Restore intangible assets to avoid depreciation Assess the possibility of maintaining the activity
Data protection for companies in difficulty	Assess the impact of difficulties on the protection of company data Ensure that the company was and remains in compliance with the regulations in the context of insolvency procedure

consent to the way their data is used, and also provide for the transferability of the data to the users as well as their permanent deletion;

- the right to be informed in case of data piracy (Articles 33 and 34 of the GDPR). Thus, "*Companies and organizations shall be obliged to inform the national supervisory authority immediately in the event of a serious breach of the data so that users can take appropriate measures*"[9]; and
- the need to improve security features, that is to increase the level of protection but also the ability of devices to detect data thefts.

Faced with this new economy and regulatory developments, what are the new responsibilities of insolvency professionals?

What are the challenges for insolvency professionals?

As part of their mandate, in accordance with the Order of 14 January 2009[10], insolvency professionals will be required to take into account the cyber-risks.

Including the cyber-risk factor in the analysis of the origin of a company's difficulties

From the moment firms are able to identify cyber-attacks and their consequences, (e.g.: Decommissioning of an e-commerce company's website) in terms of loss of turnover, this could become a cause of their failure. Thus they could seek the assistance of the Commercial Court.

The failures could have originated from two different levels of responsibility:

Direct causes, if the difficulties originate from an attack on the infrastructure and the systems of the company such as its servers and information networks:

In this case, the company's data might have been compromised and the company can be held accountable. It will be necessary to ensure that the company has taken the necessary measures to protect the data of its customers, but also to evaluate the company's ability to carry on its activities. The immediate consequences are the depreciation of the value of the assets and of the company's reputation. In October 2016, DYN, an American company hosting websites, was the victim of an attack rendering several platforms and websites inaccessible. The company was bought the following month by Oracle.

Indirect causes, in the event that a company suffers from the failure of an operator of essential services, such as a web host:

This scenario applies, for example, to vendors selling via e-commerce sites and mobile applications. In case the website crashes or becomes inaccessible because of a cyber-attack, their sales are negatively affected, generating a net loss of turnover which, in turn, does not allow companies to meet their due dates.

In these cases, the insolvency practitioner may have to call on cybersecurity professionals in

order to make a diagnosis:

- Compliance with data standards.
- Analysing the origin of the attack and involving the insurance company.
- Identifying solutions to secure the networks, in order to maintain the business and safeguard employment.
- Researching the responsibilities of the different stakeholders.

Depending on the findings, the insolvency practitioner may initiate procedures to repatriate data, to request the deletion of personal data, hosted or in transit, as per the defaulting company's framework of compliance requirements.

The challenge of identifying data and stakeholders

In the same way that the administrator and the legal representative ensure that the administered company carries out its activity in compliance (as may be the case for a restoration activity with an IV license or compliance with a company's environmental norms), the insolvency practitioner must ensure that the company complies with national standards for cyber-fraud and risk.

However, the digital economy being international in nature, identifying the stakeholders, especially in terms of responsibility, is difficult.

Conclusion

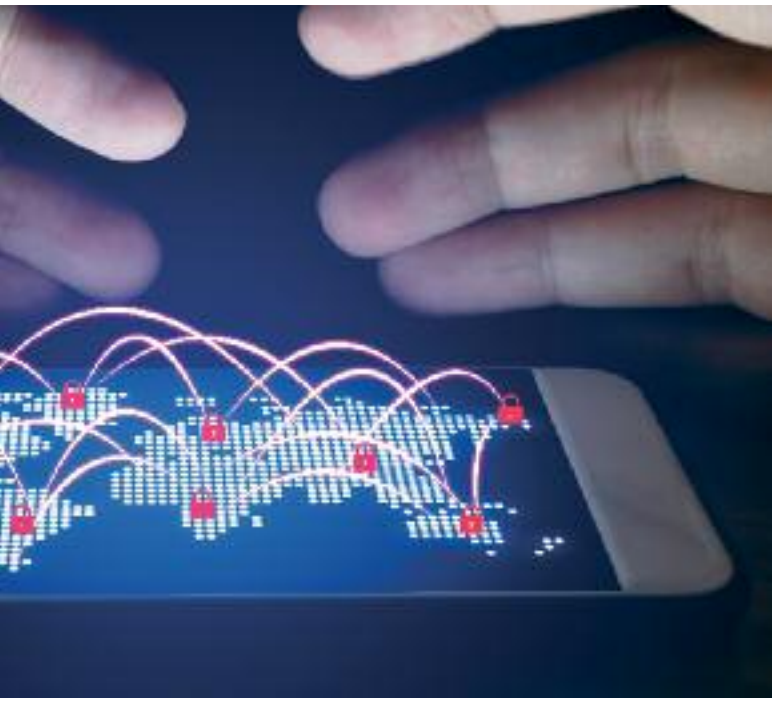
Frauds and company failures linked to cyber-risk and cyber fraud have emerged as a result of the digital economy, leading the European Union and Member States to acquire new means of protection and to create a legislative framework necessary for the protection of data collected by companies.

The European Directive was necessary to standardize the legal framework of national institutions because of a continuously evolving risk, thus guaranteeing the security of the common market and the interests of European consumers.

The European framework created for business activities related to the digital economy provides an initial orientation for the treatment of failures. Insolvency professionals will be required to take into account the potentially international aspects of this type of activity, in particular:

- **The nationality of the structure hosting contracts:** the user data can be hosted in different countries;
- **Contracting or subcontracting the companies' nationality,** especially in the case of the involvement of a holding company structure for tax purposes;
- **The ownership of data** by the insolvent company, and getting in touch with each country's relevant insolvencies within the European Union; and
- **The possibility of initiating or joining collective actions** by several European insolvency professionals.

Finally, the treatment of the insolvency of digital companies has a supranational dimension: it can be just European, but also international. ■



> **THE INSOLVENCY PRACTITIONER MUST ENSURE THAT THE COMPANY COMPLIES WITH NATIONAL STANDARDS FOR CYBER-FRAUD AND RISK**

Footnotes:

1 European Commission, A DIGITAL SINGLE MARKET FOR EUROPE, https://ec.europa.eu/commission/priorities/digital-single-market_en (20-03-2017)
2 Journaldunet, "*In 2016, French E-commerce raised 72 billion euros*", http://www.journaldunet.com/ebusiness/commerce/1172030-chiffre-d-affaires-e-commerce-france/ (20-03-2017)
3 Official French government website dedicated to cyber-risk http://www.gouvernement.fr/risques/risques-cyber, (20-03-2017)
4 Michael Bittan & Fouzi Akermi "*Cyber 2016, The Hidden Face of Cyber*"; DELOITTE Office, publicised in 2016
5 Jean-Louis Di Giovanni , Fabienne Borde , Thomas Estève, "*Fraud explodes in France Cybercrime at the heart of all concerns*", Global Economic Crime Survey 2016, published March 2016
6 European Commission, "*The Directive on security of network and information systems (NIS Directive)*" https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, (20-03-2017)
7 European Union, "*Areas of action of the European Union*" https://europa.eu/european-union/topics/consumers_fr (20-03-2017)
8 European Union Council, "*Improving cybersecurity in the EU*" http://www.consilium.europa.eu/fr/policies/cyber-security/ (20-03-2017)
9 European Parliament, "*New EU rules on data protection put citizens in charge*" http://www.europarl.europa.eu/news/fr/news-room/20160413BKG22980/nouvelle-l%C3%A9gislation-europ%C3%A9enne-sur-la-protection-des-donn%C3%A9es, (20-03-2017)
10 Légifrance : Arrêté du 14 janvier 2009 - art. (V) https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000005634379&idArticle=LEGIARTI000020163273&dateTexte=&categorieLien=cid, (20-03-2017)

Share your views!