BOOK I

JANUARY 2018

REPORT

INSURING CYBER RISK

le club des juristes

CYBER RISK COMMISSION REPORT

BOOK I

INSURING CYBER RISK

REPORT FROM THE CLUB DES JURISTES

Cyber risk commission report

JANUARY 2018

le club des juristes

Registered association - 4, rue de la Planche 75007 Paris - France
Phone : +33 (0)1 53 63 40 04

www.leclubdesjuristes.com

Follow us on:

Composition of the Commission

CHAIRPERSON :

Bernard Spitz, President of FFA, the French Insurance Federation

GENERAL SECRETARY :

Valérie Lafarge-Sarkozy, Partner lawyer, Altana law firm

MEMBERS :

Nicolas Arpagian, Strategy & Public Affairs Director, Orange

Agnieszka Bruyere, Security Services Director, IBM France

Brigitte Bouquot, VP Insurance and Risk Manager, Thales, and Chairperson of AMRAE, the association for corporate risk and insurance management

Alice Chérif, Deputy Public Prosecutor of the Cybercriminality unit at the Tribunal de Grande Instance de Paris

Philippe Cotelle, Head of Insurance Risk Management Cyberdefense, Airbus Defence and Space

Georgie Courtois, Lawyer

Christophe Delcamp, Deputy Director of general and liability insurance, FFA

Emilie Dumérain, Legal Deputy, Syntec Numérique

Philippe Gaillard, Director, Corporate accident insurance, Axa France

Agathe Lepage, Professor at Université Panthéon-Assas (Paris II)

Charles-Henry Madinier, Head of Marsh Risk Consulting France, Marsh

Alexandre Menais, Executive Vice President and Group Head of M&A, Strategy & Development, Atos

Martin Pailhes, Head of the Legal team "Information Technology – Intellectual Property", BNP Paribas

Christian Poyau, Chairman, Medef Digital Transformation Commission

Didier Parsoire, Chief Underwriting Officer Cyber Solutions, Scor

Sylvie Sanchis, Police Commissioner, Head of the brigade investigating information technology fraud, Director of the Legal Police at the Préfecture de Paris

Cécile Vignial, Senior consultant for the OECD

François Weil, Member of the State Council

Leigh Wolfrom, Policy analyst – Directorate for Financial and Enterprise Affairs, OECD

CONTRIBUTORS TO WRITING THIS BOOK :

Cécile Vignial, Senior consultant for the OECD

Christophe Delcamp, Deputy Director of general and liability insurance, FFA

Célia Hamouda, Lawyer**,** Altana law firm

Nicolas Arpagian, Strategy & Public Affairs Director, Orange

Mariette Bormann, Deputy Director for Compliance, FFA

Philippe Cotelle, Head of Insurance Risk Management Cyberdefense, Airbus Defence and Space

Laetitia Daage, Lawyer, Altana law firm

Philippe Gaillard, Director Corporate accident insurance, technical and cyber risks, Axa France

Carole Gintz, Associate Managing Director, Moody's Investors Service

Olivier Hassid, Director, PwC

Sébastien Heon, Deputy Chief Underwriting Officer Cyber Solutions, SCOR

Marine Kociemba, FFA research analyst

Valérie Lafarge-Sarkozy, Partner lawyer, Altana law firm

Charles-Henry Madinier, Head of Marsh Risk Consulting France, Marsh

Jean-Guy de Ruffray, Lawyer, Altana law firm

Benjamin Serra, Vice President – Senior Credit Officer, Moody's Investors Service

Emmanuel Silvestre, Senior Vice President Financial risk, Liberty Mutual

Stéphane Spalacci, Technical manager, GAREAT

Luc Vignancour, Cyber & Crime Practice Leader, Marsh

Leigh Wolfrom, Policy analyst – Directorate for Financial and Enterprise Affairs, OECD

COMMISSION SECRETARY :

Bérénice Hahn de Bykhovetz, Doctoral student at Université Paris II Panthéon-Assas

BOOK I
Insuring cyber risk

From Christopher Columbus to the invention of the combustion engine, from the printing press to nanoscience, technical progress has always carried new risks. This has never been truer than of cyber technologies. Anyone now has cheap and easy access to hacking tools. Meanwhile, the unrelenting digitisation of production processes has created windfall opportunities for criminals. Add the human factor and the unavoidable loopholes it introduces anywhere where protective, but costly, redundancies were not included from the start. It's no longer a question of whether cybercrime may occur but when it will.

There is no end of examples. On 7 September 2017, Equifax, one of the biggest US credit agencies that collects and analyses consumers' personal data when they apply for a loan, announced that its computer system had been hacked. Equifax was threatened with the potential theft of sensitive data for no fewer than 143 million Americans (names, addresses, credit card numbers, social security numbers, and more). Soon the date of Uber's 57 million users were similarly endangered.

Again in 2017, in Europe, British hospitals, the Spanish telecoms provider Telefónica, Saint Gobain, the Russian home ministry, Deutsche Bahn and many others were targeted by the "WannaCry" and "Petya" ransomware attacks.

The evidence is clear: no one is safe any longer.

These threats are not haphazard. The latest Lloyd's of London cyber risk study presents as most likely massive attack scenario an attack aimed at a cloud service provider. Lloyd's estimates the losses between US$15 billion and US$121 billion, with average losses of US$53 billion.

Faced with such challenges, our societies must rally at every level – individual, professional, corporate. This applies particularly to small-sized companies that often have not had the time, the organisational experience or the wherewithal to build their own consistent cyber defence policy. Those who reassured themselves by mistakenly assuming that hackers would go only after the biggest fish are especially at risk.

Our economies have a considerable arsenal to protect themselves. Professionals already design corporate solutions to effectively safeguard their digital life safe; these are in fact prime opportunities to develop and to excel. The French cyber security market has grown by over 10% in 2016. This, for better or for worse, is only the beginning. However, even today, such firms are small and scattered, dependent upon still-inadequate funding, especially from the private sector.

At the forefront of economic players, insurers and reinsurers actively participate in the evolution of digital economies, even though Europe and France still lag behind

The numbers speak for themselves: today, the global cyber insurance market is estimated at between US$3 billion and US$3.5 billion. The American market accounts for 85% to 90% of these premiums. Europe, however, still accounts for only 5% to 9% of this market, with a maximum amount of €255 million (US$300 million) in premiums, of which France represents only €40 million. Plainly, there is a huge gap between developed countries in terms of their perception of this risk, and in the insurance investment they are willing to make to protect themselves.

The French and the European public authorities have taken the matter in hand. They have laid the foundation of a new regulation within the Union, the transposition of which is under way. This first step is essential; it is not enough. The existence of a legal framework must be accompanied by the vigilance of all economic stakeholders, and by the steadfast backing of public authorities for the development of a French and European cyber-protection sector.

To address this very real threat, Le *Club des Juristes*, together with all parties concerned, has come forward to contribute to an approach taking fully into account the complexity of all these economic, legal and insurance dimensions.

Following its deliberations, the group, which I have been honoured to chair, has not only taken stock of the situation, but has also put forward a consistent set of recommendations. The first volume explores a wide range of solutions that would promote the emergence of a true cyber insurance. At the end of this document, you will find our ten recommendations for a global and effective approach to the problem. Two other volumes will follow, examining in particular the legal dimension and the conditions for the prevention of this new cyber risk, which we will have to get used to understanding, fighting and managing.

General Douglas MacArthur used to say: "The history of failure in war, or in any other human endeavour, can be summed up in two words: 'too late'." We are indeed fighting a war in this beginning of the 21st century. Let us give ourselves every chance of winning it.

Bernard Spitz
President, French Insurance Federation

Table of contents

We are at the dawn of smart transport and smart territories, industries 4.0, virtual reality, widespread personal data processing or the Internet of Things, but have only seen the first stirrings of digital transformation. It is drastically changing the ways in which we communicate and consume, our *rapport* with health, energy, education or the State, it has crept into our homes and in the weave of the clothes we wear, on our wrists, in pacemakers, etc. It is recasting the production processes and services of companies, their relationship with their clients, and their interconnections with their value chain. Today, it is a key enabler of growth, innovation and competitiveness for economic stakeholders.

The risks are proportionate to the challenges; they include the risk of a cyber incident that could jeopardise all the economic and social benefits obtained from digital transformation[1]. A cyber attack or an unintentional data manipulation error may compromise privacy, integrity and accessibility of data and information systems resulting in heavy financial losses and even threaten the very survival of a company, or the functioning and the security of a State.

In 2017, the "WannaCry" attack in mid-May, followed by "NotPetya" detected on 27 June, and the hack exposed on 25 September[2] on all of the emails exchanged between the Deloitte advisory and law firm employees and the firm's clients probably over six months (the hackers may have had access to five million messages) are reminders of the threats posed by cyber risks on the economy and on society. Economic stakeholders have two key complementary tools to tackle the proliferation of cyber incidents: prevention – this will be the topic of another book by this group – and risk transfer through insurance in cases where the prevention measures do not suffice to protect oneself from a cyber incident.

The cyber insurance market contributes towards reducing the financial impact faced by the economic stakeholders following an attack, by providing an ever-broadening range of cover and service offerings. It

(1) See OECD, *Supporting an effective cyber insurance market, OECD report for the G7 Presidency,* May 2017

(2) The Guardian, *Deloitte hit by cyber attack revealing clients' secret emails,* Sept. 2017, [https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails].

also participates in raising awareness about the exposure to cyber risk, sharing expertise on managing these risks, encouraging investments to curb those risks, and improving the response to cyber incidents[3].

In France, and in Europe for that matter, the cyber insurance market is still embryonic, particularly in the SME and micro business segment. SMEs are at the receiving end of 60% of the attacks on businesses reported in France[4].

We need to adapt to this new, particularly favourable legal and economic environment to improve the conditions of transferring cyber risk. By optimising their financial protection in addition to their digital security, the economic stakeholders will boost national and European resilience to a risk against which no one can claim to be immunised.

(3) OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, 2017.
(4) French Home Ministry, *État de la menace liée au numérique en 2017*, January 2017

PART 1
Cyber insurance in Europe: an emerging market

Products dedicated to covering cyber risk saw the day over nearly twenty years ago in the United States, and under ten years in France. At present, Europe represents less than 10% of the global cyber insurance market, which is far from proportional to the risks involved.

Why has the market remained so thin in Europe and particularly in France to this day, and how can we make it more efficient for companies and other economic stakeholders seeking cover against cyber risks?

I. The specificities of cyber risk

Identifying the specificities of cyber risk as regards conventional insurability criteria[5] can provide some insight into these issues.

The insurability criteria of a risk are generally divided into three categories[6]:

- actuarial criteria (randomness of occurrence/relative absence of correlation between the risks; maximum loss that can be measured and covered, and moderate average loss per event; sufficiently high exposure to risk to establish a statistical database; limited moral hazard and adverse selection);
- market criteria (premium considered to be affordable by prospects with respect to the cover provided);

(5) This section refers notably to the findings of one of the very few studies on the insurability of cyber risk: Biener, Christian, Eling, Martin, Wirfs, Jan H., *Insurability of cyber risk: an empirical analysis,* 2015.
(6) Berliner, *Limits of insurability*, 1982.

- societal and regulatory criteria (legal restrictions to covering certain risks in particular).

At present, cyber risks display a number of characteristics that put them on the borderline of insurability as regards several of the above criteria.

A. Losses likely to get considerably heavier in the future

For a risk to be insurable, the expected losses must be lower than the insurers' available capacity to cover them. Insurers can use the average loss, maximum loss and loss frequency measurements to calculate their capacity to cover a risk without putting their solvency at risk, and the premium that their prospective policyholders may find affordable.

Estimating the cost of cyber incidents is a complex matter. As an example, the table below shows the results of data gathered on losses from cyber incidents suffered by companies in the United States over a ten-year period.

Focus – Estimated average, median and maximum costs of cyber incidents, 2005-2014*

Event type	*N*	Average cost	Median cost	Maximum cost
Total (In million US$)	921	7.84	0.25	750

** The data given refers to a sample of incidents spread over the 2005-2014 period. They concern only incidents for which a cost estimate was made.*
Source: Romanosky, Examining the costs and causes of cyber incidents, Journal of Cybersecurity, August 2016.

The overall maximum cost of cyber incidents has until now remained far lower than that of other major risks and several natural disasters in particular: the overall cost of hurricane Katrina in 2005, for example, was estimated to exceed US$80 billion (2016 USD) of which US$40 billion was insured; the cost of other disasters such as the 9/11 attack in 2001 was estimated at US$25 billion (2016 USD)[7]. While it is still too early to measure the overall impact of the WannaCry and NotPetya attacks, given the extent of the losses incurred in other past cyber incidents (such as the Epsilon attack that cost US$4 billion, or the Sony PlayStation attack of $171 million), one cannot conclude to the uninsurability of cyber risks.

Beyond the steady rise in the cost of the harmful consequences of cyber incidents and their frequency, the new challenges faced by insurers relate mainly to the uncertainty of potential future losses incurred through mega attacks or a series of smaller but simultaneous attacks.

As of 2018, insurers will also need to deal with the increased cost of cyber incidents due to the new requirements relating to the development of the regulatory framework and notably the additional notification duties of companies. The anticipation of these new costs should accelerate the cyber insurance penetration rates.

Recent scenarios show losses arising from a major cyber incident targeting, for instance, critical infrastructures that, by nature, have a wide outreach, or from a series of incidents (cyber hurricane scenario) that could reach unprecedented levels, putting the solvency of one or more insurers at risk.

In the United Kingdom, for example, the financial market infrastructures' exposure to cyber risk is a major cause for concern[8]. A massive cyber incident suffered by it would impact national and world economy, entailing considerable costs.

(7) Swiss Re Institute, *Catastrophe naturelle en 2016 : une année de dommages tous azimuts,* Sigma, No. 2, Feb. 2017.

(8) See for example Bank of England (2014), *The Bank of England's supervision of financial market infrastructures,* p. 10, that describes the four pillars of the programme designed to step up the financial sector's resilience to cyber risks.

An insurer[9] also drew a parallel between the worldwide collapse that would occur after a major cyber incident, for example with a prominent cloud services provider, with immediate cascading effects on the actual economy (suppliers of water and energy, medical equipment, banking or transport networks, etc.), and the Lehman Brothers collapse with its cascading consequences in September 2008. In the latest cyber risk study by Lloyd's, the most likely massive attack scenario is also that of an attack on a cloud services provider. According to Lloyd's, the losses could be in the range of US$15 billion to US$121, with an estimated average of US$53 billion[10]. These figures are comparable to those incurred in the biggest natural disasters mentioned earlier[11].

For many observers, cyber risk is currently the biggest and the most systemic of risks.

Given the magnitude of certain cyber events that could entail considerable cumulative damages, certain key players consider that the risk exceeds the market's capacity to absorb it[12], and that "certain cyber risks, especially those related to extreme catastrophic loss events, such as the disruption of critical infrastructures or networks, may be uninsurable[13]".

(9) Zurich, *Beyond Data Breaches: Global Interconnection of Cyber Risk*, 2014.
(10) Lloyd's, *Counting the Costs, Cyber Exposure Decoded,* Emerging Risk Report 2017, July 2017, p. 30.
(11) It must however be noted that only one segment of these losses (insured losses) will need to be borne by the insurers. After accounting for the estimations of penetration rates, limits and retentions, Lloyd's assessed insured losses to be US$4.6 billion for an overall loss scenario of US$53.05 billion.
(12) Financial Times *Cyber risks too big to cover, says Lloyd's insurer,* citing Stephen Catlin., 5 Feb. 2015, [https://www.ft.com/content/94243f5a-ad38-11e4-bfcf-00144feab7de?mhq5j=e3].
(13) Swiss Re, Cyber: *getting to grips with a complex risk*, Sigma 1/2017, p. 38.

B. Potentially highly-correlated risks

L'Insurance relies on the pooling of risks. The insurer can generally calculate the average loss (and therefore the premium) per policyholder by applying the law of large numbers according to which the average compensation per policyholder, although random, is nevertheless almost constant, with an identical and independent distribution of losses.

In the case of cyber risks however, the law of large numbers cannot be applied owing to the interdependence of information systems and economic stakeholders that increases the likelihood of the spreading of certain types of cyber incidents. A computer virus can spread by replicating itself in a legitimate program and go from one computer to another, infecting the systems that it comes across. Moreover (unlike biological viruses that are transmitted from one person to another), computer viruses can transmit themselves "from a single node to n computers in x companies[14]". They can therefore infect tens of thousands of computers almost instantaneously, as was the case with the NotPetya malware that used the update procedure of a Ukrainian accounting software to infect various targets in Ukraine, including the Kiev airport and the radiation surveillance system of the Chernobyl nuclear power plant, and went on to contaminate Russia, the United Kingdom, Norway, the Netherlands and France on 27 June 2017, only five hours after it was first detected.

The widespread use of certain operating systems (such as Microsoft Windows), that make several computers and systems vulnerable to the same incident[15], further increases the correlation of risks. This was once again seen recently in the impact of WannaCry that exploited a flaw in Microsoft Windows operating systems prior to Windows 10, for which the security update had not been installed.

(14) A. Jaghadam, *Les conditions d'assurabilité des cyber-risques, Risque magazine*, No. 77, 2009.
(15) D. GEER, *Cyber Insecurity: The Cost of Monopoly*, Computer and Comm. Industry Assoc., 2003, [http://www.ccianet. org/papers/cyberinsecurity.pdf.].

The correlation between several cyber risks is a two-fold challenge for insurers. It firstly complicates their risk portfolio diversification strategy that guarantees their solvency, and leads to accumulation risks. For example, the geographical diversification of the underwritten risks is inoperative given that cyber incidents may be cross-border. Unlike the risk of natural disasters, whose consequences are generally confined to a single region, several cyber incidents can develop instantaneously over a wide national or international area. An entire country can be affected, as was the case with Estonia that, in 2007, suffered the first known cyber attack against a State[16]. Other types of attacks directly have a global reach, such as WannaCry and NotPetya. "The entire world becomes an accumulation zone[17]." Cyber incidents also lead to the accumulation of the insurance lines opened (property damage, operating losses, work accident, civil liability, etc.).

Moreover, the correlation between a large number of risks makes it far more complex to quantify the risk and define the insurance premium. In fact, a company's level of cyber risk does not depend solely on its own prevention efforts. A weak link in the value chain could contaminate its entire ecosystem (subcontractors, counterparties, supply chains, clients, etc.). The "interdependent security[18]" concept that was used to characterise terrorism risk, is equally relevant to cyber risk.

A recent study by Swiss Re[19] points out that the degree of dependency is hinged on the type of cyber threat involved.

(16) An attack that was coordinated from 60 different countries saturated the sites of its Parliament, ministers, banks and the media, causing long-drawn Denial of service.
(17) A. JAGHADAM, *Les conditions d'assurabilité des cyber-risques, Risque magazine*, No. 77, 2009.
(18) H. KUNREUTHER, E. MICHEL-KERJAN, *Insurability of (mega) terrorism risk: challenges and perspectives in OECD* (2005), *Terrorism Risk Insurance in OECD Countries*, 2005.
(19) Swiss Re, *Cyber: getting to grips with a complex risk*, Sigma 1/2017, p. 19.

Focus – Probable losses within and outside the company based on the type of cyber incident

	Damage within the company	**Damage outside the company**
Failure of a personal computer due to a hardware problem	Limited	Limited
Person belonging to the company misuses his or her access rights	Could affect almost all computers of the internal network and cause considerable disruption within the company	Probably limited
Attacks involving interaction with the users, such as phishing or spyware/ malware	Could lead to considerable disruption	Could entail correlated vulnerabilities between firms if some employees in a large number of different companies are targeted
Other types of attacks: malware such as worms, viruses and Trojan horses	Correlated damage	Correlated damage

Source: according to Swiss Re (2017), Sigma 1/2017 – *Cyber: getting to grips with a complex risk,* p. 19

This interdependency between devices/computer systems is increasing exponentially in our ever-more digitised societies: the extension of the scope of digital transformation of organisations, the correlation between the millions of hyperconnected users in the Internet architecture, the widespread use of software that may turn out to be vulnerable, the sky-rocketing number of connected devices and the use of the cloud are all major catalysts in the correlation of risks. Risks that were one-off only a few years ago in the insurer's portfolio – those of corporate clients in different regions of the world or different business sectors, or whose computer systems relied on different operators, etc. – could for example become correlated instantaneously following the decision to store their data in the same cloud.

Although one can still take out insurance or work around the risk in different ways such as reinsurance, the correlation of cyber risks leads to uncertainty and accumulation and makes the task of defining an appropriate cyber insurance offering all the more complex.

C. Lack of a reliable statistical database on cyber loss events

To be insurable, the losses associated with a given risk must be estimated and modelled by analysing the historical series of past events.

In the case of cyber risk, there is little hindsight regarding the frequency and the severity of cyber incidents: as the risk itself is recent, the actuarial calculations are based on narrow historical series.

What's more, the actuarial databases of past incidents are incomplete. In a move to safeguard their reputation and avoid prosecution in case of personal data breaches, many economic stakeholders choose to not reveal the cyber incidents they suffered from publicly, or not disclose the amount of the losses incurred.

Others are unaware that they had suffered attacks, as they are increasingly difficult to detect. Certain recent attacks were in fact detected only one year after the intrusion.

Firstly, most of the data available is published by the companies that provide advisory services or develop solutions for cybersecurity or risk transfer, which leads to potential bias on two counts – it is not in their interest to minimise the threat, and their data – often based mainly on the statistical sample of their client base – is partial.

The statistical databases available on cyber incidents are not only narrow and partially biased, they are also undermined by two technical constraints.

On the one hand, there is no standardised methodology to establish a homogeneous inventory of cyber incidents and their impact on the national and international scale. What cyber incidents should be logged in a database? Should there be a threshold based on their severity so that the authorities in charge of gathering information are not flooded by notifications of minor incidents that do not really have harmful consequences? How should the severity threshold be defined? The absence of shared responses leads to bias when comparing the published statistics.

Also, while there are several private agencies that publish statistics relating to cyber incidents (IT service providers, consultants, etc.), there is no body in France to date, whether private or public, whose task is to collect and anonymise information on cyber incidents at the national level in order to draw up statistics that can be shared with all the market players.

The lack of a reliable database deprives insurers of a key tool for modelling cyber risks, and all stakeholders of an information source that could contribute to increasing awareness of cyber risk.

D. Broadly intangible, difficult-to-measure losses[20]

Cyber risk often generates intangible damage that is very difficult to measure, such as tarnished brand reputation following a massive data breach. The lack of trust in a company's ability to safeguard its own data as well as its clients' data could be drastic and persistent, causing genuine harm to the company. This type of damage could be significant: the loss of brand value of a company that suffered a data breach in 2015 in the United States was estimated at an average amount between US$184 million and US$330 million depending on the type of data affected[21]. Besides, the attacks directed at major groups such as Sony, Target and Equifax show that being exposed to a massive attack could adversely affect the company's stock market value in the short term.

These impacts however tend to decrease as the number of cyber attacks continues to increase. As this type of incident becomes more commonplace, the clients and shareholders of the targeted companies tend to penalise them less or do so for a shorter length of time. The impact on the share price is lower[22].

(20) See the previous chapter.
(21) Ponemon Institute, *Reputational Impact of a Data Breach Study*, 2015.
(22) *Artemis (2017), Cyber risks and government pools. Too soon?, Artemis news articles,* 30 March, [www.artemis.bm/blog/2017/03/30/cyber-risks-and-government-pools-too-soon/].

The Equifax example

On 7 September, Equifax, one of the biggest US credit agencies that collects and analyses personal data of consumers applying for a loan, announced that its computer system had been hacked. This incident resulted in the potential breach of sensitive data of about 145 million[23] North-Americans (names, addresses, credit card numbers, Social security numbers, and more).

On 7 September, Equifax's share price on the New York Stock Exchange was US$142.7.

On 8 September, the share was trading at US$123.23, having fallen by 14%.

On 15 September, the share price was US$92.92, having lost 35% of its value in one week. On the same day, Equifax announced that its security manager and IT head had been fired. From that date onwards, the share price started to pick up.

On 22 September, Equifax's CEO, Richard Smith, resigned.

(23) As estimated on 5 October 2017.

E. Complex analysis of the risk to insure, due to the technicality and sensitivity of the information exchanged

To cover cyber risks, insurers need to have extensive cyber expertise and in-depth knowledge of the client company in order to understand the threats faced by the company, and take into account all of the cyber exposures and vulnerabilities detailed by the Risk Manager or the department handling the matter.

However, policyholders are often not very keen on sharing all the information with the insurers and other providers involved in the insurance contract that would allow them to accurately quantify their risk exposure; this data that relates to the concerns their core business and their value (ongoing projects, patents, etc.) is particularly strategic and confidential.

Sometimes, companies are also reticent to share information on the resilience level of their information systems, including operational systems, and notably the results of practice test attacks when they engage in that type of drills.

At this point in its development, the cyber insurance market is confronted with information skewness between the insurers and the insured, which can be very high. This could hinder the calculation of an insurance premium that is in line with the specificities of the policyholder's profile, and lead to anti-selection – companies that have already fallen victim to attacks and those that consider being most exposed to that risk are more willing to take out insurance than other companies, causing an imbalance in the insurers' risk portfolio.

F. A highly dynamic risk

About 90% of cyber loss events reported "result from human error or human behaviour[24]". The unpredictability of human behaviour, whether

(24) W.TOWER WATSON, *When it comes to cyber risk, businesses are missing the human touch*, 7 March 2017, [https://www.willistowerswatson.com/en/press/2017/03/when-it-comes-to-cyber-risk-businesses-are-missing-the-human-touch].

voluntary or not, that determines the occurrence and severity of several cyber incidents (likelihood of data theft or data manipulation errors, choice of the target in case of an attack, etc.) make the cyber risks intrinsically more versatile and difficult to foresee or model compared to other types of events.

Additionally, as with terrorism risk, the choice of targets and the modus operandi of the attacks are constantly adapted to various parameters[25] such as the targets' level of protection or earning power (for example due to the fluctuations in the resale price of stolen data on the dark web), that creates "dynamic uncertainty[26]". This complicates risk anticipation, with respect to natural disasters, whose location does not depend on the vulnerability of the sites.

Also, the risk of cyber attacks completely changed in just a few years, as the cyber attacker profile fast became increasingly sophisticated. From geek teens looking for a challenge or recognition, we went on to organised crime gangs, professionals, sometimes supported by States for reasons that are financial (i.e. extortion), economic (i.e. industrial espionage) or political (i.e. to undermine a State, protest against its diplomatic action, influence an election process, etc.). We can observe that concomitant to the professionalisation of cyber attackers, there is a proliferation of players who lack the resources and the expertise and therefore take advantage of the expanding offering of low-cost turnkey attack solutions in the black market[27]. Fortinet recently warned about the development of ransomware-as-a-service solutions that increase the risk of this type of attack[28]. While ordinary theft of data that is sold on the dark web remains a major source of damage, the cost of the ransomware (blocked access to data or a system until the payment of an amount that is often deno-

(25) See the graphical illustration of the attack types by sector, by Lloyd's, in association with KPMG and DAC Beachcroft (June 2017), *Closing the gap – insuring your business against evolving cyber threats*, p. 18.

(26) See for example H. KUNREUTHER, E. MICHEL-KERJAN, *Insurability of (mega) terrorism risk: challenges and perspectives in OECD* (2005), Terrorism Risk Insurance in OECD Countries, 2005.

(27) Swiss Re (2017), *Cyber: getting to grips with a complex risk*, Sigma No. 1/2017.

(28) J. ROMMEL, *Ransomware-as-a-Service: Rampant in the underground Black Market*, Fortinet, 16 Feb. 2017, [https://blog.fortinet.com/2017/02/16/ransomware-as-a-service-rampant-in-the-underground-black-market]

minated in bitcoins) is said to have reached USD one billion in 2016[29]. Insurers must understand and pre-empt these changes in cyber attacks.

The cyber risk has also evolved in pace with the technological progress of ever-more-powerful computer and electronic systems, and the expanding cyber space scope. The arrival of connected devices and the progress in artificial intelligence paved the way for a new age of opportunities that the cyber attackers immediately took advantage of. On 21 October 2016, access to Amazon, Netflix, Twitter or PayPal was blocked in one part of the United States due to the attack on the cloud producer Dyn through connected devices (networked remote monitoring cameras). The use of artificial intelligence to "create personalised tweets to get the targets to click on malicious links[30]" was also highlighted recently.

Lastly, as with the terrorism risk, the actions implemented by the States could have a real impact on the level of cyber risk, and the choice of the target. The cyber attacks could also originate from the States themselves. The political and diplomatic stance may also trigger cyber protests. The State-level dimension of cyber risks adds further uncertainty in calibrating the risk.

This dynamics makes the insurer's task of modelling risks considerably more complicated. Like Risk Managers and risk officers in companies, as well as security solution providers, insurers must keep learning and maintain a constant technological watch on new vulnerabilities and new forms of attacks on systems. The analysis of past incidents has only limited predictive value. The creation of forward-looking and disruptive scenarios is therefore crucial to this nascent market.

For the insurer, each of the difficulties given above is a hurdle to the development of the cyber market. However, as with the natural disaster, terrorism or environmental risk, the insurers' growing experience and the use of reinsurance in particular will enable them to steadily improve their offerings to companies.

(29) Idem.
(30) Swiss Re (2017), *Cyber: getting to grips with a complex risk*, Sigma No. 1/2017, p. 7.

II. Developments in the cyber insurance offering

The harmful consequences arising from cyber, accidental or malicious loss triggering events are only partly covered by the existing conventional contracts that were not designed for the largely digital economy that we have today. New contracts dedicated specifically to cyber risks were gradually developed to cover the harmful consequences that were not necessarily covered by conventional contracts.

A. A risk partly covered by conventional contracts

Before specific contracts came up, several harmful consequences of cyber risk were already covered by conventional insurance contracts (and still are, barring specific exclusions).

1. Property damage contracts

Whether they are caused by malicious intent or human error, cyber loss triggering events can lead to material damage. This is covered under the property damage contract.

This contract covers physical damage to the policyholder's property and the resulting operating losses, regardless of the cyber loss triggering event. In contrast, if the cyber loss triggering event did not cause material damage, the operating losses cannot be covered by this contract.

Focus – BTC Pipeline explosion in Turkey in August 2008

Facts

In August 2008, one portion of the BTC pipeline exploded in Turkey.

The explosion was triggered by a malicious cyber attack. The attackers intruded into the operating system of the refinery station, took over control and tampered with the pressure and flow rate calculations, causing the refinery station to explode. The station was out of service for three weeks[31] and the operator incurred huge financial losses.

Possible consequences to the property damage contract, had the cyber incident been insured in France

In this case, the material damage and the resulting operating losses could have been covered by the property damage insurance taken out by the operator.

2. Civil liability contracts

Civil liability contracts, by nature, cover bodily, material and non-material damage caused to third parties, whatever be their triggering event. They also cover the legal defence and appeal costs when the policyholder is the injured party. Civil liability losses resulting from a cyber loss triggering event due to malicious intent or human error will therefore be covered by these contracts.

For example, a personal data processing manager accused of invasion of privacy[32] following a personal data breach and disclosure due to a malicious act or an accident could be covered by his or her civil liability insurance contract.

(31) EURASIANET, *U.S. Intelligence : Russia Sabotaged BTC pipeline Ahead of 2008 Georgia War*, 10 Dec. 2014, [http://www.eurasianet.org/node/71291].
(32) Civil Code, Art. 9.

This also holds true for a company that suffers from a cyber attack that obliges it to stop production and suspend its deliveries. Due to the shortage of supplies, the company's clients may in turn be forced to stop production. They suffer harm for which the company that was hit by the cyber attack may be held liable. Such harm can be covered by the civil liability insurance contract of the company that suffered from the cyber attack.

Focus – Data theft in the Intercontinental Hotels Group, December 2016

Facts

A computer virus corrupted the servers of 1,200 hotels of the Intercontinental Hotels Group, in December 2016. The hackers were able to access payment card details of the hotels' customers. The customers concerned by the data theft were informed by the company, which had to bear the expenses. This malware was supposedly eradicated only in March 2017[33].

Possible consequences to the hotel owner's civil liability insurance contract, had the cyber incident been insured in France

- The customers of the hotels whose data had been stolen could have held the hotel group liable for invasion of privacy.
- Bank card issuers (Visa, MasterCard, etc.) needed to cancel the affected cards and issue new ones. They could claim the expenses involved from the hotel chain. The damage caused to third parties could have been covered under the hotel group's civil liability insurance contract unless specific exclusions had been laid down in the contract.

(33) Le JDD, *"Comment les entreprises se défendent face aux cyberattaques"*, 25 Apr. 2017 [http://www.lejdd.fr/economie/comment-les-entreprises-se-defendent-face-aux-cyberattaques-3310139].

3. The Director liability insurance contract

The Director liability insurance contract covers the court appearance costs, legal defence costs, and monetary consequences for any director of the company who is held personally liable to his or her company, its shareholders or partners, or to any third party (regulating authorities, creditors, employees, suppliers, etc.) due to non-compliance with the laws or regulations, breach of company by-laws, or management errors that, depending on the types of proceedings initiated against the person, could be a fault that is separable from his or her functions, or just wrongful negligence.

Following a cyber event, the directors may be held liable (for not considering the risk).

The insurance contracts that cover director liability could cover such triggering events.

4. Fraud contract

Fraud contracts have been around for a long time. They cover fraudulent acts such as misappropriation of funds, fraud, forgery or use of forged documents, counterfeiting and theft.

The harmful consequences of computer-assisted fraud are covered by the Fraud contracts and not by the cyber contracts. As an example, the false funds transfer orders issued after usurping identity (CEO fraud) fall with the scope of Fraud contracts exclusively, even though new technologies (false emails, identity theft, etc.) were used.

When the fraud is made easier by introducing malware in the computer system, the harmful consequences of this triggering event alone can be covered either by Fraud contracts or by cyber contracts.

B. Le développement de contrats spécifiques

The new risks that emerged with the progress made in new information and communication technologies and their increased use called for – and still call for – suitable legal frameworks to be adopted. In France, the 1978 consolidated data protection act[34] and the act governing military programming in the 2014-2019 period[35] have been updated with new requirements for companies whose non-performance or non-compliance are not covered by the conventional contracts (e.g.: notification duty, administrative inquiry).

These new risks led to the appearance of a new type of damage, such as breach of personal data of third parties and company data, or ensuing operating losses that are not covered by the conventional contracts.

To cope with these new risks, insurers have developed new services. More and more of them are entering into partnerships with companies providing advisory services and/or that develop cyber security solutions. These services can be grouped into four categories:

- Risk analyses
- Forensic, or search for causes
- Crisis management
- Bank monitoring cost cover

These new requirements in terms of guarantees and services led to the creation of a new contract, the cyber insurance contract.

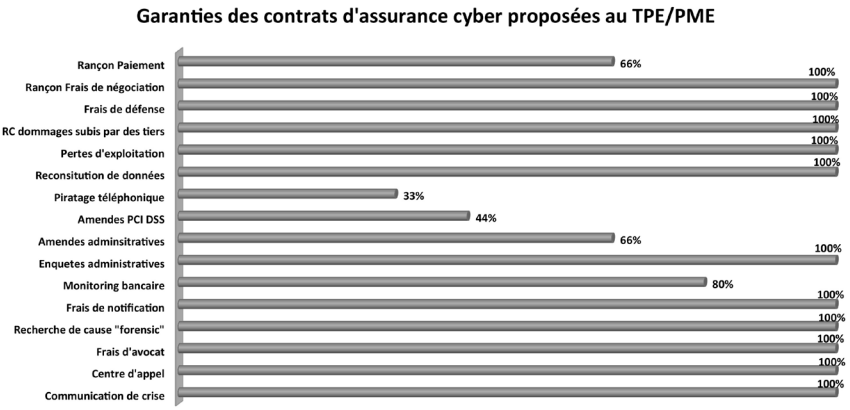
Cyber insurance contracts are often all-risk contracts: they cover damages (expenses and losses incurred) and civil liability (non-material damages to third parties), and include crisis handling services.

(34) *Loi relative à l'informatique, aux fichiers et aux libertés*, 6 Jan. 1978, No. 78-17.
(35) *Loi relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, 18 Dec. 2013, No. 2013-1168.

These contracts mostly offer the guarantees given below.

- Costs and losses incurred due to malicious intrusion (damage category):
  - Computer expert assessment costs (post-loss event forensics[36])
  - Incident and crisis management expenses (safeguarding brand image)
  - Data rebuilding costs
  - Infected system repair costs
  - Resulting operating losses (without material damage)
- Costs following breach of personal data:
  - Administrative inquiry costs
  - Notification costs
- Consequences of civil liability;
  - Damages caused to third parties due to the security default by the policyholder
  - Damages caused to third parties due to the failure to protect third party personal, banking or health data
  - Lawyers' fees
  - Appeal costs

(36) Search for the cause.



The percentages refer to the proportion of a representative sampling of insurers on the French cyber insurance market who offer this type of guarantee in their cyber insurance contracts for micro businesses and SMEs (source: FFA/2017).

Focus – The consequences on insurance of the consolidated data protection act No. 78-17 of 6 January 1978 and the military programming act No. 2013-1168 of 18 December 2013 for the 2014-2019 period

According to the laws on personal data protection and information system security, certain operators are duty-bound to notify a competent authority and/or third parties who are victims of a digital incident.

In connection with personal data protection, electronic communication service providers[37] must send this notification to CNIL (the French data protection commission) and to third parties whose personal data has been breached.

(37) *Loi relative à l'informatique, aux fichiers et aux libertés*, 6 January 1978, No. 78-17, Art. 34a.

Under the regulation governing information system security, operators of essential services[38] (OES) are required to make this notification to ANSSI[39] and to the Prime minister in case of an incident involving their information system.

These regulations also include ANSSI's supervisory power over the information systems of operators of essential services (OES)[40] and that of CNIL over personal data processing[41]. In case of an inquiry by one of these supervisory authorities, the operators must place their resources at their disposal.

The notification costs and the administrative inquiry costs are covered by contracts dedicated to cyber risk. When the stakeholders are implicated in a penal or administrative sanction procedure, they may incur legal defence costs that may also be covered in contracts dedicated to cyber risk.

Following these proceedings, the administrative authority can impose the payment of a fine on the company. In France, insuring these administrative files seems to be contrary to public policy (Articles 6 of the Civil Code, decree of 14 February 2012 of the Cour d'Appel de Paris). Also, the insurers/policyholders understand the regulation differently. Certain insurers therefore propose to cover administrative fines, solely to natural persons, within the framework of sub-limits, and "subject to their effective insurability", whereas others do not.

(38) *2014-2019 military programming act with provisions for defence and national security,* 18 December 2013, No. 2013-1168, Art. 22.
(39) French national agency for information system security (ANSSI).
(40) Idem.
(41) *Loi relative à l'informatique, aux fichiers et aux libertés*, 6 January 1978, No. 78-17, Art. 11.

C. Market capacity and current limits of available cover amounts

While the changes to conventional contracts and the development of contracts dedicated to cyber risk testify to the fact that insurers are taking cyber risk more into account, the capacity of the pure cyber insurance market internationally, and especially in France, remains limited to this day.

The maximum overall capacity that can be arranged for a single contract is estimated at US$500-700 million[42].

Considering the capacity delivered by certain insurers to be about US$75-100 million[43], the average capacity per insurer would be around US$25 million in 2015[44].

These levels may seem to be modest given the magnitude of the risk to which the companies are exposed. They must however be compared against the working capital that needs to be arranged by the insurers to cope with potential massive cyber attacks, and against the market's still-limited demand. For the micro business and SME segment, this unit capacity seems adequate.

For the large companies segment however, the demand for insurable capital, even prior to the regulatory changes that are expected to be made in 2018, is considerably higher than the supply.

(42) Marsh, *Benchmarking trends: interest in cyber insurance continues to climb,* April 2014. The level mentioned in this study is reported to have remained unchanged since.
(43) J. FINKLE., *Cyber insurance premiums rocket after high-profile attacks,* Reuters Technology News, 12 Oct. 2015 , [www.reuters.com/article/us-cybersecurity-insurance-insight- idUSKCN0S609M20151012.] ; Insurance Journal, *Munich Re, Beazley Partner to Provide Enhanced Cover for Large Cyber Risks,* 20 Apr. 2017, [http://www.insurancejournal.com/news/international/2017/04/20/448519.htm.] ; FAULKNER M., Munich Re Syndicate targets deeper cyber exposure, Insurance Day, 13 Apr. 2017, [www.insuranceday.com/ece_incoming/munich-re-syndicate-targets-deeper-cyber-exposure.htm.].
(44) Council of Insurance Agents & Brokers, *Cyber Insurance Market Watch Survey: Executive Summary,* Oct. 2015.

III. Cyber insurance demand still restrained

A. A changing market

The first "pure" cyber contracts emerged in the beginning of the 2000s in the United States and developed considerably owing to a regulatory change making it mandatory to notify of any breach of the concerned person/entity's personal data.

Focus – California Data Breach Act (2003)
and the cyber insurance market in the United States

In the early 2000s, the State of California was hit by a security incident that resulted in the disclosure of the salary information of over 200,000 public sector employees.

In the wake of this theft, the security breach notification requirement was introduced for the first time in California through the "Data Breach Notification Act" in 2003[45]. It requires businesses or public authorities to notify individuals of security breaches of their personal data.

As the costs of notification were very high, the economic stakeholders wanted to transfer the financial risk to insurers, which substantially accelerated the development of cyber insurance[46]. Several States followed suit, adopting similar laws.

The new legal framework for personal data protection and information system security established in May 2018 is expected to have a similar impact on the European cyber insurance market.

(45) K. D. HARRIS , *California data breach report,* Feb. 2016, [https://oag.ca.gov/breachreport2016].
(46) OECD, *Digital Economy Outlook*, 2015, p. 256.

Today, the worldwide cyber insurance market is worth US$3 billion to US$3.5 billion[47].

The American market accounts for 85% to 90% of the annual premiums[48]. The European market represents a mere 5% to 9%[49] of the world market, with a maximum premium amount of about €255 million ($US300 million[50]). The volume of premiums written in France was approximately €40 million in 2016[51].

The global penetration of cyber insurance is particularly complex to measure.

– In Europe, this market is gaining strength.

– §The few figures available generally depict only premiums written for dedicated cyber insurance contracts. Premiums for guarantees covering a cyber loss triggering event included in conventional contracts (damages and civil liability) are therefore not taken into account.

Going by the latest barometer for cyber security published by Orange Cyberdefense in January 2017:

- 73% of French industrial undertakings surveyed were not insured against the risks of cyber security failures at end-2016;
- 32% of them were planning to get insured against cyber risk within twelve months;
- 79% of companies with less than 250 employees and 60% of companies with over 250 employees[52] were not insured.

(47) Lloyd's, *Counting the Costs, Cyber Exposure Decoded*, Emerging Risk Report 2017, July 2017, p. 8.
(48) Aon Benfield, *Cyber update: 2016 cyber insurance profits and performance*, 2017 (this study also points out that the risk for the United States is shared between insurers in the United States, in Bermuda and in London); OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, 2017.
http://thoughtleadership.aonbenfield.com/Documents/20170504-ab-cyber-naic-supplemental-study.pdf.
(49) OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, 2017. This data that relates only to premiums on contracts dedicated to cyber risk is a result of the estimations from studies or surveys conducted by private sector companies. There is no official consolidation to date.
(50) Marsh, *Continental European Cyber Risk Survey: 2016 Report*, October 2016.
(51) L.THEVENIN, "*Le premier vrai test pour un marché de la cyberassurance en plein essor*", *Les Échos*, 15 May 2017, [https://www.lesechos.fr/finance-marches/banque-assurances/0212089405169-le-premier-vrai-test-pour-un-marche-de-la-cyberassurance-en-plein-essor-2086949.php#.].
(52) Orange Cyberdefense, *Baromètre cybersécurité 2017 – Où en est l'industrie française ?*, Jan. 2017, p. 15

These figures tally with the study conducted in April 2017[53] by Cigref[54] primarily with large companies, which found that only 43% of them were covered by cyber insurance.

The studies converge to show that major companies are now aware of cyber risk and the benefits of transferring that risk to insurance, whether or not by taking out a dedicated cyber policy. By contrast, this awareness is far from being widespread in micro businesses and SMEs. The smaller the size of the company, the less it is informed about the possibility of transferring this risk to an insurance contract.

B. Main hurdles to the growth of the demand

Apart from the hurdles to developing the cyber insurance supply mentioned in part 1.I, there are also various obstacles in expanding the demand.

1. Lack of technical and legal expertise prevents many economic shareholders from tackling cyber risk appropriately

Most companies, especially the smaller ones, still lack technical and legal skills even as they are going digital.

According to a recent study[55] on the United States, England, France, Germany, Australia, Japan, Mexico and Israel, over 80% of the surveyed companies, and 75% in France, criticised the lack of cyber security skills within their organisation; one third believes that due to this shortcoming, their organisations are perfect targets for hackers; a little less than a quarter consider that it is the cause for damage in terms of reputation and data loss following cyber attacks.

(53) Cybersecurity Insights, *How to unleash the French cyber insurance market?*, June 2017, p. 10.
(54) Cigref is an association founded in 1970 that brings together 140 major French companies and organisations. Its aim is to "enable large companies to develop and to leverage digital capabilities".
(55) Intel Security, in partnership with the Center for Strategic and International Studies (CSIS), *Hacking the Skills Shortage,* 2016.

Another study[56] that analysed the data relating to organisations based in North America and in the EMEA and Asia Pacific regions, concluded that 46% of the organisations surveyed in 2017 estimated that they had a "problematic shortage" of cyber security skills. The increase in this rate in two years is the most telling fact; only 28% has concluded to the fact in 2015, which probably proves that organisations are more aware of the risk at present but have still not upgraded their skills.

The shortage of technical skills in cyber risks is often coupled with the shortage of legal skills and monitoring. It hinders the understanding of the new requirements to be met by organisations and the compliance procedure. In this respect, the preparation for implementing the European regulation on data protection and that of the NIS directive are conspicuous barometers. 97% of European companies appear to have heard about the European regulation on personal data protection, but 57% of them know little or nothing of what it implies[57].

This shortage of skills is an obstacle to rolling out cyber security solutions adapted to the risk exposure. It also explains that many companies do not plan on taking out financial cover for cyber risk by transferring the risk to insurance as the case may be.

Regarding mid-caps and major companies, AMRAE has undertaken a major campaign to raise its members' awareness of this topic. AMRAE has developed risk analysis tools that will be described in a book dedicated to risk management and prevention/protection.

(56) ESG, ISSA, *Through the Eyes of Cyber Security Professionals: An Annual Research Report (Part II)*, 2017.
(57) Lloyd's, *Facing the cyber risk challenge*, 20 Sept. 2016, p. 5

2. Cyber risk underestimated

A vast majority of the companies continue to underestimate cyber risk. Although most of them are aware that the risk exists, they do not consider being necessarily exposed to it, as seen in the various studies. According to a study by PwC in 2016[58], "the risk of cyber criminality is still poorly understood by French companies today, regardless of their size (bearing in mind that over 99% of French companies are micro businesses and SMEs[59]): only 17% feel that they are exposed, and are mostly companies in the industrial sector". In December 2016, the firm Denjean & Associés noted that only 38% of French companies considered the risk of their facing a cyber attack to be high or very high[60].

In the micro business and SME segment in particular, most companies feel that there is little chance of their being hit by cyber incidents, especially when they outsource their information system maintenance and data hosting to providers without being aware of the risk issues associated with that choice. And yet, according to Symantec's 2016 Internet Security Report, they represent 77% of the victims of digital attacks in France.

3. Poor knowledge of insurance cover for cyber risks

As they underestimate their exposure to this difficult-to-understand risk, most economic stakeholders do not consider the option of transferring it to insurance.

What's more, many of them are still unaware that there are specific insurance contracts to protect themselves against cyber incidents. According to a study by Lloyd's[61], it would appear that 73% of the directors of European companies have only limited knowledge of cyber insurance, and 50% of them do not know of the existence of cyber risk guarantees against data leaks.

(58) PwC, *The cyber-insurance market: a revolution is underway*, Jan. 2016, p. 7.
(59) Insee, data for the year 2015 published on 6 October 2017; https://www.insee.fr/fr/statistiques/2016091.
(60) Denjean & Associés, *Les entreprises françaises face aux cyber-attaques*, Dec. 2016. p. 4.
(61) Lloyd's, *Facing the cyber risk challenge*, 20 Sept. 2016, p. 5

Several companies also know little about the scope of cyber cover, dispersed across different types of contracts (see II), which is a major impediment for taking out insurance, in many ways.

- The complexity of cyber cover due to the increasing number of policies, their likelihood of overlapping, their restrictions and exclusions, in addition to the technicality of the risk itself and its consequences for the company, may deter certain companies from taking out insurance even though they are unsure of the extent of their guarantee, limits and deductibles.
- The difficulty in comparing the offers of the different providers is an additional obstacle to taking out insurance. In the context of fast-evolving risk and insurance offers, the terms and conditions of cyber insurance policies vary substantially. The definition of the key cover components itself may vary: "computer system" may or may not include the systems of a data manager on the cloud, for example.
- Besides, as the scope of cover of their contracts is not clearly defined as regards cyber risks, many companies mistakenly believe that they are protected against all the harmful consequences of the cyber risk, and do not feel the need to take a dedicated contract or extend their conventional contracts. Yet, the New York Supreme Court's decision in this matter, and notably on Sony's claim for damages, should prompt them to exercise caution and conduct detailed audits of cyber cover to avoid becoming aware of the loopholes in the cover only after a massive attack has occurred.

Focus – Lessons from the Sony case law

In 2011, Sony PlayStation Network suffered a major hack: data on 80 million users had been stolen.

Following the attack, Sony had filed a claim against its insurers, under its civil liability insurance, to reimburse the amounts disbursed to comply with the notification requirement. Sony initiated proceedings when the insurers refused to cover the loss.

In the end, the New York Supreme Court rejected the claim for damages filed by Sony Corporation against its insurance companies under its civil liability insurance – it ruled that the civil liability insurance did not cover the personal harm or publication-related harm resulting from the personal data theft by the hackers. The company that had fallen victim to hackers therefore had no cover against cyber attack.

The Court considered that notification costs were not covered by conventional contracts, whether property damage or civil liability.

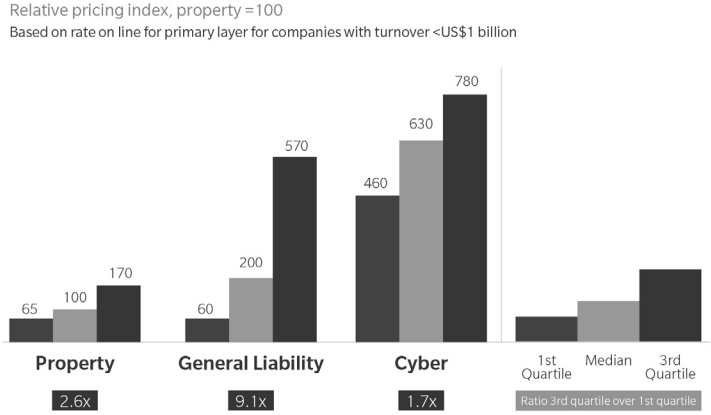
A standard exclusion of civil liability contracts has since been adopted in the United States to clarify the scope of cover and avoid other companies' going through the same experience as Sony.

4. Premiums inadequately correlated to the risk

As with all nascent markets, risk quantification is fraught with uncertainties: lack of loss statistics, poor technical knowledge of risk vulnerability, lack of proven knowledge as regards prevention and protection, etc.

The difficulties in quantifying risk lead to limited price segmentation. A report by Marsh, in 2015[62], highlighted the fact that the differences in premiums in the cyber branch were small compared to the property damage and the civil liability branches.

Focus – Analysis of premiums for cyber, property and the civil liability insurance contracts



Source: UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk – Marsh 2015

The measures taken by the policyholders and prospects to step up their digital security may not be adequately factored into the premiums[63].

(62) Marsh, *UK cybersecurity, the role of insurance in managing and mitigating the risk,* Marsh 2015, p. 22.
(63) O. BOGOMOLNIY, *Cyber Insurance Conundrum: Using CIS Critical Security Controls for Underwriting Cyber Risk*, published by The SANS Institute, 2017, p. 8.

Price adjustments can be made through deductibles, limits and loading.

As a result, the premium payable based on the assessment of the cover is often mentioned as one of the main obstacles to taking out cyber insurance[64].

(64) See for example PwC, *Insurance 2020 & beyond, Reaping the dividends of cyber resilience,* 2015, p. 11:
"Many insurers are also setting limits below the levels sought by their clients (the maximum is $500 million, though most large companies have difficulty securing more than $300. Insurers may also impose restrictive exclusions and conditions. Some common conditions, such as state-of-the-art data encryption or 100% updated security patch clauses, are difficult for any business to maintain. Given the high cost of coverage, the limits imposed, the tight attaching terms and conditions and the restrictions on whether policyholders can claim, many policyholders are questioning whether their cyber insurance policies are delivering real value."

PART 2
Optimising the insurance offering to respond to recent developments in the legal and market environment

For several months now, a combination of factors has contributed to creating an environment conducive to the development of cyber risk coverage. The various players concerned now need to take this dynamic into account and develop less complex and more flexible insurance products, meet a demand that is expected to grow rapidly, and contribute to making the national economy more resilient to the expanding cyber risk.

I. A new economic and regulatory environment that is favourable to cyber risk coverage...

We can identify four main drivers of the demand for financial protection against cyber risk: awareness of the risk that has risen over the past months, a change in the civil liability structure in France, the homogenisation of the European legal framework, and the call to increasingly account for cyber risk in corporate governance. Additionally, the works on harmonising the definitions and the categorisations of cyber risks, and, in France, the clarification of the scope of the cover by Gareat in the case of cyber terrorism, have also removed some of the obstacles to the development of cyber insurance.

A. Increased awareness of the risk

Despite the insurance rates that still remain low, notably in the case of micro businesses, SMEs and local government bodies, recent indicators point to the increased awareness of cyber risk. This is illustrated in the fact that in 64% of the companies with less than 250 employees, investment in cyber security may have increased in the past twelve months[65].

The recent cascade of major cyber incidents has definitely helped to step up awareness of this risk. Four aspects of recent attacks have made several stakeholders realise the IT firms or the players in economy 2.0 (Internet service providers, IT start-ups, ISS, etc.) were not the only potential victims, and that it was useful, or even crucial, for many companies to set up technical and financial protection (a great number of micro businesses and SMEs do not survive a cyber attack).

- The broad spectrum of the players affected – as an example, the WannaCry attack hit institutions of very different origins, all over the world; NHS hospitals in the UK, the American shipping company FedEx, the Russian home ministry, the Spanish telecom operator Telefónica, the railway company Deutsche Bahn, etc.
- The costs incurred by the victims – Maersk, for example, announced an estimated cost mid-August that could reach €300 million[66], a large portion of which was due to interruption of business.
- The concerted reaction of certain victims – Considering that Equifax had not adequately protected their data, several of its clients (individuals, companies and federal states) filed a complaint against the company. Collective procedures are considered, among the biggest of its kind in American history as regards the number of people concerned[67].
- The wide media coverage of the events.

(65) Orange Cyberdefense, Baromètre cybersécurité 2017 – *Où en est l'industrie française ?*, Jan. 2017, p. 17.
(66) Zdnet, Ransomware Petya : *un colis à 300 millions de dollars pour Maersk*, 17 August 2017, [www.zdnet.fr/actualites/ransomware-petya-un-colis-a-300-millions-de-dollars-pour-maersk-39856172.htm].
(67) *L'Express, L'Expansion*, "Equifax : enquête du régulateur américain du commerce après le piratage", 14 Sept. 2017, [http://lexpansion.lexpress.fr/actualites/1/actualite-economique/equifax-enquete-du-regulateur-americain-du-commerce-apres-le-piratage_1943639.html].

The recent rise in awareness owes a lot to the awareness-raising campaigns by companies, local governments and associations, conducted by players specialised in cyber risk, such as ANSSI, AMRAE, professional federations, as well as ISPs and consulting firms specialising in cyber risk. These initiatives notably include:

- The computer hygiene guide *Guide d'hygiène informatique*, published in 2017 by ANSSI[68] that proposes 42 measures to guide information system security managers;
- The ACYMA platform "cybermalveillance.gouv.fr" (launched on 30 March 2017 by a public interest group of the same name), to provide assistance to victims of malicious cyber acts, and educate the general public about the stake involved in the security and protection of privacy;
- The "SECNUMACADEMIE" MOOC security training platform run by ANSSI, that is open to all at no charge;
- FFA's awareness-raising guide for micro businesses and SMEs to anticipate and minimise the impact of cyber risk *"Anticiper et minimiser l'impact d'un cyber-risque sur votre entreprise : TPE, PME, vous êtes concernées !"*, published in May 2017;
- Dedicated works and contributions by AMRAE:
  - > Cyber-risk help tool for analysis and insurance handling[69],
  - > Management of digital risk in the company[70],

(68) ANSSI, *Guide d'hygiène informatique,* [https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/].
(69) AMRAE, *Cyber-risques : outil d'aide à l'analyse et au traitement assurantiel,* technical workbook, March 2015 [http://www.amrae.fr/cyber-risques-outil-daide-%C3%A0-lanalyse-et-au-traitement-assurantiel].
(70) AMRAE, *La gestion du risque numérique en entreprise,* February 2014 [http://www.amrae.fr/la-gestion-du-risque-num%C3%A9rique-dans-lentreprise], "Dialoguer AMRAE" collection, updated in January 2018.

> The white paper *"Cyber risk governance throughout the value chain and its transfer to the insurance market"*[71],

> The cyber risk governance report published jointly[72] by FERMA[73] and ECIIA[74].

These cyber risk awareness-raising initiatives are directed at all tiers of the company, including the senior management that must ensure that the prevention measures binding upon all the employees are complied with by one and all, regardless of their position in the company, and by itself.

B. Broader scope of duties and responsibility of companies

The new pan European liability law system governing the personal data protection and information system security that came into force in May 2018, potentially leads to a sizeable increase in cyber attack costs for companies. This is likely to prompt companies to take out cyber risk insurance policies that not only cover the incident notification costs (this requirement has become more stringent) but also the company's being held accountable by victims (which is likely to become more frequent).

1. The notification requirement

The notification requirement has been generalised as regards the breach of personal data, and the scope of application of the notification requirement as regards information system security incidents has been extended. This should have a dual impact on the insurance business.

(71) System X working group, [http://www.irt-systemx.fr/v2/wp-content/uploads/2016/11/ISX-IC-EIC-transfert-risque-LIV-0401-v10_2016-10-25.pdf].
(72) *Cyber Risk Governance report* [http://www.ferma.eu/exclusive-ferma-eciia-cyber-risk-governance-report-available?type=advocacy].
(73) Federation of European Risk Management Associations (FERMA).
(74) European Confederation of Institutes of Internal Auditing (ECIIA).

a. *The expected increase in notification costs and the extension of civil liability of companies*

At present, the notification requirement for victims of a cyber incident in which data or information system security is breached, is limited to critical service operators in case of incidents affecting the working or the security of information systems[75], and to electronic communication service providers in the event of a personal data breach[76].

As from 25 May 2018, this notification requirement will be extended to all companies engaged in the data processing business[77].

The requirement to notify about information system security incidents will apply not only to critical service operators (OVI) but also essential service operators and digital service providers[78].

(75) *Loi no 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale,* Art. 22.
(76) *Loi relative à l'informatique, aux fichiers et aux libertés,* 6 Jan. 1978, No. 78-17, Art. 34a.
(77) *Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general regulation on the protection of data),* 27 April 2016, 2016/679.
(78) *Directive (EU) of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union,* 6 July 2016, 2016/1148, Art. 14, Art. 16.

Notification of incidents under the NIS Directive[79]
Directive on the security of networks and information systems, known as the "NIS Directive – Network and Information Security"

As with the military programming act or the general regulation on data protection, the NIS Directive (Article 14) stipulates that all operators of essential services (OES) are required to notify the national authority of incidents having an impact on the continuity of their essential services.

In the case of digital service providers, Article 16 of the Directive expressly states that the notification requirement will be applicable only if the digital service provider has access to the information necessary to assess the impact of the incident considering, in particular, the following parameters:

- the number of users affected by the incident, in particular those that use the service to provide their own services
- the duration of the incident
- the geographical reach, as regards the zone affected by the incident
- the severity of the disruption of the service provision
- the extent of the impact on economic and societal functions

For operators of essential services and digital service providers alike, the notification to the general public is limited to cases where it is in public interest to disclose the incident.

As with requirements in security matters, these stipulations are not applicable to micro businesses and small companies.

(79) *Directive (EU) of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union,* 6 July 2016, 2016/1148, Art. 14, Art. 16.

The notification costs incurred to inform third parties of a personal data breach comprise several expense items, notably the IT costs of updating databases, ensuring compliance with regulatory requirements, recruiting external experts, postal expenses, configuring alternative contact information for notifying by mail, and of handling return emails and incoming communication.The potentially extremely high amount of these expenses provides a strong incentive to take out cyber insurance to transfer the risk to the insurer.

Besides, before the data breach notification requirement was generalised, the victims did not know that their data has been disclosed and could not hold a company that was hit by an attack accountable.

As of May 2018, when the notifications will clearly mention the nature of the breached data, it will be easier for the third party victims, once they know of the breach, to hold the company hit by the attack liable and demand compensation for the harm suffered by them. There should be an increased demand for civil liability insurance contracts.

b. Enhancement of databases with cyber incidents and their handling

With the notification requirement and the possible transfer of its implementation expenses to the insurer, the number of claims registered and losses paid is likely to increase. The insurer's databases should therefore become more exhaustive. Collaboration in this matter between the data protection agency CNIL – that records the notifications – and the insurer – that bears the associated compensation – could substantially improve the understanding and handling of cyber risk, provided that the incidents to report are defined and calibrated accurately.

The expanding portfolio of policyholders should enable better segmentation of the insured companies by their size and business sector, a better understanding of the loss events and more accurate correlation with prevention and protection measures, as well as a pricing procedure that is better adjusted to the reality of the risk (see below). All of these factors will contribute to the optimised management of this risk by insurers

and reinsurers, and allow them to propose a more sophisticated product offering to companies.

2. Heightened risk of companies' incurring liability

The European regulation on personal data protection that will enter into effect on 25 May 2018 marks a change in the framework applicable to personal data processing.

This text is based on the accountability of the players in their personal data processing business. In France, this means that the formalities preceding data processing will be replaced by more stringent mechanisms for checking and determining the accountability of those in charge of the processing.

a. Civil liability

By stepping up the requirements to be fulfilled by the persons in charge of data processing, the European regulation on personal data protection will increase the risk of civil liability claims against the company following a cyber event. As regards its contractual relations, its risk exposure can be all the higher as the cyber loss triggering event is likely to cascade damages to several players along the full length of the value chain (e.g. production line shutdown, no production, no product delivery, abrupt termination of business relationships, etc.).

This reinforcement of the mechanisms of processors' accountability has a direct incidence on civil liability insurance contracts. They compensate the monetary consequences of accountability claims made by third parties against the victims of a digital incident, barring specific exclusions set down in the contract.

b. Director liability

The accountability system taken from the European General Data Protection Regulation (GDPR) that will become effective as of 25 May 2018 and the heavy sanctions imposed by the regulating authorities (notably CNIL) – that could reach €20 million or 4% of the world revenue, where the higher value is applied – in case of failure by processors to notify of personal data breaches will probably urge companies to invest:

- in prevention, by integrating security measures in their information systems
- in protection, by taking cyber risk insurance cover

Failure to do so could be considered as a management fault entailing the accountability of the director of the company hit by a cyber incident, especially if the incident has a significant impact on the company's earnings or its continuity.

Focus – Status of the proceedings against the Management of the supermarket chain, Target

The 2013 theft of 110 million items of personal data (including bank information) of the customers of the supermarket chain "Target" led to over 80 legal proceedings and class actions, including against its Management.

According to the latest assessment announced by the insurer in charge of covering the Management's civil liability, at October 2017, the cost of these claims stood at US$65 million towards legal defence and investigation.

Besides, the entry into force of Law 2017-399 of 27 March 2017 related to due diligence of the parent companies and main contractor companies imposes upon these companies to supervise their subcontractors more closely, especially in matters of cyber risk.

Articles L. 225-102-4 and 5 of the Commercial Code has now established the requirement to set up an effective watch plan that includes measures to help "*identify the risks and prevent serious abuse of human rights and fundamental freedoms, health and safety of persons, and the environment, arising from the operations of the company or by the companies over which it has control (…), as well as the operations of subcontractors or suppliers with which it has established business relations"*.

Although this requirement is currently imposed on companies that employ over 5,000 persons with its registered office in France, or that employ over 10,000 with its registered office in France or abroad, the extensive due diligence procedures (including, in particular, the protection of personal data, the protection of systems against cyber risks, etc.) will be difficult to implement over such a broad scope, with the understanding that:

- the concept of control is defined by Article L. 233-16 of the Commercial Code, that includes not only the holding of the majority of voting rights and the appointment of the majority of the members of the management boards, but also the right to exercise dominant influence on a company by virtue of a contract or a statutory clause;
- the concept of subcontracting is defined by Article 1 of the Law 75-1334 of 31 December 1975 as the "operation whereby a contractor entrusts, under a subcontract under its responsibility, to another party termed subcontractor, the performance of all or a part of the public contract signed with the project owner";
- To determine whether or not a business relationship can be qualified as established, case law takes several criteria into account, such as the duration of the relationship between the partners, the continuity of that relationship or the volume and growth in earnings. A series of one-off contracts may suffice to characterise an established business relationship, provided that it is sizeable, regular and stable.

Should they fail to identify, prevent and implement all measures needed to avoid or limit the impact of such loss (through dedicated insurance, notably), company directors may be held liable for not fulfilling their duties of verification, supervision and compliance with laws and regulations. This threat may lead to an increased interest in cyber loss insurance and director liability insurance of the companies that fall under the new system.

3. Expected Europe-wide standardisation of the legal framework

The increasingly paperless exchanges and operations between Member States have sparked several questions regarding the law applicable to personal data protection and information system security.

The new legal environment to be set up in May 2018 through the NIS Directive and the General Data Protection Regulation GDPR, provides a unified applicable legal framework.

- Article 1 of the NIS Directive states that its scope of application extends to all the Member States of the Union.
- Article 3 subparagraph 1 of the regulation states that it is applicable to all "processing of personal data in the context of the activities of an establishment, of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not".
- Subparagraph 2 of the same article extends the scope of application of the regulation on personal data protection to controllers or processors not established in the Union[80]. This extension protects private persons from the practices of operators making use of personal data from abroad.

(80) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general regulation on the protection of data), Art. 3.

This unification is a component that supports the implementation of cyber insurance that extends beyond the borders to cover "deterritorialised" loss events. Besides, it simplifies the practices of insurers who will have only one legal framework to comply with.

Focus – The incidence of GDPR on collective actions in data protection

Collective action made its *début* in French law in 2014[81]. Referred to as "representation of data subjects" in Article 80 of the European regulation on the protection of data, this new practice is a true challenge for the development of cyber risk insurance. This article notably provides the right to representation in order to obtain compensation referred to in Article 82 of the Regulation.

Article 80 of the Regulation however stipulates that the right to obtain compensation by representation can be exercised only if it is provided for by the laws of a Member State.

In 2016, the law to modernise justice, inserted the collective action in matters of data protection in Article 43c of the 1978 information technology and civil liberties law. Such action may be initiated for the sole purpose of stopping non-compliance with data protection rules and not to obtain compensation.

In the present state of the law, collective action for personal data protection does not provide for claiming compensation for the harm suffered. A company can however be faced with individual actions for compensation that will be made easier by a ruling against it in a collective action.

(81) See Chapter 1.

C. Accounting for cyber risk – a criterion of good governance of the company

Cyber risk handling is increasingly considered as an indicator of good corporate governance, and no longer a technical aspect to be handled by the IT department alone.

FERMA[82] and ECIIA[83] pooled their efforts to produce a joint report with recommendations for setting up this good governance in organisations. This report advocates the creation of a cyber risk governance group chaired by a Risk Manager, which will bring together key business and security representatives, from the first and second lines of defence, as described in the ERM standard[84].

This group could be entrusted with the task of quantifying the company's exposure to cyber risk in financial terms and of making suitable remediation proposals. With this approach, the Management will have a clear view of the company's exposure to cyber risk in its technical, legal and business dimensions, and can also allocate the company's resources dedicated to prevention as part of a comprehensive risk handling plan[85].

(82) Federation of European Risk Management Associations (FERMA).
(83) European Confederation of Institutes of Internal Auditing (ECIIA).
(84) Enterprise Risk Management (ERM).
(85) See Prevention book, to be published.

Focus – Assessment of cyber risk in credit analysis:
Moody's point of view

Cyber risk or the growing importance of this parameter in credit analysis

Cyber risk covers a broad spectrum of threats, from denial of service attacks on the Internet to data theft, with disruption of essential infrastructure services placed somewhere in between. It is difficult to assess the capacity of a debt issuing entity (issuer) to react to cyber risk given that this risk is complex and changes very quickly. Besides, there is very little public information as regards both cyber security measures and cyber events. When such information is available, no comparison can be made between the issuers. We consider massive cyber event risk in the same way as we deal with risk of storms or natural disaster, as we cannot accurately state at which point in time it is likely to occur, and because it is difficult to determine the consequences of a successful attack. In a previous report *(Cyber risk of growing importance to credit analysis, November 2015)*, we studied how our credit analysis integrated the fast changes in cyber risk in a certain number of business sectors.

The manner in which we include the risk in our analyses and ratings depends on how severe the cyber threat is and how long it lasts. In other terms, the risk of a cyber attack is not explicitly considered in our credit analysis as a main rating factor. However, for all business sectors, our analysis includes several stress test scenarios, and a cyber event, just as other exceptional events, could act as a trigger for these scenarios. The severity and timespan of a "successful" cyber event would be essential to determine the incidence it may have on the issuers' credit quality.

Cyber risks vary from one business sector to another. Sectors in which huge volumes of personal data are concentrated mostly face threats of attacks involving large-scale data theft, which are likely to lead to severe damage in terms of reputation and financial impact. The sectors exposed to these risks include financial institutions and intermediaries, health institutions, higher education institutions, social networks and retail. Infrastructure sectors that are considered to be essential face a cyber risk of a different nature, leading to the prolonged interruption of the concerned services. More broadly, this is likely to have economic and social repercussions that can put States and local government authorities in a difficult position. The sectors that are most exposed to these risks notably include the telecommunications and chemical industries, the transport sector, banking services, as well as public utility services.

Cyber-risk intensifies as Internet connectivity expands. Internet connectivity – an entry point for computer hackers – is fast expanding to include new products, devices and services, such as in the car industry, water pumps and home heating systems. The expansion of this new Internet development phase called the Internet Of Things, to more products and more devices opens up new markets. As a result, cyber risk will surely become more prevalent, and we will need to increasingly prioritise this parameter in our assessments and credit analyses.

Companies and institutions are reinforcing their governance and increasing their outlay for computer security, even though spending more is no guarantee of absolute reliability. In all sectors of activity, cyber risk is taking greater priority in terms of governance. Executive board members are stepping up their cyber security expertise, and we expect that large numbers of these issuers will set up sub-committees dedicated to computer security, which we consider to be a positive factor for their credit quality.

Infrastructure services that are termed essential will avail of exceptional measures by governments. A successful large-scale cyber attack on essential infrastructure services or assets will, in our opinion, prompt governments to take action. This may be an exceptional action to stabilise a regional economy, or restore civil liberties. In the United States, the US Department of Homeland Security defines the following as essential infrastructure sectors: water supply and sanitation, energy, emergency services, financial services, healthcare, communication systems, information technologies, transport, nuclear, chemicals and government buildings.

In this context, by opting for cyber insurance, the company demonstrates that it has taken this risk into account, which is a mark of good governance.

D. Towards the standardisation of cyber risk definitions and categorisations?

In order to dispel any misunderstandings arising from the various covers involved in transferring cyber risk to insurance, it is essential to clarify the definitions of cyber risk for each market segment.

In Europe, an undertaking of this type was initiated by:

- The Cambridge Centre for Risk Studies[86] as part of a private and public sector production partnership, in which the University of Cambridge was involved, to produce median definitions that are common to all the parties participating in the partnership;

(86) Cambridge Center for Risk Studies, Cyber Accumulation Risk *Management, Managing cyber insurance accumulation risk,* fev. 2016.

– The CRO Forum[87] that brings together the Chief Risk Officers of major European insurance and reinsurance firms; in June 2016, it also published a report proposing a methodology for categorising cyber risks[88]; the proposed methodology provides a common working base (still being built) for cyber incidents.

E. Clarification of the cover by GAREAT in France in case of cyber terrorist acts

Certain cyber loss triggering events may constitute terrorist acts.

In France, the Penal Code took note of this reality in Article 421-1 by adding *"computer offences, as defined under Book III of the present Code"* as acts of terrorism.

To be qualified as such, the offences must be committed *"intentionally in connection with an individual or collective undertaking the purpose of which is to seriously disturb public order through intimidation or terror"*.

To cover the material damage resulting from a terrorist act, the French market set up a co-reassurance pool called GAREAT.

(87) CRO FORUM est un groupe réunissant les risk managers du marché de l'assurance.
(88) CRO Forum, *Concept Paper on a proposed categorisation methodology for cyber risk*, juin 2016, [https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf].

Focus – The GAREAT

The law of 9 September 1986 requires that insurers include terrorism cover in their property insurance policies. Following the 11 September 2001 attacks in the United States and fearing fresh attacks on French soil, in the context of the collapsing reinsurance capacity of the industry, a private and public sector partnership founded a co-reinsurance pool with unlimited guarantee from the State backed by the Caisse Centrale de Réassurance (CCR) beyond a given threshold[89].

GAREAT is a market structure that was founded in end-2001. It manages the reinsurance of the risks of terrorist attacks and acts[90].

Article L 126-2 of the Insurance Code sets down the principle of mandatory cover of risks of terrorist origin in property damage insurance. However, this guarantee covers only material damage and the immaterial damage that results from it (such as operating loss), suffered in France by assets located in the national territory and covered by an insurance contract that guarantees against fire damage, and damage to the body of motorised land vehicles.

GAREAT is a reinsurance pool. Its limits of action are enforceable only to member insurers who transfer the risks to it. The guarantees given to the policyholders are defined only in their policies.

Does GAREAT get involved in case of damages caused by an act of cyber terrorism?

There are three distinct situations.

(89) AMRAE, GAREAT Technical Note, [http://amrae.fr/sites/default/files/fichiers_upload/GAREAT%20Note%20technique_AMRAE.pdf].
(90) GAREAT: Who are we? [http://www.gareat.com] (consulted on 10 May 2017).

– The cyber event generates direct damages.
In this case, GAREAT will cover the damages.
Example: malware affecting the safety system of an industrial process which causes a fire and operating loss.

– The cyber event generates operating loss without direct damages.
In this case, GAREAT will not be involved, even if the asset affected by the attack is covered against fire damage.
Example: in case of a distributed denial of service attack (DDOS) on a computer network, there is a potential operating loss and expenses exposure, but no direct material damage.

– The cyber event generates a data breach.
The circumstances are more complex in the case of a data breach. When the information system covered by a fire policy is affected by illegal access, loss, theft or corruption of data, can the material damage be transferred to GAREAT or is this purely non-material damage that cannot be transferred?

In response to this question, GAREAT considers that according to the framework given by Article L. 126-2, one must go beyond just data loss and take a look at the information medium (hardware, memory, hard disk, USB stick, etc.) on which this data was located, and which firstly must be covered by a fire insurance guarantee. It identifies three situations.

If the medium is irremediably corrupted and technically beyond repair: this is a case of breach of the structure of the insured medium which has definitely suffered from material damage. GAREAT covers the damage to the medium and the resulting expenses, including the cost of recovering the data on the terms and within the limits provided for by the contract.

If the medium can be repaired from the technical standpoint: the structure of the medium is not damaged; there is no material damage. The fees to put the medium back into use and to recover the affected data constitute an immaterial damage that is not consecutive and will not be covered by GAREAT.

As a result, GAREAT modified its internal rules of procedure as of 2017 and clarified at that juncture, the limits of its cover against cyber terrorism

by redrafting its specific exclusion for the consequences of cyber terrorist acts other than material damages, resulting expenses and resulting operating loss covered legally by the insurers pursuant to Article L. 126-2 of the Insurance Code. Article 9 subpara. 3 and Article 14 subpara. 3 of the GAREAT's 2017 internal rules of procedure give an indicative list of the contracts and guarantees that are excluded or that do not fall under the scope of application of the major risk and the low and moderate risk section. The following are excluded, notably:

"Non-consecutive non-material damages caused by acts of cyber terrorism defined by Article 421-1 point 2 and Articles 323-1 to 323-8 of the Penal Code, in particular those caused by malware, viruses and cryptolockers, by hacks and attacks on the information system and attacks through denial of service, as well as by data theft. The consequences of an attack on data alone or their loss or their inaccessibility, and leading to the technically irreversible changes to the information medium, are also excluded."

Therefore, the cyber insurance contracts that do not guarantee against damages to the structure of the medium are not included in the reinsurance transfer to the GAREAT pool.

II. … which calls for an appropriate insurance response

At present, to take advantage of this new context and to support the efforts made by the industry to reduce the cyber threat, public authorities and institutional investors have a role to play.

The French and European public investment plans should promote the development of a French and European chain of excellence in the area of cyber protection. Also, the institutional investors, including insurers, could integrate the need to reduce cyber risk in their asset allocation policies. The support for leading-edge projects in the cyber protection chain seems particularly consistent from this standpoint.

Moreover, the insurance offering needs to evolve, so as to give new impetus to the cyber insurance market, especially in France. For all the reasons

mentioned in the previous chapter, the projected change in the cyber insurance market expects price hikes for premiums written in the coming years. The cyber insurance should increase two-fold in the United States[91] and triple in Europe by 2018[92].

This growth should go hand in hand with a clarified cyber offering, a broader service offering to assist policyholders, and optimised risk pricing and controlled accumulation (which impacts the decision to take cover), that should become easier as the statistical databases get larger.

A. Clarify the scope and junctions of the cover

As cyber risks increased, the question as to whether "conventional" property damage and civil liability contracts covered these new risks, even though this was not explicitly mentioned in them, became more and more crucial: this is the "silent cover" issue.

Silent cover refers to the coverage of cyber-initiated triggering events by existing conventional contracts:

- without being identified as such;
- without being accounted for in the pricing of the conventional contracts by the insurer.

To clarify the cover, the junctions between conventional contracts and dedicated cyber insurance contracts must be spelt out. For insurers, there is a dual stake in clarifying the scope and the junctions of cyber cover:

- assist the large number of companies, micro businesses and SMEs in particular, that often shy of taking cyber insurance due to the complex and opaque nature of cyber cover dispersed across several types of insurance contracts (see 1.III.B.);
- better quantify their own commitments and accumulations by removing uncertainties arising from silent cover that must be clarified.

(91) PwC, *Insurance 2020 & beyond: Reaping the dividends of cyber resilience,* 2015.
(92) Insurance Information Institute, *Cyber risk: threat and opportunity, Insurance Information Institute, New York,* 2015.

With these aims in mind, and to start discussions about the changes in the different types of cyber risk cover in the medium and the long term, several initiatives were taken recently to analyse all of the cover that could be impacted following a claim for compensation. The IRT System X[93] partnered with the French insurance federation FFA, FERMA and AMRAE to develop a matrix to cross-reference the triggering events and the cyber insurance cover (conventional or cyber-dedicated) in order to have a clearer view of the junctions between the guarantees called up to cover the risk. This work highlights the triggering events that can be covered by different types of policies, as well as the triggering events that are not covered by insurance.

FFA is heading a study of the French market to clarify the junctions between the cover by the different contracts concerned (property damage, civil liability and cyber loss). This work on the silent cover will enable:

- insurers and reinsurers to better manage their accumulated commitments
- their clients to have a better understanding of the different covers that can be called up to cover the risk

By way of comparison, the insert below shows what the London market did to address these issues and undertake the task of clarifying the scope of cyber coverage, through four initiatives.

(93) IRT System X, *"Cyber risk governance throughout the value chain and its transfer to the insurance market,* 2016, [http://www.irt-systemx.fr/publications-archives/english-la-maitrise-du-risque-cyber-sur-lensemble-de-la-chaine-de-sa-valeur-et-son-transfert-vers-lassurance/]. See the Appendix (on the site).

Focus – Definition and junction of cover types:
the British study

I) Lloyd's cyber strategy: oversee the cyber activity of syndicates

Right from 2015, Lloyd's set up a "Lloyd's Cyber-Attack Strategy[94]" whose aim is to enable the monitoring and oversight of cyber insurance underwriting by British insurance syndicates.

For this, in the first stage, the syndicates were asked to detail their mechanisms for handling cyber risk, their understanding of this risk and the factors they considered when underwriting and calculating the premiums.

In the second stage, they were asked to determine their risk level and analyse potential accumulations. To do so, the syndicates need to develop three likely worst-case cyber attack scenarios to calculate the aggregated exposure of their various covers, should the scenario actually take place.

These scenarios must also identify the typology of the policies that can be involved (conventional policies and specific policies) and the assumptions of potential "silent cover".

Lastly, the syndicates must show Lloyd's before 31 December 2017 that they have addressed the issue and have taken measures accordingly.

(94) Lloyd's, *Cyber-Attack Strategy*, June 2016.

II) Action of the British regulation authority

The Prudential Regulation Authority (PRA) also published a consultation paper in November 2016, for which insurers had to identify, quantify and manage cyber risks covered by their contracts[95]. A letter was sent to insurance firms to raise awareness about this topic[96]. They were given time until 14 February 2017 to respond to it.

On 5 July 2017, PRA published a "supervisory statement[97]" in which it stated its expectations for insurance firms based on the feedback from the British market through the consultation.

PRA's expectations relate to three aspects.

"Non-affirmative cyber-risk" the new term for "silent cyber risk").

PRA does not intervene in regulating the price and the content of the products. It merely ascertains that the insurance firms are fully familiar with the risk they cover and have sufficient reserves and own funds to guarantee their solvency.

The firms must therefore identify the policies that can cover cyber risk. They are expected to adjust their premiums accordingly, and add firm exclusions and limitations to the associated cover.

Where no exclusions have been added, and the firm has not voluntarily adjusted its premiums, PRA will verify that this move was approved by the senior management of the firm. The contracts must be redrafted to clearly state that cyber risk cover is included in the product.

(95) PRA, *Cyber insurance underwriting risk, consultation paper,* CP39/13, Nov. 2016. [http://www.bankofengland.co.uk/pra/Documents/publications/cp/2016/cp3916.pdf].
(96) PRA, *Cyber underwriting risk, letter,* 14 Nov. 2016 -http://www.bankofengland.co.uk/pra/Documents/about/letter141116.pdf.
(97) PRA, *Cyber insurance underwriting risk, supervisory statement,* SS4/17, July. 2017, [http://www.bankofengland.co.uk/pra/Documents/publications/ss/2017/ss417.pdf].

Cyber risk strategy and risk appetite

The firms must define a clear cyber strategy that is approved by their management bodies. This strategy must establish the junction between the different commitments, manage silent cover, identify the sectors concerned by the cover, aggregate limits… It must also include stress tests to spot potential aggregations of risks.

Cyber expertise

This is about being in step with the constantly changing cyber environment and demonstrating one's commitment to keep pace with the changes in the cyber risk covered by the insurance contracts.

III) Example of a clause available to the market: the cyber risk exclusion clause in maritime insurance on the London market

In the beginning of the 2000s, the London market for transport insurance conducted works to account for cyber risk by proposing a standard model clause for the entire market. The international transport assurance market today, and maritime transport in particular, is mostly in favour of excluding cyber risk. For this, a model clause is therefore used to exclude covering cyber risk arising from malicious intent in damage and civil liability contracts. This general exclusion clause called CL 380 does not apply to cyber loss triggering events resulting from human error or malfunctioning.

The standard exclusion clause provided to the maritime transport insurance market is perfectly clear to insurers and policyholders alike, and dispels all ambiguity as to cyber risk cover.

This clause remains open to discussion between the parties.

Institute cyber attack exclusion clause CL 380 (10/11/2003)]

"1.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile."

IV) A new initiative by the London market for aviation insurance undertaken by the Aviation Insurance Clauses Group (AICG)

This London market working group is considering introducing an exclusion clause like the one proposed for maritime transport

B. Improved assistance for the company

Given the new risk context and regulatory constraints, insurers must not only provide insurance cover for cyber incidents but also assist and guide companies. In the underwriting process, their role includes the following:

- inform about the growth of the threat and the legal watch – this is all the more crucial given that insurers are a key providers of information to their clients and prospects as regards legal developments;
- provide risk analysis and advisory services for preventing and mitigating risk in order to reduce vulnerability to cyber incidents during the cover period;
- follow up crisis management and analyse its financial and operational impact, so as to reduce the impact of cyber incidents (on this point, cyber attacks and notably ransomware call for extremely short response times; with their operating system paralysed, companies need to receive a nearly instantaneous response from their service providers; technical expertise is all the more important during massive attacks as insurance firms will need to rally several experts specialised in cyber risk).

These extended functions call for cyber expert skill-building both for underwriting and for loss management. In a recent survey it conducted, Verisk Analytics underscores the fact that more than half of the insurers do not have underwriters dedicated to cyber risk and appoint specialists from other lines of insurance to manage cyber insurance policies[98].

It is urgent for insurance firms to specialise their staff, notably by encouraging them to obtain the Certificate of Digital Skills for the Insurance Sector to have their cyber risk credentials recognised.

(98) Cited in Oleg Bogomolniy, *Cyber Insurance Conundrum: Using CIS Critical Security Controls for Underwriting Cyber Risk*, published by The SANS Institute, 2017, p. 14.

C. Narrow down risk segmentation

As they gather experience, insurers will be able to become increasingly accurate in quantifying the policyholders' actual exposure to cyber risk, and as a result, discriminate between risks and segment their pricing in a more relevant manner.

Cyber experts' training in the insurers' firms as well as in the policy holders' companies, partnerships established with cyber security service providers, ongoing efforts to adopt harmonised risk definitions and gather data on past cyber incidents across the market in order to enhance the statistical databases should contribute to this development.

A pricing approach that reflects the real exposure of policyholders to cyber risk should help develop a greater penchant for covering better risks.

D. Settle the question of insurability of administrative sanctions and ransoms

The French Insurance Code does not deal with the question of whether the sanctions or ransoms are insurable.

1. Open question about administrative sanctions

In France, CNIL has the power to impose administrative sanctions against companies that breach data security rules, following the amendment to the 1978 data protection act in 2004[99]. This power was reinforced at the national level by the Lemaire Act of 7 October 2016, as well as by the European Regulation on the protection of personal data (GDPR), that will be applicable to all Member States as from 25 May 2018[100].

(99) *Act No. 78-17 of 6 January 1978 on information technology, data files and civil liberties,* Art. 45.
(100) GABRIE, *"Les pouvoirs des autorités de protection des données"*, Dalloz IP/IT, 2017, p. 268; *Loi 2016-1321 du 7 octobre 2016 pour une République numérique;* EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016.

The question raised is whether the administrative sanctions imposed following breach of the regulations governing personal data protection are insurable. This question is all the more important given that the administrative sanctions are hefty (and will be all the more so when GDPR will be applicable).

The answer to this question is not unanimous. Some consider that insurance is necessarily unlawful by analogy with the penal sanctions, as it goes against public law and order. The Cour d'Appel de Paris, in its judgement of 14 February 2012[101], stated that a sanction imposed by the French market regulator AMF was not insurable under Article 6 of the Civil Code that states *"One may not by private agreement derogate from laws that concern public order and good morals"*.

This judgement of the appellate court upholds that the insurability of administrative sanctions imposed by AMF goes against public law and order, as it would strip them of their deterrent effect.

By contrast, a judgement by the Cour de Cassation on 14 June 2012[102] leaves room for doubt. In that particular case, a managing director had been fined by AMF. He intended to call up his "Director liability" insurance that covered all fines and/or civil penalties. The Cour de Cassation did not rule on the insurability of that risk, but defeated the insurance game on the sole grounds that the policyholder has committed an intentional fault, which was inconsistent with the contingency concept.

This judgement gives rise to one certainty and one question.

Certainty: the Cour de Cassation did not rule on the validity of the insurance, although it had the opportunity to do so as it was a matter of public law and order.

(101) Cour d'Appel de Paris, Unit 02 Ch. 05, 14 Feb. 2012, No. 09/06711.
(102) Cass. 2nd civ., 14 June 2012, Appeal No. 11-17.367.

Question: does the fact of remaining silent regarding the validity of the clause and of focusing the discussion exclusively on the intentional nature of the policyholder's fault mean that the Cour de Cassation deems the risk of sanctions by AMF to be insurable?

Legal writers are divided in their views, with some in favour of voiding the stipulation, and others who consider a contrario that it is acceptable to insure oneself against such a risk, provided that the fault covered is not intentional[103].

This being said, and assuming that this interpretation is valid, another problem will come up.

Given that CNIL does not impose certain sanctions without having first summoned the entity to comply, can the processor's failure to do so be considered as an intentional act, which therefore precludes the insurability of the sanction?

This analysis must be qualified in the context of the Law of 7 October 2016, according to which CNIL can now exercise its power to sanction without prior summons. The question of intentional fault post-summons does not arise in these circumstances. Besides, CNIL has already applied this new system in the "Hertz" decision of 18 July 2017 by imposing a €40,000 fine on the processor[104] for negligence, after large volumes of the latter's clients' data was made accessible to the general public following a change of its subcontractor's server.

Certain insurance firms seem to have developed a practice that consists in compensating monetary administrative sanctions "provided that they are insurable". By nature, it is difficult to identify what is "insurable[105]". This lack of clarification may be due to the lack of a stable solution set down by law or established by case law. It is by putting the guarantee clauses in writing that these insurance firms make compensation possible, as seen in the text below.

(103) RTD Com.2012 p 813, Nicolas Rontchevsky; Bulletin Joly Sociétés 01/10/2012 No. 10 – page 696 by Bernard Saintourens.
(104) Deliberation by the restricted committee No. SAN-2017-010 of 18 July 2017 pronouncing a monetary sanction against HERTZ FRANCE.
(105) Helenon Nicolas, Heslaut Clarisse, *"Données personnelles – Sur l'assurabilité des sanctions administratives"*, Expertises, May 2017, No. 424.

"Fines and penalties: where applicable, and by partial derogation to the general exclusion of guarantee No. XX below, any fines and penalties imposed upon you in connection with the investigations and actions referred to below, and provided that they are legally insurable in respect of the applicable law[106]*."*

The lack of consensus on the subject plainly points out the need to officially clarify the legislation, so as to identify the non-transferable/non-insurable risks borne by companies on the one hand, and avoid discrepancies between insurance professionals in their interpretation of the law.

Focus – Proposal for the reform of civil liability and uninsurability of civil fines

In the civil liability reform proposal[107], the draft Article 1266-1 of the Civil Code stipulates that the perpetrator of damages who deliberately committed a fault for gains or savings can be sentenced by the judge at the request of the injured party or the public prosecutor, in a specially substantiated decision, to the payment of a civil fine. It is not insurable..

2. Ransom

A new form of cyber criminality has spread fast – ransomware, malicious software that encrypts data and demands the payment of a sum of money, or "ransom", for the owner to be able to retrieve that data. It spreads, for instance, through emails by opening a link or an attachment they contain. The data of the infected system is "hijacked" by the hacker who demands a ransom in exchange for restoring the data.

(106) Idem.
(107) Ministry of Justice, *Projet de réforme de la responsabilité civile*, March 2017, [http://www.justice.gouv.fr/publication/Projet_de_reforme_de_la_responsabilite_civile_13032017.pdf].

There are two assumptions for retrieving the data that has become inaccessible.

- Use an IT expert, who can attempt to restore the backups of the data that has been "hijacked" by the cyber attacker. These costs may be covered by the insurance contract.
- Pay the ransom, which does not necessarily ensure that the data will be decrypted (as an example, the NotPetya ransomware was a virus that did not enable retrieving the decryption keys, and therefore, the data); its insurability is open to discussion.

In the French market, some recommend that such ransoms be uninsurable for reasons of public law and order. In fact, on grounds of that fact that the funds obtained by such acts could be used to finance terrorist acts, one could argue that any contractual clause that provides for insuring these ransoms would be void pursuant to the provisions of Articles 6 and 1102 subparagraph 2 of the Civil Code and 421-2-2 of the Penal Code, as it is contrary to public law and order. This position seems to be shared by most countries of the European Union except, notably, The Netherlands, the United Kingdom (from 1981 since the "Ransom Act of 1782" was repealed) or Switzerland where criminal risk can be insured.

Other firms guarantee them by analogy with "kidnap and ransom" contracts that are called up first when human lives are at stake, and that provide additional guarantees against cyber extortion.

Focus – Stance of the Finance Ministry on the insurability of ransom payment to terrorist entities

The French Treasury Directorate[108] took an official position banning *"insurance contracts whose purpose is to guarantee ransom payment to Daesh, as to any terrorist entity"*, and encouraging "*the insertion of clauses in "kidnap and ransom" insurance contracts to exclude the refund or the payment of ransom, directly or indirectly via intermediaries, that would benefit Daesh"*.

This release is based on Article 421-2-2 of the Penal Code that states *"It also constitutes an act of terrorism to finance a terrorist organisation by providing, collecting or managing funds, securities or property of any kind, or by giving advice for this purpose, intending that such funds, security or property be used, or knowing that they are intended to be used, in whole or in part, for the commission of any of the acts of terrorism listed in the present chapter, irrespective of whether such an act takes place"* and on the EU Regulation 881/2002 according to which "funds include guarantees; no funds or economic resources shall be made available, directly or indirectly, to terrorists designated by this regulation; it shall be prohibited to participate, knowingly or intentionally, in activities the object or effect of which is to circumvent this prohibition".

In cyber matters, it is often difficult to know the perpetrator of an act or to determine whether or not an incident is of terrorist origin.

Unless it can be proved that the hack was carried out by a terrorist organisation, there is a legal vacuum regarding the insurability of ransoms.

(108) Release from the Finance Ministry, *Lutte contre le financement de Daech, Dispositif de vigilance financière à l'encontre de Daech*, December 2015, [http://www.tresor.economie.gouv.fr/10858_lutte-contre-le-financement-de-daech].

Also, as is the case with administrative sanctions, certain insurance firms tend to cover risks inherent to ransomware under the terms and conditions defined by the contract, in the absence of specific legislation. It is difficult to analyse such contracts owing to the privacy clause they contain. As regards ransom payment, whether for persons or for electronic data, if potential kidnappers or cyber attackers were to know of such an insurance, policyholders would become choice targets.

E. Control accumulated commitments

"Without effective accumulation risk controls, a (re)insurer could find itself burdened with catastrophic losses that exhaust its capital, impairing its ability to make good on promises to policyholders[109]." Like the author of the last Swiss Re study on the topic, an increasing number of observers are underscoring the fact that underwriting cyber risk is weighing heavily on the (re)insurer's track record due to a very specific accumulation risk. "Underwriters are concerned about their exposure to a breach [of personal data] that would affect a large number of their policyholders simultaneously."

For the insurers, there is a strong likelihood of their having to compensate a large number of policyholders for the same cyber triggering event, mostly due to the reasons outlined below[110].

- Information systems are more and more interconnected, which may lead to the snowball effect in case of a computer virus infection, for example.
- The worldwide use of the same IT components (software, computers, servers, systems, routers, etc.), the same services (cloud, outsourcing), and the same connected objects, aggravate the risks. The vulnerability of any one of the providers could lead to a massive serial loss event.

(109) Swiss Re (2017), Cyber: getting to grips with a complex risk, 2017, No. 1, p.21.
(110) See Part 1, I, B.

- There are no geographical constraints to the propagation of a cyber incident: the WannaCry virus that was propagated using former versions of the Windows 10 operating system on which the security updates had not been carried out, illustrates this fact.
- Accumulated guarantees: conventional property damage and civil liability policies can be called up in addition to specific cyber cover, leading to the risk of a tricky arbitrage depending on the deductibles and guarantee amounts (capped annually or by loss event), and on how the loss event is handled.

Therefore, a given cyber event is likely to cause multiple loss events through the various policies taken out by multiple policyholders around the world[111]. This risk of simultaneous compensation through the different contracts is an obstacle to mobilising sufficient funds to cover the needs of the market. Working on clarifying the guarantees and the exclusions of cyber risk cover should enable us to have a better understanding of the commitments and better knowledge of accumulated commitments.

For reinsurers, accumulation risk will be further amplified.

- As a company is covered by several insurers, a single cyber incident faced by the company can trigger loss events under several reinsurance contracts.
- A cyber incident suffered by a policyholder can be compensated through several insurance contracts. These contracts may be transferred through different reinsurance contracts.
- In case of a massive cyber disaster, it remains uncertain as to how conventional reinsurance contracts (general or professional civil liability, damage, etc.) will respond.

(111) See Part 2, II, A. Clarify the junctions of the cover.

To avert accumulation risk, (re)insurers gather as much information as they can about the likely common vulnerabilities (identification of cloud service providers and the software used, notably) in order to map the potential accumulation risk and establish indicators to measure the impact of business interruption of the Internet service provider, the cloud service provider or the payment service provider, for example.

One of the solutions to fully understand these accumulations is to create cyber disaster scenarios.

These scenarios must meet several requirements: be massive while remaining probable ("end-of-the-world" scenarios must be avoided), and enable assessing the financial impact not only from the general viewpoint (impact on the economy) but also for the reinsurers.

The scenarios built by major policyholder companies will supplement the ones designed by insurers and reinsurers.

Regulators such as rating agencies – who have made it clear since 2015-2016 that a poorly controlled accumulation of cyber risk could adversely affect the (re)insurer's rating – are particularly watchful about whether the accumulations are managed properly.

F. Growing proportion of intangible assets – a challenge for insurers

Reputation, intellectual property or loss of opportunity are intangible assets that are highly exposed to cyber risk. In an increasingly digitised economy, their weighting in the company's worth has risen considerably.

Focus – Recognition and measurement of intangible assets

Over 50% of the company's worth is represented by intangible assets (value of the brand, value of patents, value of the technology, value of the information system, value of the teams set up, etc.), whereas less than 20% of these assets are accounted for[112].

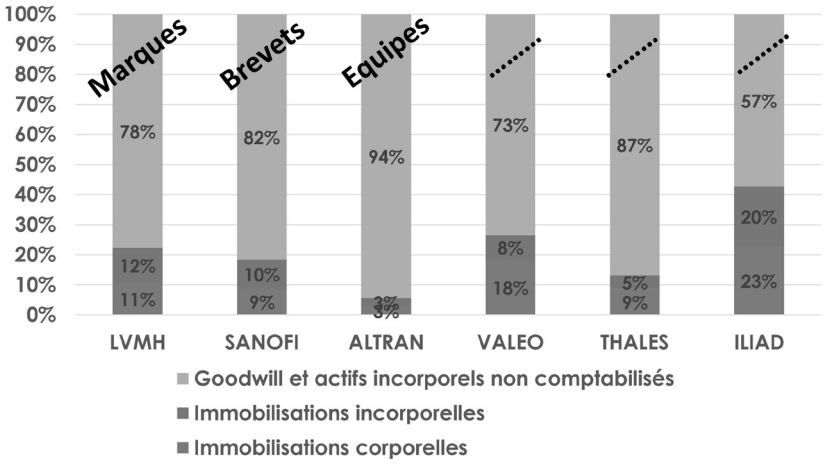


Illustration based on the market capitalisation of French listed companies

EIn case of a cyber incident, intangible assets now represent a large share of the potential losses.

The market today is not capable of insuring assets of this type in a standard manner.

(112) E. CHASTENET, *Recognition and measurement of intangible assets, overview – The case of brands,* Presentation given at the IRT System X meeting of 18 April 2017.

This demand mainly comes from major companies. The intangible asset insurance issue is not a new one and is more important than the cyber risk issue. The solutions offered by insurance today are not quite suited to cover these assets, notably because it is difficult to quantify the asset and measure the risk. There may be alternative solutions for key clients.

The terms and conditions for transferring these risks to insurance and reinsurance are therefore still being studied at present.

PART 3
Ten recommendations to insure against cyber risk better

The recommendations given below concern cyber insurance for companies and more specifically micro businesses, SMEs and local government bodies. Cyber risk transfer to the insurer must be a part of a global strategy for the financial management of cyber risk and must be preceded by the assessment of the risk, its prevention (theme to be dealt with in another book by this commission) and anticipated crisis management.

Recommendations intended for insurers and risk managers

Recommendation 1: accelerate the development of a cyber risk culture

1) **Inform** the policyholder companies **about the risks inherent to the use of new information and communication technologies; raise awareness among them about the European and national regulatory requirements** by inviting them to regularly visit the new website cybermalveillance.gouv.fr, as well as the ANSSI and the CNIL websites.

2) Develop partnerships with the representatives of economic stakeholders (professional federations, professional syndicates and associations, local government groups) in connection with the new national measure for proving assistance to victims (the public interest group ACYMA), so that they **inform their members of the option of transferring cyber risk to insurance.**

3) Encourage the employees of insurance firms to have their cyber risk credentials certified at the earliest by obtaining the **Certificate of Digital Skills for the Insurance Sector.**

Recommendation 2:
clearly explain the content of the different cyber cover options and make it easier to compare insurance offerings

When underwriting or renewing an insurance contract, propose an **audit of the insurance cover against cyber risks** to companies, to show the extent of their cover, clarify the junctions between the cyber insurance cover offered by the different policies already taken out (property damage/civil liability/fraud or policies dedicated to cyber risk) and identify any redundancies and/or loopholes in the cover.

Draw up and regularly update a **list of the key components of the cyber insurance contract** (relating to territoriality, the scope of the guarantees, the associated services and exclusions, etc.), to enable companies to better understand the insurance offering and its relevance to their risk exposure. A group of experts will be set up for this purpose, bringing together insurers and specialists in risk management.

Recommendation 3:
strengthen the relationship of trust between insurers and the insured in managing cyber insurance contracts

Draw up a **standard charter** binding upon the insurer (and associated providers) to safeguard the privacy and security of the information shared by the policyholder when taking out the insurance and when managing a loss event.

This task will be undertaken under the supervision of FFA and in collaboration with ANSSI, AMRAE and any other stakeholder concerned.

Recommendations intended for insurers and reinsurers, ANSSI and CNIL

Recommendation 4: develop a digital security framework for micro businesses and SMEs

Develop a digital security framework for micro businesses and SMEs suited to their size and business sector, based on the standards developed by ANSSI for the major companies and critical service operators (OIV).

Insurers will promote compliance with these standards.

Recommendation 5: pool the data collected from cyber incidents

Define the **methods and procedures for sharing information on information system security incidents or data breaches** with the collaboration of ANSSI, the public interest group ACYMA, CNIL and FFA.

The information can be shared through the works that have already been conducted at the international level, notably by CRO Forum[113]. This will be useful to create a database of qualitative and quantitative data on cyber incidents (and the amounts of the compensations relating to them) so as to improve their financial management.

(113) The CRO Forum is a group of Chief Risk Officers from large multi-national insurance companies that focuses on developing and promoting industry best practices in risk management (see https://www.thecroforum.org).

Recommendation 6: manage risk exposure and accumulated risk of insurers and reinsurers

Create cyber disaster scenarios to make the national economy more resilient to this type of event by encouraging the main market players of the insurance and reinsurance market to work hand in hand with ANSSI

Recommendations intended for European bodies

Recommendation 7: define a European set of technical standards to make it easier to assess the level of security of policyholders

Set up a framework for certifying the security level of software and technical products that will enable creating a **European cyber security label** for players in the digital world[114].

Recommendation 8: establish the conditions for fair competition between cyber insurers

Call on the regulatory authorities of the European Union to adopt a legal framework that will enable the harmonised handling of the issue of ransom insurability in the European market.

(114) Proposal by EU Cyber Security Agency regulation (ENISA) and Its appendix - France 24, *Une agence et un label de l'UE pour affronter les cybermenaces,* 19 Sept. 2017, [http://www.france24.com/fr/20170919-une-agence-label-lue-affronter-cybermenaces].

Recommendation 9: set up a European and international regulatory watch and follow-up of market evolution

Develop, at the initiative of European bodies, an online platform giving a brief account of the **regulatory and market information on cyber risk management**[115] in the main OECD countries, **with the cooperation of the relevant international organisations.**

This platform will notably report national and international public and private sector initiatives regarding the development of the cyber insurance market.

(115) This platform could draw from the OECD report called: *Enhancing the Role of Insurance in Cyber Risk Management*, 2017.

Recommendation intended for public authorities and French and European investors

Recommendation 10: orient public and private sector investment towards the creation of a French and European chain of excellence in cyber technology

The investment effort by public authorities and consistent choices by institutional investors should support the development of the cyber insurance market.

The French and European public investment plans should promote the development of a French and European chain of excellence in the area of cyber protection and support the undertakings of the market to curb cyber threat.

As institutional investors, insurers could also add the need to reduce cyber risk in their asset allocation policies, notably by supporting leading-edge projects in the cyber protection chain.