Cyber Risk and Insurance Cyber Risk Governance throughout the value chain and its transfer to the Insurance

Philippe Cotelle, Philippe Wolf, Bénédicte Suzan

Cyber Risk Governance throughout the value chain and its transfer to the Insurance Market

RESULTS of the RESEARCH Seminar
November 2015 - July 2016

IN PARTNERSHIP WITH

AMRAE	FERMA Federation of European Risk Management Associations	Fédération Française de l'Assurance

REPORT

ESTABLISHED BY

PHILIPPE COTELLE HEAD OF RISK MANAGMENT & INSURANCE AIRBUS DEFENCE AND SPACE	PHILIPPE WOLF PhD PROJECT MANAGER EIC IRT-SYSTEMX	BENEDICTE SUZAN PhD R&T AND INNOVATION COORDINATION (CIS) AIRBUS DEFENCE AND SPACE

FOR MORE INFORMATION ABOUT THIS REPORT, YOU CAN CONTACT THE IRT-SYSTEMX DETAILS BELOW :

IRT SystemX
8, avenue de la Vauve
CS 90070 – 91127 Palaiseau Cedex
Web site: www.irt-systemx.fr
Email: philippe.wolf@irt-systemx.fr

VERSIONS	Relecture	DATE	Modification
ISX-IC-EIC-transfert-risque-draft-v0	ISX et Airbus Group	17/06/2016	Initial Version
ISX-IC-EIC-transfert-risque-LIV-0401-v10	Groupe de travail	29/08/2016	Version diffusable
ISX-IC-EIC-transfert-risque-LIV-0401-v10_2016-10-25-ang.docx	English translation	01/11/2016	Publishable
ISX-IC-EIC-transfert-risque-LIV-0401-v10_2016-10-25-ang-v2.docx			Wording corrections

Table of Contents

I. Presentation of works

This research, conducted under the EIC Program at IRT-SystemX[1], concerns the **conditions needed for knowledge, management and control of cyber risk so that it would be possible to transfer it to insurance**. Chapter III summarizes the results. Later chapters detail all the work undertaken. The initial work plan, presented below, lays out the main lines of the work.

EIC T5.2 Cyber Insurance	Subject of session	Purpose of session	Results	Deliverable	Contributions
First year of research (3 envisaged)	The first year to be devoted to pinpointing the problems; Seeking shared definitions of cyber risk exposure and its criteria for the insured and the client.				The secretariat of the sessions and written production is provided by EIC.
1st meeting 24 November	Presentation of the proposed research and challenges for the year, and what will follow depending on results where relevant. Presentation viewed from the insured's standpoint. The importance for industry to step up management of cyber risk and its assessment, and the capacity to dialogue with the insurance and compare its in house risk analyses Presentation of insurance point of view: clear obstacles in insurance market. Presentation of the Public authorities' standpoint : obstacles to overcome, initial actions	Presentation of work envisaged for the year Ascertain organizations' need to learn how to control cyber risk via dialogue with insurance Expression of insurance and insured needs Show how the legislator can help	Seek agreement on The interest of creating tripartite exchanges between industry, insurers, reinsurers and the public authorities and/or professional associations. Blocking points, definitions and objectives of the discussion. Agreement on method and contributions and expectations of each participant Agreement on the finality of the research	Minutes of meeting. Document including a taxonomy, identification of technical and regulatory bottlenecks. Roadmap, schedule of activities and contributions of stakeholders.	Call for contributions from partners. Provision of legal EIC resources in support of T5.2.

[1] **EIC : Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité.** Appendices 1, 4 and 5 detail the context of implementation of this study.

2nd meeting 2h30	Market statistics: Insurance lacks data and models for anonymous communication approved and usable by all	Produce a definition and qualification of cyber incident from the standpoints of the insured and the insurer. Propose common, factual criteria to show that an organization is meeting the requirements for protection against cyber risk.	Define the conditions for a framework agreement for internal (for organizations) and external reference (for insurers and reinsurers).	Minutes of meeting Summary of problems and consensus reached and describing progress Document describing the means for modelling	
3rd meeting 2h30	Cover: what is the insured party's need for cyber risk cover?	Address the issue of compensation for loss of IP, R&D and operating data or production means How to manage disastrous events (accumulation scenario), the responsibilities of the client, insurer, public authorities. Finding methodology to calculate maximum events, is mutualisation a possibility?	Produce initial elements	Minutes of meeting Summary of problems and consensus reached and describing progress	
4th meeting 2h30	Subscription and cyber risk management information : need for a sworn representative	Discuss the following: in the current absence of market statistics and in view of existing cover, how can trusting dialogue between client and insurer be established? What role should the public authorities play?	Define conditions for trusting dialogue between insured and insurer Define the trustworthy third party enabling collection, validation and anonymous character of data contributing to building of models Propose the creation of a joint organization defining the content and validation of a qualifying training course for Insurance Cyber Experts	Minutes of meeting Summary of problems and consensus reached and describing progress	

5th meeting Conclusion 2h30	Presentation of work over the year, proposed concluding document	Consolidation e of reference framework, common criteria and methodology.	Agreement on standards and dissemination of research results. Proposed plan of action.	Presentation of concluding report on the three work topics proposed at first session Research report presenting proposed common criteria and a standard. Presentation of plan of action for implementation of common criteria and standards, design monitoring methods Presentation of means needed Proposition – depending on opportunities: Publication of research results Organization of a half-day colloquium with the support of ANSSI.	

Figure 1 – Work plan

II. Method

This research was conducted by a pluridisciplinary team including insurers, reinsurers, an international organization, public organizations and researchers. Appendices 2 and 3 list the participants in this work.

Regular seminars were held to compare opinions and ideas on the various topics described in Fig.1. Consensus was reached on the **five consolidated recommendations** of Chap. III.3. Chapters IV – VII described the various approaches and ideas explored, which will be examined in more depth in later works described in Chap. III.4.

Meeting 1 – introductive (November 2015). In addition to presenting the project and the research proposal, the purpose of this meeting was to put ourselves in the risk manager's shoes when taking account of and managing cyber risk: what should be the normative framework for addressing cyber risk? What proposals should be made?

Airbus Group presented its feedback on SPICE – *Scenario Planning for Identification of Cyber Exposure* – which was developed in-house in 2015. SPICE enables a financial value to be placed on digital risk exposure so disastrous that it threatens the survival of an organization. The approach used information collected from operating staff to quantify how a major attack would affect each sector and draw up scenarii. The exercise can be carried out annually and allows the risk manager to identify, manage and control risk exposure and begin dialogue with the market with a view to transferring it to the insurer. It was suggested that the SPICE approach could be used as a standard for assessing digital risk exposure and that a standard scenario should be replaced by a risk analysis specific to each organization, taking account of digital risk for each sector.

Meeting 2 – Common categories, definition, qualification and quantification (January 2016) – presented a table of causes and consequences. The preparatory work for meeting 2 included initial definitions of metrics, harmful events and prejudicial consequences on the lines of a periodical table. The purpose was to produce bricks to constitute digital risk exposure scenarii: a series of predefined events/elements with which objective metrics were associated. Their combined complexity, like that of molecules, atoms and combinations thereof, constituted the complex scenario of the cyber-attack. The idea was to propose a consistent, logical system to illustrate cyber-attack scenarii. The definitions of the metrics, the harmful events and the prejudicial consequences were prepared with the help of the legal experts.

A reality check was then organized (March 2016) to test whether the table of causes and consequences worked. It showed that using the table did indeed allow cyber-attack scenarii to be played. Those played were averred cases made public or recovered by stakeholders in the market. The template nevertheless underwent re-writing during the meeting.

Meeting 3 – Cover and scenarii management by insurance (April 2016). The purpose of this meeting was to show how the market could respond to all the cases of cause and consequence and what insurance cover could be envisaged for digital risk. The mapping table of insurance cover was drawn up on the basis of the causes and consequences table and above all based on the work already

accomplished by the insurers of the FFSA (French federation of insurance companies, renamed FFA in July 2016). Their document is innovative and unique.

Meeting 4 – subscription information (May 2016) concerned the conditions for dialogue between insured and insurer. How could this dialogue be built up, how could the interested parties communicate on subscription information, how could confidentiality be dealt with, how could claims be lodged, and how to address the issue of loss assessment (recourse to experts)?

An additional meeting was devoted to the presentation of the initial research results and the proposed recommendations.

Meeting 5 – Concluding. This was devoted to presentation of the research report for approval and the decisions concerning subsequent actions and works.

Many parallel meetings were organized by Philippe Cotelle and/or Bénédicte Suzan to advance on various points.

III. Summary of results

III.1. Today

Increasingly aware of the threat of cyber risk for their businesses, companies and other organizations are endeavouring to assess their cyber risk exposure more precisely. However, they face many obstacles: acknowledgement, grasp and control of this risk. In the absence of reliable procedures to back their approach, many risk managers have failed to take a comprehensive view of cyber risk throughout the value chain, nor have they integrated the possibility that it could threaten the company's very existence. Many wonder whether it is worthwhile investing in cyber insurance cover, because they are aware that securing their information systems and protecting their infrastructures, products and strategic data will never guarantee them from all attacks.

The public and private figures on the cost of cyber-attacks are currently inadequate: there are as yet no series of statistics over a sufficiently long period, nor widely approved metrics that would define the overall cost of past attacks, or reliable economic models enabling loss arising from future IT attacks to be predicted.

These obstacles hamper the development of the cyber-insurance market. While all the interested parties agree that it has high potential, the market, first developed in the United States, remains in its infancy in Europe.

In parallel, the national and international public authorities have also begun examining cyber risk management and possible transfer to insurance, the better to improve the resilience of economic players. In some countries, regulatory or statutory tools have been developed.

Cyber space is definitely different from the real world because it complies with a different sort of laws: digital networks have no borders, are infinitely expandable and are abstract and virtual in nature. Time and space are compressed in cyber space: potential attackers might be your own neighbours; transitions cannot be seen; the precursors of an attack are very difficult to perceive; identities are difficult to discern and actions are ambiguous. The malicious nature of a computer code is not something intrinsically easy to prove.

Finally, the digital economy defies traditional concepts: the cost of an attack may be marginal (free tools) compared to the cost of the consequences or that of protecting information systems.

Today, digital risk is poorly identified:

- Digitization of all human activities, from business to home, has increased the surfaces that can be attacked and means that digital risk must be taken into account by all levels of society;
- Today, it is difficult to have common references and vocabulary because the threat is constantly changing, even though the fundamentals remain the same ;
- The lack of public and private figures for the cost of attacks, methods for calculating which are approved by the entire community, and the absence of statistics and econometric models, means that it is difficult to assess the losses arising from digital attacks;
- For an organization, it has become indispensable to quantify or calculate the economic and financial impact of a cyber incident on its value chain. This evaluation will enable it to decide whether to transfer it to insurance;
- Insurance methodologies are not yet consolidated or established enough to calculate the cost of cyber risk. Today there are no **tried and tested metrics** enabling precise evaluation of the cost of a cyber-attack, determination of risk reduction strategies and the insurance company's decision to transfer the risk. The state of the art is still immature.
- However, the **risk manager can measure the risk and decide to control it via a constructive dialogue with the insurance market.** However, obstacles arise in the form of lack of knowledge, understanding and control of his risk in house, and he has no **references, criteria and standards,** to help him. The references provided by corporate risk management have not yet integrated a comprehensive, all-inclusive approach to cyber risk throughout the value chain, not to mention any disastrous event that could threaten the company's existence. The risk manager must address cyber risk and no longer leave it to the organization's IT department or cyber security technicians.
- The research project endeavours to meet the risk manager's needs, to help him control cyber risk and transfer all or part of it, as the case may be, to the insurance market.

The first year of the project concerned the causes and consequences of cyber incidents, and the various insurance lines covering them. The works also attempted a better definition of subscription information. Investigation was made into creation of a joint organization defining the content and validation of a qualifying training for Cyber insurance experts. These would be the trustworthy third parties helping companies and organizations to quantify their cyber risk and would also enable the collection, validation and anonymity of the data needed for modelling cyber risk.

These works formed a reference base that insurers and reinsurers could be invited to share.

III.2. Research objectives

The applied research work concerned the conditions for knowing, managing and controlling cyber risk as well as transferring it to the insurance market where deemed necessary.

More especially, the goal of the working group was to identify the obstacles hampering understanding and assessment of cyber risk, those in particular that prevent the cyber insurance market from developing. It also wished to advance on certain issues and produce its first recommendations. A White Paper, based on this report, will then propose a plan of action synchronized with current legislative and regulatory schedules (national and international).

Private and public organizations have begun to examine the definition of their exposure. However, they are finding it difficult to express their needs, understand their risk exposure and find effective protection, all the more so as the cost of cyber insurance cover, investment in securing their IS (Information System) and protecting their infrastructures, products and strategic data, is very high. They hesitate whether to transfer all or part of their cyber risk to insurance, especially as it may already be covered by other guarantees they have subscribed to.

The national and international public authorities are also investigating the question and wondering by what means to foster constructive dialogue and pass the necessary regulatory or statutory provisions.

The working group's investigation included the problem of reinsurance, because cyber risk is deemed to be systemic. Fear that subcontracting chains, reputation, the general public will be affected by these systemic effects, not to mention cascading, unpredicted and uncontrolled damage, the speed with which technologies change and the unceasing evolution of attack scenarii, has led the market to consider it the greatest future threat (intelligent territories, increasing robotization, intelligent transport, exploitation of personal data).

Over the first year, work was done on defining cyber risk exposure. The following ideas were suggested:

- Common categories, shared definitions, qualification and quantification of cyber incidents;
- Insurance lines to cover them;
- Improve subscription information and draw up confidentiality rules.

The work and cyber risk exposure analysis at the heart of the seminar's work was based on the reference work by the NIST, National Institute of Standards and Technology in the USA and ENISA (the European agency for IS security). The French LPM (military planning law) – OIV (for operators of vital importance) was drafted pursuant to the European law (NIS Directive, Network and Information Security), and also follows the UN GGE (group of government experts).

The works were therefore international in their approach.

Consolidated Recommendations

Recommendation 1

Each company should conduct a **financial analysis of cyber risk**, to**:**

- Analyse its **operating impact**;
- Define the **appropriate level of investment** in prevention and protection;
- Deduce what risk to **transfer to the insurance**.
- This analysis should be conducted by the **risk manager**[2] who must arbitrate between operating imperatives and his organization's security constraints. This cyber risk analysis should be based on critical scenarii drawn up with the help of operating staff. It should include scenarii that would be disastrous for business and financial quantification of their consequences over time. This exercise would enable him to assess the organization's exposure to this risk and take better decisions in terms of risk-reducing policy. Presentation of the *Airbus Defence and Space*- SPICE approach enabled a concrete demonstration of how the process could be set up.

Chapter IV develops this recommendation.

Recommendation 2

It is useful to define a **common reference and language** that will enable cyber risk analysis to be carried out for transfer to insurance. This common reference will provide a useful framework in which to reference and also make relative comparisons of risk exposure in the various entities. **We recommend that each exposure scenario be separated out into the elementary risk categories** (combining insured events and consequences), which will provide a common analysis framework for all entities, regardless of size, nature or activity.

The research work led to an innovative proposal of a cyber risk analysis reference framework including elementary categories that, put together, can cover all the scenarii that might affect these entities. The concepts enable them to build their own references if they wish (pursuant to competition law provisions).

This common analysis framework is a considerable advance in rationalizing risk assessment and allows relative mapping of the risk profile of the various entities in a shared reference.

Chapter V develops this recommendation.

Recommendation 3

Better communication and knowledge of cyber risk insurance cover must be developed. Risk managers and risky entities need better understanding of the way in which the various covers

[2] This approach must also be adapted to very small and SMEs for definition of their cyber risk exposure and transfer to insurance. Later we will refer to the risk manager as a generic function that also covers professionals called in to help organizations that cannot afford a dedicated risk manager.

protecting their entity combine to address their exposure. The **template** drawn up by this research program will allow:

- Risk managers to check how the various policies they subscribed to offer complete, effective cover of their entity's needs;
- All the interested parties better to understand insurance cover by distinguishing the guarantees of traditional insurance policies from those of dedicated cyber policies. Silent cover, where the cyber risk is not expressly excluded, may thus be identified more easily;
- The national authorities to have an instant overview of their insurance market's response to this risk;
- International organizations to have a better view of the subject. The template could become the basis for an international benchmark if the responses of the various national markets to this exposure were compared.
- The template can be used by all stakeholders, with no exclusivity or constraint, not least in the framework of international benchmarks. It can be simplified to make it easier to use for small entities.

Chapter VI develops this recommendation.

Recommendation 4

Managing confidential dialogue when exchanging subscription information and dealing with the event, requires a neutral, secure platform for communication between insured and insurer. Better dialogue will enable insured to reveal their exposure and manage their cyber risk more efficiently, so that the subscription to the most suitable cover is adequately tailored to needs. It enables better exchanges where an event occurs because confidentiality will be guaranteed.

Three types of structure may be envisaged:

- An extension (which would require legal structuring) of the "platform for assistance to victims of cyber harm" set up by ANSSI with the French Ministry of the Interior (announced in the National Strategy for digital security[3] presented on 16 October 2015) ;
- Another, neutral platform for information exchanges between insurer and insured. It would be run by a trustworthy third party. This "secure mutualist platform for controlling and insuring against cyber risk" would be non-profit making. Its legal status remains to be defined.
- A "national cyber risk observatory". One possible model is the National Observatory for Natural Risks[4]. The structure could enforce anonymity in collecting reliable statistics to help improve evaluating the price of suitable risk cover. It would also deal with qualification of the trustworthy expert *tiers de confiance*.

Chapter VII develops this recommendation.

[3] http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf
[4] See http://www.onrn.fr/

Recommendation 5

We must work to normalize dialogue and pursue work on convergence between technical, insurance and legal vocabularies.

To avoid turning to litigation, it would be particularly useful to create links and convergence between technical, insurance and legal elements to define the scope of the contract and the areas of liability.

For this purpose, contractual and regulatory definitions must be compiled and definitions, probably median, proposed (on the lines of the British PPP by Cambridge University) and adapted to the international dimension of entities.

Furthermore, the following should be suggested:

- Identify the loopholes in digital law to improve legal certainty in insurance contracts;
- Follow the changes in law (Common Law);
- Legally qualify intangible data, identify the expectations it undergoes and allow quantification of its value;
- It may be relevant to associate certified accountants, auditors and corporate financial officers in this process.

Chapter V develops this recommendation. Appendix 7 lists the initial vocabulary for building common definitions.

III.3. Subsequent works

All 5 of these recommendations define points for collective work so that progress can be made in understanding how to control cyber risk.

I. Build up a common language: what are we talking about?

II. Technically:

Define IT risks in a language understandable by all

a) Legal:

Qualify data in legal terms

Compile contractual and regulatory definitions, propose median definitions, possibly based on the model of the Cambridge University PPP

Identify possible legal risks

Analyse the consequences of these new risks on the legal environment (regulatory, legislative etc.)

Identify the new areas of legal uncertainty and propose changes to the law to secure the contractual relationships between insured and insurer, e.g. insurability of ransomware, criminal fines etc.

III. Metrics

Statistical knowledge of issues is required for all transfer to insurance.

This knowledge requires exposure and hazard to be mastered.

a) Exposure: quantify the cyber risk

b) Pursue study into quantifying cyber risk (with the help of the research accomplished at the IRT).

Develop research into quantifying cyber risk in companies, not least taking account of the consequences of the new GDPR European regulation. Help companies, consultants and insurers in better addressing the issue of evaluating the cost of cyber risk for companies.

c) Hazard: Build up a data base of cyber events. These must be referenced, grouped into categories and evaluated within the data base.

Include actuaries, Chief Data Officers and Digital officers in the study

Propose a model for collecting data via the various available sources (insurers, public authorities, others) to extract reliable, shared statistics *Transfert des cyber risques à l'assurance*.

d) Share a common definition of the insurance intervention perimeter.

e) Validate, develop and communicate on the risk template and the definitions proposed by this working group, so that a credible, recognized and shared reference can emerge. This could improve the understanding and trust of the various interested parties, and even contribute to convergence among the various players' practices and thus improve the quality and suitability of the offers.

f) Covering terrorist cyber risk

Analyse the consequences of a terrorist cyber-attack, agree the insurance market's capacity to intervene and examine, as the case may be, alternative solutions like those GAREAT has produced for tangible terrorist risk.

Create trust

g) A risk culture that needs to progress

Encourage, promote actions directed at the public and companies to improve knowledge of cyber risk.

h) Develop references

Facilitate qualification of the various professionals in cyber risk control, reduction and transfer (not least consultancy, audit, prevention, protection, financial instruments, insurance etc.)

i) Foster confidentiality:

The role of the public authorities:

In addition to the promised ANSSI platform, examine whether to set up a neutral platform for exchanges of information between insurer and insured. This could be operated by a trustworthy third party, to be defined. The “Mutualist secure platform for cyber risk control and insurance” could be a non-commercial undertaking in the form of a public-private partnership between ANSII and insurance companies. Its legal form would need defining.

Ensure confidentiality in the dialogue between insurer and insured.

Both upon subscription and indemnification develop a climate of trust and confidentiality enabling insured parties to give the insurer full and transparent information so that their risk can be transferred and indemnification awarded in optimum conditions.

Accordingly, study should be made of very small and SMEs on the one hand and large groups on the other, to ascertain the nature, the required level and the guarantees of information at subscription needed by the insurance market, while at the same time respecting each insurer’s contractual freedom to define the information he requires when fixing a price for risk cover.

IV. The Risk Manager's knowledge of Cyber Risk

Issues to be addressed

Ignorance, or indeed absence of method and standards, in defining financial exposure to cyber risk where an organization is transferring risk to the insurance company.

The risk manager needs to know his risk exposure.

The risk manager needs to dialogue with the market.

For constructive dialogue, parties must have common knowledge of the subjects.

IV.1 An innovative approach for the risk manager to determine his exposure to cyber risk

The risk manager possesses tools to assess the risks his organization confronts. In large companies such as *Airbus Defence and Space*[5], top-down activity gives an annual overview of risk parameters inherent to each entity within the group, and each entity receives some 150 "risk questionnaires". Once this information is consolidated it provides a basis for a corporate tool that gives an accurate, detailed vision of macroscopic exposure. This tool is then transferred to the Group's insurers for use in subscribing to policies. The advantage of a top down approach is that it provides continuous improvement.

The risk manager uses mapping to determine critical risks, in collaboration with the sales managers and project managers, the better to be able to find the best insurance solutions. Insofar as Airbus Group receives some twenty first-line commercial offers monthly (over 100 million euros), mapping must be dynamic and fast. Risk is then evaluated in the Risk Management Committee, a formal review of all the insurance offers.

As regards cyber risk, there is no annual overview of all its parameters, nor is there controlled risk mapping. However, the Management Committee must decide which cyber risks its organization wishes to cover, at what cost and by what method, before drawing up its insurance portfolio. It must be part of its insurance strategy.

However, the state of the art currently shows that this risk is not yet taken into account in the same way as other corporate risk. There is neither consolidated method nor shared standard. The risk manager must be creative if he is to find solutions and interact with his usual interlocutors. He must be capable of responding to a simple question: what is the organization's degree of cyber risk exposure? So that he can examine how to transfer part of the risk to the insurance market.

To answer this question, *Airbus Defence and Space* developed an innovative approach with the help of *CyberSecurity*, an entity that proposes solutions for controlling technical cyber risk for the Group and its clients.

[5] Philippe Cotelle, *Les 1001 facettes du Risk Manager*, Atout Risk Manager, La Revue des Professionnels du Risque et de l'Assurance, n°9, Juin 2016.

Based on the technical expertise of *Airbus Defence and Space — CyberSecurity*, the company's risk manager developed an innovative method producing a quantified analysis of the business and financial impact of cyber risk, using SPICE – *Scenario Planning for Identification of Cyber Exposure* – a pilot developed in-house in spring 2015.

This analysis is a departure from more traditional methods.

The MARION[6], MEHARI[7], or EBIOS[8] types of cyber risk analysis (conformity mechanisms, conforming to an ideal model, IS027005[9] which concerns technical cyber risk, do not allow qualification or quantification of cyber risk using the logics of insurance (financial).

Furthermore, these methods concern IT measures and are often used in perimeter security environments: a central information system protected like a fortress keep (protected system). It was known who was connected to what and who did what. Insurance covered hardware, software, and saved data. However, today, the IT System in large groups and indeed SMEs goes far beyond the company itself: the Cloud, etc. Data has flown the fortress. Data is with the contractor, the client, in USB keys, in cyberspace etc.

These methods do not allow the business impact of a cyber incident to be understood, and even less so that of a cyber disaster scenario. They do not allow cyber risk to be quantified financially. This is because financial quantification using a mathematical model of presumed threat (in deterministic mode since a probabilistic one is not available) to correlate present or absent security measures and the presumed threats ensuing therefrom, will not work. Yet it is these presumptions that lead to a guarantee.

The SPICE pilot bridged the gap between IT risk analysis methods and the need for cyber risk analysis viewed from the risk manager's standpoint when seeking insurance. It answers the question of the cyber risk to which an organization is exposed depending on its business and its degree of digitization (the higher its degree of IT, the more exposed it is).

Thus, insofar as digital risk is linked to the business, and considering the lack of historical and statistical data, it would seem pointless to reason in terms of a portfolio of cyber disaster scenarii for each operating field or business sector. It would be better to start with operating staff's knowledge of their jobs and their perception of how sensitive their assets are. They are the best placed to identify the major cyber risk their assets are exposed to. Thus there is no standard, homogeneous digital risk scenario usable by all companies.

This seminar's proposed research into controlling cyber risk throughout the value chain and its transfer to insurance is based on the approach of the SPICE pilot.

---

[6] This determinist method abandoned the probability aspect and correlated presumed threats with present or absent security techniques: this is what a balanced system looks like.

[7] MEHARI 2010 : https://www.clusif.asso.fr/fr/production/mehari/download.asp

[8] EBIOS 2010 : http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

[9] See https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory

First, the risk manager sets up an in house exercise. Once he knows his exposure level, once he has provided the financial data that will enable the directors of the organization to make investment decisions to raise the cyber protection level, there may be a residual risk which would require an investment excessively important, and this will be transferred preferably to the insurance market.

On principle the insurance market is not the only one able to absorb this risk. As shown by the responsibility taken for the new risks (large scale or technological), organizations may prefer to opt for self-insurance (self-financing), with risks syndicated by several insurance companies, and /or transfer of risk to the capital markets.

Multi-national industries find themselves exposed to high risks due to their size and the nature of their activities. Insurance companies hesitate to cover them, or conversely, large companies may decide not to pay high insurance premiums, deeming that capital could be better invested elsewhere.

However, these organizations must think carefully about transferring risk to insurance because a cyber disaster scenario could jeopardize the very existence of their company and indeed destroy it. They must also take account of their professional liability as well as that of their corporate officers.

During the working group, presentation of the SPICE pilot approach led to the following questions:

- What are the various impacts to be taken into account?
- What metrics should be used?
- What financial, temporal and technical items should be taken into account?
- Will the conclusions of a methodology similar to SPICE be tailored to subscription needs?
- Can an insurer use SPICE results for subscriptions?
- What are the advantages and drawbacks compared to subscription questionnaires that are both more static and more technical?
- Anyway, what are we talking about?

Recommendations

It is essential to have a cyber risk analysis that quantifies and analyses the operating impacts on an organization. It must be set up by the risk manager who must arbitrate between operating imperatives and security constraints. This cyber risk analysis must be based on critical scenarii drawn up by operating staff that will enable exposure to this risk to be measured and will also lead to better strategic decision-making for reducing risk.

Presentation of the *Airbus Defence and Space (SPICE)* approach gave a concrete illustration of how the process could be set up.

The approach should be developed to adapt it to the needs of very small and small companies to help them define their exposure to cyber risk and decide whether to transfer it to insurance.

IV.2 Dialogue requires knowing the subject

Participants acknowledged that each profession had gone as far as possible towards understanding cyber risk and creating new solutions. One key element emerged from the discussions. Each

industry addressed the subject using its own definitions, its own notions, without sharing them or at least not knowing what the other professionals' understanding was (insurers, industry, IT experts etc.). It was clearly essential to share the same language to foster quality dialogue between the risk manager and the insurer, and help the insurance market develop.

Sharing common definitions conflicts with the contractual freedom of the stakeholders. Thus, while complying with competition law, a compilation of existing definitions would enable concepts shared by the majority to be identified.

Before subscribing an insurance policy, the parties must agree on elementary notions: what risk is covered? What is the insured event? What are the limits to the guarantee? Etcetera. Yet there is no cyber list to tell you which category your system belongs to, its environment compared to this or that volume of data, etc.

So what are we talking about?

Each profession talks its own professional language.

The definitions used in today's insurance policies are essentially a compilation of definitions drafted by insurers and reinsurers who, in complete contractual freedom, have made definitions that do not necessarily address the new risks. They may have duplicated definitions of risks or guarantees for known, mastered events such as fire, liability, machine breakdowns, that do not necessarily cover cyber risks.

Moreover, observing new insurance paradigms, each individual insurance or reassurance company has developed definitions that correspond to their experience of past subscription and compensation policy.

What is more, legislation providing for cyber risk is developing at both national and European level, and so past references are no longer necessarily adapted to these new risks.

The limits:

The question of legal uncertainty arises because there are many definitions and no common language has emerged spontaneously. Insured parties are concerned at the possibilities of legal uncertainty in their contracts. Agreement on the scope of the definitions may be called into question in court. Litigation can occur. In the event of a dispute or a claim, the judge may interpret the articles setting forth the contractual triggering of a guarantee, the costs, or the losses to be compensated for. He may say that the insurance policy deforms legality and that the insured event in the case does not fall under criminal law, etc. By its nature, nothing contractual can be certain since it is judged in the light of the law and general principles that are above it.

Furthermore, since cyber risk ignores borders, there can be problems with territoriality and jurisdiction. Thus the territorial nature of the guarantee against cyber risk needs to be clarified. This is a risk in itself. Let us take two transatlantic examples that herald future difficulties with digitization:

- Law changes, and at the time of writing, the French Parliament is examining the possibility of amending the bill for a Digital Republic that would enable class actions to be brought for invasion of privacy via personal data. European law is also evolving. The principle of choosing your jurisdiction in Europe has been introduced, which means you can bring a lawsuit where the law and case law are the most favourable.
- The United States created the Internet, its networks and the dematerialized cyber object, and controls its governance. Thus it seeks to maintain its freedom of manoeuver in strategic terms. It considers it can reserve its rights of pursuit and that all those using the Internet fall under its jurisdiction, following the old adage “who organizes becomes the master”. The American courts are also a tool in economic warfare. The amounts awarded by the courts in damages are high in the event of litigation. It is true that in the Safe Harbor decision of October 6 2015, the European court of justice struck down the European Commission’s decision that the United States offered a sufficient protection of European citizens’ personal data transferred there. This opens up the possibility of legal uncertainty.

Dialogue is also difficult because the technical, insurance and legal vocabulary used for cyber risk is different. The semantics are the same but express technical, insurance and legal realities that do not exactly correspond. A consistent body of categories and definitions should be drawn up from one profession to the other.

What is the interest of producing median definitions?

The UK is currently engaged in doing this in the framework of a private/public partnership (PPP) to arrive at median definitions. There is also the Cambridge Center for Risk Studies[10], which is also proposing median definitions common to the interested parties. While remaining in compliance with national and European competition rules, an upstream preparation of definitions would enable better common understanding of the subject and render contractual terms less risky at market level. Further downstream there would be more contractual freedom while providing better conditions of legal certainty in the event of litigation.

An initial attempt to compile definitions of what cyber risk encompasses was made by the seminar. A chart was produced (see extract below) showing the diverging definitions of the same object. This work must be continued. Appendix 7 provides a draft general glossary.

Heterogeneous contractual definitions and the possible lack of legal certainty are hampering the insurance market.

Why this question today? Some participants have wondered how suitable insurance of things (damages and liability) is for covering this new type of risk. It is proposed to insure a “cyber” thing which is not clearly defined legally, (data, software, robot etc.), and which is not yet quantifiable in economic terms. The insurance industry is required to compensate, pay for something that does not exist. How can indemnification be awarded when the object does not exist, has no legal reality and is not even quantifiable?

Insurance policies covering cyber risk cannot yet rely on consistent, stable digital law because it has not yet been created. Law has not dealt with this issue as a whole. It has not adapted to technical developments in this, and other fields. Some participants in the seminar argue that its basic principles, applicable to the physical world, cannot automatically be called upon to address the particular nature of digital technology and the technical reality of cyber security.

At best, the law has addressed the issue piecemeal, dealing with each profession without ever laying the foundations of digital law. However, there is considerable legal and regulatory activity at national and European levels (the development of the Information Society concerns Europe).

[10] Cambridge Risk Framework, Cyber Accumulation Risk Management : Cyber Insurance exposure data schemaV1. https://cyberpolicymagazine.com/media/k2/items/cache/2cebfdae7a8ea5d691033c085990a9d4_XL.jpg

TERMS	DEFINITIONS 1	DEFINITIONS 2	Assureur XXX	Definitions Cyber YYY	Definitions Cyber ZZZ	Assurance FFF	Definitions AAA	Courtier	Juridique	remarques	complément
Computer Systems	"Computer Systems" means computers and associated input and output devices, data storage devices, networking equipment, and back up facilities: 1. operated by and either owned by or leased to the Insured Organization; or 2. operated by a third party service provider and used for the purpose of providing hosted computer application services to the Insured Organization or for processing, maintaining, hosting or storing the Insured Organization's electronic data, pursuant to written contract with the Insured Organization for such services.	Computer System means computer hardware, software, firmware, and the data stored thereon, as well as associated input and output devices, data storage devices, networking equipment and Storage Area Network or other electronic data backup facilities.	Planning, engineering, development, delivery and installation of IT systems, software and hardware for technical, scientific and commercial data processing.	Computer system means computer hardware, software, networks, networking equipment, applications, associated electronic devices, electronic data storage devices, input and output devices, and back up facilities operated by, owned by, leased to the Insured or for which the Insured provides technology services to others for a fee by written contract for such purposes.	système d'information : Ensemble composé d'un ou plusieurs ordinateurs en réseau, de périphériques (y compris de dispositifs physiques de stockage ou de sauvegarde de Données Numériques), de logiciels et d'installations de réseau, coordonné de manière à permettre le traitement et l'échange d'informations. Est inclus dans la présente définition tout système d'information accessible par internet, intranet, extranet ou réseau privé virtuel. Système d'information de la Société souscriptrice : un système d'information : - que la société souscriptrice loue, exploite ou dont elle est propriétaire; ou - qu'un prestataire exploite pour le compte de la société souscriptrice.	Tout système de traitement automatisé de données dont l'assuré est propriétaire, tel que visé par les articles 323-1 à 323-3 du Code pénal (ou toute législation étrangère équivalente).	SYSTEME INFORMATIQUE a) Le matériel et les équipements informatiques, les logiciels et leurs composants qui font partie intégrante d'un système ou d'un réseau accessible par internet ou le réseau intranet ou connecté à une plateforme de stockage ou tout autre appareil périphérique appartenant à, contrôlé, exploité ou loué par la société souscriptrice; b) Tout ordinateur ou tout système électronique d'un tiers (y compris tout ordinateur, tout téléphone portable ou toute tablette numérique appartenant à ou sous le contrôle d'un préposé de la société souscriptrice) utilisé pour accéder au système informatique ou aux données stockées dans le système informatique; c) Les services de cloud utilisés par la société souscriptrice. L(ES POINTS b) ET c) CI-DESSUS NE SONT PAS APPLICABLES A LA « GARANTIE INCIDENT TECHNIQUE » LORSQUE CELLE-CI EST SOUSCRITE), ET A LA « GARANTIE PERTES D'EXPLOITATION SUITE A UNE INTERRUPTION DU SYSTEME INFORMATIQUE » (LORSQUE CELLE-CI EST SOUSCRITE). 63. SYSTEME INFORMATIQUE DU PRESTATAIRE D'EXTERNALISATION Les matériels ou équipements informatiques, les logiciels et leurs composants qui font partie intégrante d'un système ou d'un réseau accessible par internet ou le réseau intranet ou connecté à une plateforme de stockage ou à tout autre appareil périphérique appartenant à, contrôlé, exploité ou loué par une prestataire d'externalisation.	Système informatique : Ensemble des ressources informatiques comprenant, notamment : les matériels informatiques, progiciels, logiciels, bases de données et périphériques, équipements, réseaux, installations électroniques de stockage de données informatiques, y compris les Données. Le Système informatique de l'Assuré s'entend comme celui : • appartenant à l'Assuré et/ou; • loué, exploité ou détenu légalement par l'Assuré au titre d'un contrat avec le détenteur des droits sur ledit système et/ou ; • exploité pour le compte de l'Assuré par un Tiers dans le cadre d'une relation contractuelle et/ou ; • contractuellement mis à disposition de l'Assuré dans le cadre d'un système mutualisé.	S ystème informatique : Tout système de traitement automatisé de données dont l'assuré est propriétaire, tel que visé par les articles 323-1 à 323-3 du Code pénal (ou toute législation étrangère équivalente).	Depuis 1986, nous traitons en France **la sécurité des systèmes d'information et non pas la sécurité informatique**. Un système d'information, c'est de l'informatique, des procédures et des hommes. Les américains avaient fractionné cela en COMSEC, COMPUSEC, TRANSSEC, etc. avec l'objectif, quand nous avons mis au point les critères de sécurité européens ITSEC (qui ont abouti aux critères communs) de nous empêcher de traiter de la cryptographie. Les bonnes définitions sont les suivantes. **Sécurité des systèmes d'information** Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. **Système d'information** Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information. http://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/	**Information system** Organised set of resources (hardware, software, personnel, data and procedures) used to process and circulate information. **Information systems security** All technical and non-technical protective measures enabling an information system to withstand events likely to compromise the availability, integrity or confidentiality of stored, processed or transmitted data and of the related services that these systems offer or make accessible

Figure 2 – Sample definitions *computer systems* / système informatique (mix of French and English)

How we can reach our goal: let's talk about the same things!

To be insured, the risk must be insurable: in what conditions is cyber risk insurable? How can the risk be defined? Or quantified? When those two conditions are met, cyber risk becomes insurable, and can be the object of a contract. It will then become possible to develop a new insurance market. Insurance companies who are professionals of risk will be able to provide answers to risk managers' requests for cover.

The technical side of cyber risk will be able to join the contractual side, at the crossroads between insurance and law. This must be the object of a trans-disciplinary study so that cyber technique and vocabulary can be associated with a legal framework in which to address them.

Legal logic seeks to order legal notions before concluding contracts. There are two legal aspects: the thing to be insured and the way to insure it. The insurance contract provides for compensation for something intangible, and the other aspect concerns the intangibility as such.

It will therefore be necessary to draw up, define and divide into categories. It is difficult because cyber risk is international and a balance must be sought between the civil law and Common Law traditions. Europe must address the question quickly if it is not to be overwhelmed by the American, or English speaking, traditions. The legal work could give rise to a draft European Directive or regulation, which are the most appropriate methods for merging or connecting the main legal systems in the EU (France, Germany and the UK).

The information system and the data

Thus, the information system (IS) must be defined. What could be the median definition of an IS that confirms the technical elements are aligned, with the necessary degree of granularity, with the common, shared notions of risk control and insurance, which themselves must be grounded on a solid base of legal categories that would materialize the object and enable its qualification?

How should the scope of the IS subject of the insurance policy be understood? From an insurance standpoint, things were simple when the information was located in the same environment – the fortress keep[11] – and comprehensive cover worked well. Today, with the end of a system the scope of which was fixed in technical and insurance terms, where is the scope of my IS? In the sense of the ISO 270XX standards? Must I take into account my server application as well as the data in my server? Or is my IS beyond my server? In my message service, my CRM, in my staff data- yet salary slips are managed by DP CGI? Can the IS extend into the staff BYOD? Into the Cloud? If the data processing system owned by the client is the only thing covered by the insurance, what happens to data located in an IS he does not own (the Cloud, or a subcontractor's IS), but for which the client of the insurance policy is liable because he is liable for security as master of the data processing under Articles 34 and 35 of the law dated 1978? In fact, Article 35 provides for liability for data of personal

[11] The *memento pour la défense en profondeur appliquée aux systèmes d'information* applies best to centralized architectures that have not been completely or partly delocalized in the Cloud
see http://www.ssi.gouv.fr/uploads/IMG/pdf/mementodep-v1-1.pdf

nature including in subcontractor or external environments. (so does L 226-17 of the French Criminal Code).

Where are my data? They are volatile. Yet the European Regulation, passed on April 14 2016, provides for joint liability depending on the extent of subcontracted services, although joint liability is still an extremely vague notion. What will the impact be for insurers?

It would also be useful to conduct research so as to lay the foundations for digital or information law, so that IT data would gain legal reality (quantification and qualification), and to close the loopholes in law so as to secure the transfer of risk to insurance. Because the work to re-create law based on the notion of data was too great, it has been adapted piecemeal to create protection standards, not of the thing to be protected but standards that corresponded to the purpose of protection. Thus personal data is protected by law (1978), authors via their creation by computer (software is a work of the mind), data base manufacturers so that they can sell them, etc. Piecemeal protection measures have been developed without ever defining what data are.

Data have no legal definition; they are neither qualified nor quantified. If they are on solid ground, the insurance market can exercise creativity when drafting contractual clauses without the risk of the contract failing under litigation.

Recommendations

The approach developed in house at *Airbus Defence and Space* in the SPICE – *Scenario Planning for Identification of Cyber Exposure* – pilot, that enables the risk manager to ascertain his cyber risk exposure, could be proposed as a basis for a quantified impact analysis of business and financial cyber risk so that it could be transferred to insurance and a standard defined.

It would be helpful to compile contractual and regulatory definitions to build up common knowledge and median definitions on the model of Cambridge University's PPP.

It would be useful to identify the gaps in digital law to build up legal certainty in insurance contracts. The following issue should be addressed: must we create consistency and convergence between technical, insurance and legal elements to define the contract scope and areas of liability, and how to contain them?

Also, it is indispensable to draft the legal qualification of IT data and elements enabling its value to be quantified, for the purpose of transferring it to insurance.

V. Common categories

Obstacles

What are the common, factual categories in analysing cyber risk exposure? Is it possible to create elementary categories of cyber risk as done in periodic tables?

Once the work on median definitions has been completed, the work on defining common categories can begin and answers can be found to the following:

What common elementary categories constitute cyber-attack scenarii?

- What are insured events in insurance contracts?
- What type of risk, impact and assessment of impact?
- What information must be elicited and collected by the insurer?
- What metrics should be used?
- How can they be associated?
- What definitions are available?

V.1. Scenario management using common elementary categories

A first step was taken during an additional reality check session. It revealed that it is possible to use the elementary categories of cyber risk in the "periodic table" in describing the scenario of a cyber-attack.

The cyber risk analysis presented earlier is one that is by nature specific to each entity, due to their specific activity, structure, location etc.

The challenge is therefore to find a common set of references for a multitude of specific analyses. We draw a parallel with chemical molecules that are infinite in Nature and could be assimilated to the risk analysis scenario. All these molecules are separable into a finite number of atomic elements grouped into the periodic table, which is the common reference in chemistry.

Therefore, our study drew the analogy between the periodic table and the definition of categories of elementary risk, the purpose being to separate each scenario into a combination of these elementary risk categories. This required definition of the categories from simple to complex: molecules, atoms, and their combinations, avoiding combinatory explosion. Thus the scenario becomes a series of events comprised of predefined elements that can be used in objective metrics. This approach lays down a consistent logical system rather than an exhaustive list of scenarii. The cells of the template are the conjunction of an insured event requiring indemnification and a consequence that could be called the guarantee. The columns are the insured events and the lines the guarantees.

This led us to define a template in which the various insured events and guarantees are described so that the cells of this template are the elementary categories (like those in a periodic table).

As regards insured events, we defined sets: six categories - events causing accidental injury, damage or loss, events maliciously causing injury damage or loss, computer abuse, acts of human error and fraudulent acts.

The columns provide an additional level of detail.

As regards consequences, we considered those suffered by the insured party and then the consequences for third parties, as well as the issues of legal protection and punishment.

Each line is detailed so as to be as explicit as possible.

The following questions were examined: how can comparable results be obtained from one company to another? How can transversal elements as well as elementary categories be defined while avoiding over-complexity of combinations? The analysis is only credible if the quantitative evaluation of exposure is acknowledged by operating staff, obtains a consensus and is understood by the market.

The following method was adopted: identify causes known by all, with minimum interactions in assessing consequences, for the purpose of obtaining elements as unitary as possible.

Hence the risk manager can use the template to translate his exposure scenarii into a combination of insured events and guarantees that are our elementary categories. Each elementary category quantifies the financial exposure for each scenario, and so each scenario can be broken down into elementary categories. By doing this, the cost of each scenario can be associated with each cell involved.

In this way the common exposure reference can be created, enabling the risk manager to define his needs. He will be able to dialogue with the market. Insofar as he knows both the nature of his risk and its cost, he is better able to express his needs to the insurer. On the basis of this shared set of references, the insurer can assess the need relative to other clients in the same sector, geographical area etc., and thus give a suitable solution.

The table in figure 3 presents the empty chart that will enable the risk manager to analyse his organization’s insurance cover.

Périmètre Cyber sur le marché français		Faits générateurs dommeageables / Garanties	Evénements causant des Dommages physiques accidentels				Evénements causant des Dommages physiques par malveillance (actes crapuleux, activisme ou terrorisme si conditions légales réunies)				Malveillance informatique (actes crapuleux, activisme ou terrorisme si conditions légales réunies)												Erreur humaine					Fraude			
											Cyber attaques diffuses				Cyber attaques ciblées																	
			Incendie	Explosion / foudre	GEN, TEM : Evénements naturels	Bris de machines	Incendie volontaire	Sabotage	Vol physique (avec ou sans effraction)	Vol physique ou dégradation d'un Bien par une cyber attaque	Usurpation d'un logiciel vérifié	Virus, vers... (codes malveillants) => perte de fonctionnement	Rançongiciel par cryptolocker	Rançongiciel sur vol de données personnelles	Rançongiciel sur vol de données personnelles	Vol de données personnelles	Vol de données confidentielles / espionnage économique	Sabotage externe	Sabotage interne (salarié ou ex salarié)	Rebot d'attaque	Intrusion et maintien dans le SI sans dommage immédiat (phi...)	Déni de service	Perte ou fichiers	Usurpation d'un logiciel endommagé	Transmission involontaire de données	Autres actions immatérielles involontaires (sans dommage matériel	Autres actions immatérielles involontaires (avec dommage matériel)	Cyber détournement de fonds	Fraude téléphonique	Vol (dans all.) à escroquerie, abus de confiance, de faux, falsification de chèque	Faux ordres de Virements internationaux - Fraude au président
Dommages subis par l'assuré (1ère partie)	Dommages matériels	Bâtiments																													
		Marchandises																													
		Matériels industriels																													
		Matériels informatiques																													
	Transport	Maritime																													
		Aérien																													
	Dommages pécuniaires	Perte pécuniaire : remboursement des fonds détournés																													
		Remboursement des rançons / sommes extorquées sous la menace																													
		Frais de recours et de poursuites																													
	Pertes d'exploitation	Perte d'opportunité																													
		Perte de marge brute / de recette																													
		Frais supplémentaires d'exploitation (pour minimiser la perte de MB)																													
		Aggravation de PE à la suite d'une décision administrative légalement prise																													
	Frais informatiques	Frais de recherche de cause: - IT : Forensic, frais d expertise, d assistance... - Mat : frais d'expertise, de recherche de cause...																													
		Frais de reconstitution de données																													
		Frais supplémentaires (travaux activité sup., gestion de crise)																													
		Conseils/ préconisations après attaque/ sinistre (remédiation)																													
		Frais d'amélioration de la sécurité informatique du SI																													
	Frais liés à une violation des données personnelles	Frais de notification aux instances administratives																													
		Frais de comparution (enquêtes administratives)																													
		Frais de notification aux personnes concernées par une violation de données personnelles																													
	frais liés au rétablissement de l'E-réputation et à la communication	Conseil en communication / Relations Publiques / Gestion de crise																													
		Nettoyage- noyage																													
		Frais de référencement																													
		Plateforme téléphonique (n° vert)																													
Protection juridique	Protection juridique	Conseil juridique (hot line, gestion de crise)																													
		Assistances juridiques : mise en oeuvre de l'action juridique																													
		Honoraires d'avocats, d'huissiers, d'experts judiciaires																													
Dommages causés par l'assuré à un tiers (3ème partie)	Dépenses nécessaires à l'indemnisation des préjudices subis par des tiers du fait de la responsabilité civile de l'assuré	Dommages matériels aux tiers																													
		Dommages immatériels (aux tiers) consécutifs																													
		Dommages immatériels non consécutifs																													
		Dommages corporels (aux tiers)																													
		Frais de retraits / dépose / repose																													
		Défense recours																													
		RC des mandataires sociaux																													
Sanctions infligées à l'assuré	Amendes et pénalités	Amendes civiles (procédures abusives)																													
		Amendes administratives																													
		Amendes pénales																													
		Pénalités de retard (consécutifs au fait dommageable)																													
		Pénalités PCI -DSS (UNIQUEMENT pour les banques)																													
		Pénalités PCI -DSS (hors banques si applicable)																													

Figure 3 – Template for harmful insured events / Guarantees

V.2. Cyber risk insured events in the insurance contract

What are harmful insured events, causes, and consequences triggering compensation for cyber risk?

The list of harmful insured events drawn up by the working group is as follows:

- Events causing accidental injury damage or loss
  - Fire; Explosion / lightning; DDE (water damage), TOC (storm, hurricane, cyclone), Natural events: machine breakdown;
- Events causing malicious injury damage or loss (heinous crimes, activism or terrorism where legal conditions met)
  - Arson; Sabotage ; Robbery (with or without break in); Theft or damage facilitated by a cyber attack
- Computer abuse (heinous crimes, activism or terrorism where legal conditions met)
- Indirect cyber attacks
    - Delivery of flawed software; Virus, worms… (malicious codes) => hampering operation: ransomware via crypto locker; ransomware for personal data theft
  - Targeted cyber attacks
    - Ransomware for personal data theft: personal data theft; confidential data theft/economic spying; external sabotage; internal sabotage (staff or ex-staff); relayed attack: intrusion and stay in IS with no material damage (APT etc.); denial of service
  - Human error
    - Lost files; delivery of flawed software; involuntary data transmission; other involuntary intangible actions WITH NO damage; other involuntary immaterial actions WITH damage; fraud
  - Cyber embezzlement; telephone fraud; theft (with no break in), fraud, breach of trust, forgery and use of fraudulent documents, check forgery, forged international money orders, fraud to the Chairman or President

The Working group's list of harmful consequences subject to guarantees is as follows:

- Injury or loss to the first party
  - Damage
    - Buildings; goods; industrial equipment; IT equipment
  - Transport
    - Shipping; Air freight
  - Loss
    - Loss: refund of embezzled amounts; refund of ransoms/sums extorted by threat; legal costs
  - Operating losses
    - Loss of opportunity; loss of gross margin/revenue; additional operating costs (to minimize lost of gross margin); Aggravated operating loss due to an administrative decision legally taken
  - IT costs
    - Costs of seeking cause - IT: Forensic, consultancy fees - Mat: costs of expertise, seeking cause, cost of data reconstitution; additional costs (additional work, crisis management); Consultants/ recommendations after attack / accident (remediation); cost of improving IS security

    - Costs due to violation of personal data
        - Costs of notifying public authorities; legal costs (administrative inquiries); costs of notifying persons involved in personal data violation
    - Costs of re-establishing E-reputation and communication
        - Communication consultant / Public Relations / crisis management; Cleaning- flooding; Referencing costs; telephone platform (toll-free hotline)
- Legal protection
    - Legal consultant (hot line, crisis management); legal assistance: engaging counsel; lawyers', bailiffs', legal experts' fees
- Harm caused to a third party by the first party
    - Cost of liability for loss or injury caused to third parties by the first party
        - harm to third parties; consequent injury or loss to third parties; non-consequent injury or loss to third parties; injury (to third parties);
        - Costs of withdrawal/dismounting/remounting; legal assistance; liability of corporate officers
- Punishment of insured party
    - Fines and penalties
        - Civil fines (abusive procedures); administrative fines; criminal fines; late-payment penalties (arising from the injury or loss); PCI ·DSS penalties (ONLY for banks); PCI-DSS penalties (not including banks where applicable)

From a legal standpoint, insurance event occurrence triggers the cover.

Certain participants in the seminar wished to draw the group's attention to the use of concepts implying inappropriate legal effects. They illustrated this with the definitions of data theft, fraud and sabotage, which orient the qualification towards criminal law categories. This led to the risk of giving a national connotation of a criminal act, generally interpreted strictly. Marginal situations which are common in the cyber environment might not be covered by such vocabulary. For instance, it is difficult to equate the notion of data theft with a basic legal notion such as "illicit act" understood as "an illicit act towards data", which might include anything corresponding to appropriation and use contrary to the wishes of the owner of the data.

Recommendations

Further examination should be made of insured events so that all possible scenarii can be covered.

Another important point raised by some participants in the group was that the cause and consequence as understood by insurance do not exactly correspond to the legal notions of cause and consequence. The qualification work that will be needed must examine upstream (the insured event) and downstream (the consequence). Upstream study of categorization must avoid becoming enslaved by pre-existing legal categories or those that are pre-existing and/or ill-adapted to the cyber environment.

Metrics

In order to quantify risk, insurers need reliable, sound measurements from insured parties.

The metrics associated with cyber risk are not consolidated due to the lack of econometric modelling. Mathematical or statistical models do exist, but the entry data that feed them do not.

Because cyber incidents have not yet been counted, entered or communicated, there are no data. Stakeholders are finding it difficult to evaluate them.

An initial examination was conducted by the legal experts participating in the seminar to start the ball rolling. They chose classical metrics used in corporate finance that are commonly accepted by the insurance market. The exercise led to defining those that could be used in respect of injury or loss, or injury or loss inflicted on others. *They examined the notions of expenses, costs, fees and prices in legal and accounting vocabularies. "Expenses" is different from "costs" which can lead to economic uncertainty as to what is being indemnified (the more or less direct nature of costs. Cost is also an initial outlay for the company. Then there is a margin to add. The insured party who has suffered loss will seek to insure what the harm cost him in total, thus a price which is the amount of what was bought/sold outside.*

Fees are understood to be "outplaced services" and price must be understood as "what has been paid".

  - Attempt to clarify "% of turnover lost on the basis of an affected area and a combination of past turnover and rate of growth" which becomes "compromised turnover", with turnover fixed by reference to the turnover accrued by the affected business and its predicted rate of growth"
  - Inventory costs becomes "costs of building and managing inventory up to the amount of [-]" taking account of the notion of building up inventory.
  - Loss of production … no change.
  - Under load … no change.
  - Increased production cost the notion of "fall in production" needs to be integrated. Thus, it becomes "increased production costs (fall in production) due to changes in production methods (compensation?)".
- Legal costs… may include "fines of all kinds, deductions and penalties, contractual or otherwise (penalties imposed for punishment but which are not in a contract and can result from regulations) as mandatory punishment because behaviour has changed due to a cyber-attack putting us in the wrong.
  - Punishment, additional compulsory deductions and contractual penalties up to the amount of [--],
- Not costs but "cost of reconstructing or reconstituting up to the amount of [--], because if I buy a service from outside, it will cost money… "
  - Reconstruction… More thought is needed.
  - Costs of increasing security (addition or correction to security measures).
- Communications costs of all kinds (including crisis communication and image rebuilding- up to the amount of [--].
  - Crisis management costs up to the amount of [--], is not relevant. It should be removed, see "communication costs" line.
  - Cost of repairing, replacing and restoring data and software (including cost of re-creation, research and engineering). Check the validity of these technical concepts that cover the time taken to remedy?
  - Cost of temporary protection and prevention before final repair.

Recommendations

With the reinsurers and insurers, pursue the study of subscription metrics to identify the subscription rules that justify their prices.

Continue analysis of balanced portfolio metrics to ascertain that the situation was properly analysed (on the basis of sufficient premiums) and arrive at a sufficiently balanced claims-to-premiums ratio even if that affects capital.

Pursue work with the actuaries, certified accountants and auditors to reach convergence.

Work on quantifying cyber risk, which is needed for proper understanding of subscription metrics (value), what premium must be paid and what compensation can be expected in return for the premium.

V.3. Associate metrics and categories

Once the characteristics of each component of insured events and the harmful consequences have been roughly identified, the participants in the seminar decided to draw up a “periodic table” that would enable causes to be cross-linked with injury or loss suffered and loss inflicted on third parties, plus the underlying metrics (see the cover template in Chapter IV).

However, discussion ensued as to the elements that should be comprised in cyber-risk metrics.

The discussion raised the issue of defining the value of data that has been compromised, how to evaluate the loss or damage, how to calculate the impact on third parties, the company and insurance company’s knowledge of the consolidated cyber threat, especially in Operators of Vital Importance (OIVs) and beyond. How can descriptive tools be found so that each party can ascertain its risk exposure based on operating scenarii at instant t? What are normal conditions, what measures can reduce exposure to unpredictable risk (0-day type)? How can likelihood or frequency (possibility that it might happen) be calculated? How can maximum risk be calculated?

At this stage of analysis and the state of the art, these issues remain open.

VI. Cyber risk cover

Problems

Produce a definition and qualification of cyber accidents from the standpoints of the insured party and insurer.

Propose common, factual categories showing that an organization meets the requirements of protection against cyber risk.

Requirement to draw up a table of cover.

Producing a definition and qualification of cyber accidents from the standpoints of the insured party and insurer was an ambitious goal that would not be attained during the initial seminar. The same goes for proposing common, factual categories showing that an organization meets the requirements of protection against cyber risk. It was deemed advisable to advance in stages, first of all to decide whether it is realistic to play out cyber-attack scenarii based on elementary categories previously identified using the "periodic table" of causes and consequences. A reality check showed that this was possible on the basis of averred real life cases made public or used by market players.

The second stage was the drafting of a template for cyber risk cover based on the first table of causes and consequences and the results of the work begun by the French insurance federation (*Fédération Française d'Assurance*, FFA).

VI.1. The table of cyber risk cover: a detailed template

The research and discussions led to the drafting of a template which constitutes an overview of the French market, a summary of the insurance offer on that market. This table could then be compared with the insurance industry in other European countries and the United States.

The document presented in the work session showed whether cyber risk was covered in the various types of insurance policy (classic property damage, third party liability, Fraud). SO indicated no object. Thus classic insurance policies cover certain digital risks. Events arising from initial causes are in columns. The lines represent the harmful consequences of events. The conjunction of these two creates cells that show which category of insurance policy covers cyber risk.

A colour code is added: property damage in blue, third party liability in green; fraud in yellow. Cyber cover is in red and pink. Red indicates that digital risk is automatically covered. Red or pink cells correspond to insurance cover offered only by cyber contracts. Pink cells indicate that there are options added to the basic cyber contracts. Hatched areas show that they are covered by two policies; In this case, the risk manager must seek how to optimize cover. Black cells show what is not insurable under the law at this time, or what the market does not wish to insure. Most of the cells in the template show that the classic policies already cover digital risk. The template does not detail the type of cyber-attack, nor the type of threat (changing technical aspects).

The template allows the risk manager to associate his cyber risk analysis of his own organization with the cyber risk exposure analysis for the purpose of transferring it outside.

Thus he visualizes the structure of the French market at instant t. The template (see Table 2, appendix 8) is a photograph of current insurance cover for cyber events and shows market trends. It should be read as an analysis of how sensitive insurance cover is for cyber events.

Reduction to two dimensions should not obscure certain difficulties, such as the fact that fraud is not the same as other insurance events.

Recommendations

Insurers' communication on insurance cover for cyber risk exposure must be improved so that insured parties can be better informed and advised on their strategy for externalizing this risk.

Our research led to a representation of the way the French insurance market deals with the various risk categories set forth earlier. The photo of the current state of the market enables the risk manager better to understand how to go about things (see fig. 4). It shows how the market proposes to deal with cyber risk today.

It is time to propose a template that could serve as a benchmark for international comparisons in a highly competitive market.

The first table (figure 3) is an empty grid to allow the risk manager to analyze his organization's insurance cover. It enables him better to characterize the sensitivity of his range of cover and organize his policies. The grid should not be used to position so-called "cyber" contracts, be they specific or backed by classic contracts.

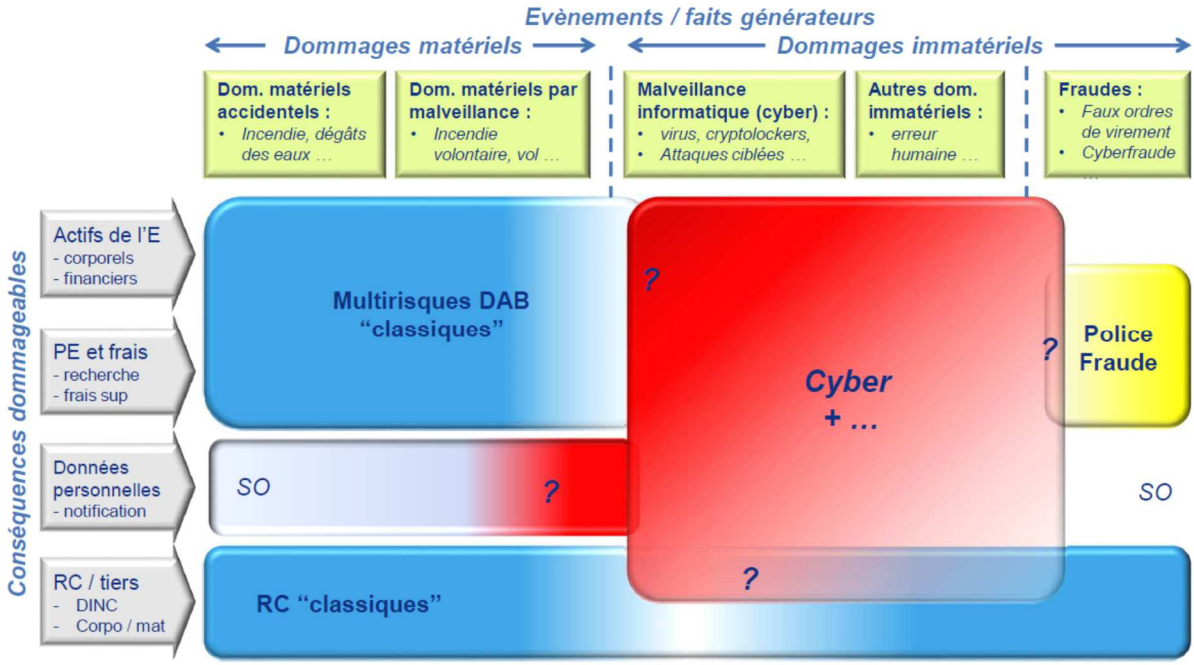
The second table (Fig. 4) provides a picture of the French market as it is at this date. It can be applied to other markets (Germany, the UK etc.) and should be reviewed over time. It facilitates dialogue between the various stakeholders by fixing a common vocabulary and separating out concepts that are often too vague.

Figure 4 – Detailed template of harmful insurance events/guarantees (next page)

.

Périmètre Cyber sur le marché français		Faits générateurs dommeageables / Garanties	Evénements causant des Dommages physiques accidentels				Evénements causant des Dommages physiques par malveillance (actes crapuleux, activisme ou terrorisme si conditions légales réunies)				Malveillance informatique (actes crapuleux, activisme ou terrorisme si conditions légales réunies)												Erreur humaine					Fraude				Commentaires
											Cyber attaques diffuses				Cyber attaques ciblées																		
			Incendie	Explosion / foudre	IDE, TOC, Evénements naturels	Bris de machines	Incendie volontaire	Sabotage	Vol physique (avec ou sans effraction)	Vol physique ou dégradation facilité par une cyber attaque	Livraison d'un logiciel vérolé	Virus, vers... (code malveillant) => entrave au fonctionnement	Ransonnage par cryptolocker	Ransonnage sur vol de données personnelles	Ransonnage sur vol de données personnelles	Vol de données personnelles	Vol de données confidentielles / espionnage économique	Sabotage externe	Sabotage interne (salarié ou ex. salarié)	Hold-up attaque	Intrusion et maintien dans le SI sans dommage immatériel (APT ...)	Déni de service	Perte de fichiers	Livraison d'un logiciel endommagé	Transmission involontaire de données	Autres actions immatérielles involontaires (DDE dommage matériel)	Autres actions immatérielles involontaires (DDE dommage matériel)	Cyber détournement de fonds	Fraude téléphonique	Vol (sans effr.), escroquerie, abus de confiance, fauxnage de flux, falsification de chèque	Vous cottez de Virements internationaux + fraude au président	
Dommages subis par l'assuré (first party)	Dommages matériels	Bâtiments	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	so	so	so	so	so	so	so	DAB	DAB	DAB	so	so	so	so	so	so	DAB	so	so	so	so	
		Marchandises	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	so	so	so	so	so	so	so	DAB	DAB	DAB	so	so	so	so	so	so	DAB	so	so	Fraude	so	
		Matériels industriels	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	so	DAB	so	so	so	so	so	DAB	DAB	DAB	so	so	so	so	so	so	DAB	so	so	Fraude	so	
		Matériels infomatiques	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	so	DAB	so	so	so	so	so	DAB	DAB	DAB	so	so	so	so	so	so	DAB	so	Fraude	Fraude	so	
	Transport	Maritime	Corps et faculté ?																								Corps et faculté ?	so	so	so	so	Exclusion du cyber (Clause 380 ou équivalents)
		Aérien	Dommage aux aéronefs, etc. ?								?																Dommages aéronefs	so	so	so	so	A l'étude
	Dommages pécuniaires	Perte pécuniaire : remboursement des fonds détournés	so	so	so	so	so	so	Fraude si pas effr	Fraude si pas effr	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	Cyber Fraude	Fraude	Fraude	Fraude	
		Remboursement des rançons / sommes extorquées sous la menace	so	so	so	so	so	so	so	so	so	so	?	?	?	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	Assurabilité des rançons en cours d'analyse
		Frais de recours et de poursuites	so	so	so	so	so	so	Fraude si pas effr	Fraude si pas effr	so	so	Cyber	Cyber	Cyber	so	so	so	so	so	so	so	so	so	so	so	so	so	Cyber Fraude	Fraude	Fraude	Fraude	
	Pertes d'exploitation	Perte d'opportunité																														Risque d'entreprise
		Perte de marge brute / de recette	DAB	DAB	DAB	DAB	DAB	DAB			so	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	DAB	Cyber Fraude	Fraude	Fraude	Fraude	
		Frais supplémentaires d'exploitation (pour minimiser la perte de MB)	DAB	DAB	DAB	DAB	DAB	DAB			so	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	DAB	Cyber Fraude	Fraude	Fraude	Fraude	
		Aggravation de PE à la suite d'une décision administrative légalement prise	DAB	DAB	DAB	DAB	DAB	DAB	so	so	so	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	Fraude	Cyber Fraude	Fraude	Fraude	Fraude	
	Frais informatiques	Frais de recherche de cause: - IT : Forensic, frais d expertise, d assistance... - Mat : frais d'expertise, de recherche de cause...	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber Fraude	Fraude	Fraude	Fraude	
		Frais de reconstitution de données	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber Fraude	Fraude	Fraude	Fraude	
		Frais supplémentaires (travaux activité sup., gestion de crise)	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber Fraude	Fraude	Fraude	Fraude	
		Conseils/ préconisations après attaque/ sinistre (remédiation)	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber Fraude	Fraude	Fraude	Fraude	
		Frais d'amélioration de la sécurité informatique du SI																														non assurable
	Frais liés à une violation des données personnelles	Frais de notification aux instances administratives	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber	Cyber	Cyber	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
		Frais de comparution (enquêtes administratives)	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber	Cyber	Cyber	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
		Frais de notification aux personnes concernées par une violation de données personnelles	so	so	so	so	so	so	Cyber ?	Cyber ?	so	so	so	Cyber	Cyber	Cyber	so	so	so	so	so	so	Cyber ?	so	Cyber ?	Cyber ?	Cyber ?	so	so	so	so	
	frais liés au rétablissement de l'E-réputation et à la communication	Conseil en communication / Relations Publiques / Gestion de crise	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
		Nettoyage- noyage	so	so	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber	Fraude	Fraude	so	
		Frais de référencement	so	so	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
		Plateforme téléphonique (n° vert)	DAB	DAB	DAB	DAB	DAB	DAB	DAB	DAB	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
Protection juridique	Protection juridique	Conseil juridique (hot line, gestion de crise)	so	so	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
		Assistances juridiques : mise en oeuvre de l'action juridique	so	so	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
		Honoraires d'avocats, d'huissiers, d'experts judiciaires	so	so	so	so	so	so	so	so	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	Cyber ?	so	so	so	
Dommages causés par l'assuré à des tiers (third party)	Dépenses nécessaires à l'indemnisation des préjudices subis par des tiers du fait de la responsabilité civile de l'assuré	Dommages matériels aux tiers	DAB	DAB	RC	RC	DAB	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	
		Dommages immatériels (aux tiers) consécutifs	DAB	DAB	RC	RC	DAB	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	
		Dommages immatériels non consécutifs	DAB	DAB	RC	RC	DAB	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	
		Dommages corporels (aux tiers)	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC / NC ?	RC / NC ?	RC / NC ?	RC / NC ?	RC / NC ?	RC / NC ?	RC / NC ?	RC / NC ?	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	
		Frais de retraits / dépose / repose	so	so	so	so	so	so	so	so	RC	so	so	so	so	so	so	so	so	so	so	so	so	so	RC	so	so	so	so	so	so	so	
		Défense recours	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	
		RC des mandataires sociaux	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC	
Sanctions infligées à l'assuré	Amendes et pénalités	Amendes civiles (procédures abusives)	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	
		Amendes administratives																														non assurable
		Amendes pénales																														non assurable
		Pénalités de retard (consécutifs au fait dommageable)	DAB	DAB	DAB	DAB	DAB / RC	DAB / RC			so	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?						Cyber / RC ?	Fraude	Fraude	Fraude	Pénalités contractuelles que les assureurs ne veulent pas couvrir
		Pénalités PCI -DSS (UNIQUEMENT pour les banques)	so	so	so	so	so	so	so	so	so	so	so	Cyber / RC ?	Cyber / RC ?	Cyber / RC ?	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	
		Pénalités PCI -DSS (hors banques si applicable)	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	so	Point de discussion !!!

Figure 5 – Summarized template of harmful insurance events /guarantees



Cyber risk may be covered by several types of policy. Pure cyber risk policies are presented in the red area.

VI.2. A proposal for a simplified template (technical standpoint)

The participants discussed a proposal for a simplified template, combining market expectations and the evolving state of the art in cyber threat.

The template presented in the work session was very explicit, didactic and pedagogical, describing current techniques. However, the threat will evolve in future and other terms will be used. How can the template follow the evolving trend? How can all-encompassing technical categories be invented that would include what exists and allow for future attacks without destroying the table? How can technical families of threat be included in the template? Should we think in terms of broad categories of attack techniques? Or should we focus on the goal of the attack: the consequence is ultimately a sort of refusal of service. Perhaps we could boil it down to a typical root category called "denial of service"?

This table (see figure 6) also reveals the market's ambivalent position, once the principle that "any damage remains covered by a property damage policy even where it results from or is aggravated by a cyber event. Third-party policies cover all cyber third-party liability except where excluded. The intersection with cyber policies is limited to non-covered injury or loss that arises from a targeted cyber-attack. The cyber policy is in addition."

Faits générateurs dommageables / Conséquences dommageables	Atteintes aux données sur attaque	Atteintes aux données sur erreur	Extorsion	Fraude	Entrave au fonctionnement sans dommage physique	Manipulation du produit ou du service client sur attaque	Manipulation du produit ou du service client sur erreur	Dommage materiel suite à attaque	Dommage materiel suite à erreur	Relais d'attaque
Actifs corporels	so	so	DAB	Fraude	so	so	so	DAB	DAB	so
Actifs financiers	so	so	Cyber	Fraude	so	so	so	so	so	so
Perte d'exploitation	Cyber	Cyber	Cyber	Fraude	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
Frais informatiques	Cyber	Cyber	Cyber	Fraude	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
Protection des données personnelles/confidentielles	Cyber	Cyber	Cyber	so	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
E-réputation / Communication	Cyber	Cyber	Cyber	so	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
Protection juridique	Cyber	Cyber	Cyber	Fraude	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
Responsabilité Civile (dommages aux tiers)	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC
Amendes et pénalités	Cyber		Cyber	Fraude	Cyber	Cyber		Cyber	Cyber	Cyber

Figure 6 – Proposal for simplified template (in French)

Traditional contracts (property damage, third party liability, corporate officers' liability etc.) extend to cover cyber events. Traditional policies will increasingly include cyber cover.

Example:

- Column G (Hindering operation): operating losses and IT costs may be indemnified by Property Damage policies. This is the case for the policies of FM, the large American insurance company that also sells in France).
- Column I (Manipulation of products): legal protection, e-reputation, fines and penalties, and data protection can be indemnified by E&O contracts.

On the other hand, specific cyber products are developing.

It is thus important to clarify what is covered by each contract so that the client avoids paying twice for the same type of cover, and also to avoid appeals that might slow down the indemnification process.

The scope of liability was the subject of considerable discussion by those participating in the seminar. In a context of cyber threat, digitized economy, ecosystems, supply chain, and subcontracting to countries outside that where the data are being used, the chain of liability can be long and difficult to identify.

Because cyber risk is unique, it imposes limits. Thus there is a high probability of litigation, all the more so as the cyber dispute may not originate in any one territory (the jurisdiction where the contract was signed? Or the jurisdiction of the injured party?). Reasoning that the insurer pays the insured party and exercises a right of action against the person liable may swiftly be found inadequate.

Cover of cyber risk, be it by property damage, third party or cyber policies, begs the question of accumulation. This is a key issue for both reinsurance and the direct insurance market.

It is crucial for insurance, which must solve the question of how to tailor the contract to the state of the art in IT and changes in information or digital law. What technical information will be needed to reach a proper qualification?

Recommendations

Pursue the work to simplify the template of insurance cover yet meet the needs of cyber technique and insurance.

VI.3. The template, towards converging definitions (from a legal standpoint)

The first stage in developing a common language has begun. It is work in progress and will be improved as we go along. The seminar enabled the beginning of convergence between the interested parties in this regard (insurance, technical, and legal professionals).

The definitions in the lines and columns began to converge during the discussions, or at least, the various representations, areas that did not overlap, and divergences emerged. All these indicated that more effort was required to reach convergence.

A certain number of words in the template were renamed, and this work must be pursued. The legal experts in the seminar proposed:

- Data theft could be renamed “illicit appropriation of data”. This is because in law, theft is a restrictive notion compared to the reality of cyber technique. Theft concerns criminal law. The notion of data theft must be brought back to the root legal notion of ““illicit act understood as illicit act towards data” which could thus cover anything corresponding to appropriation and use contrary to the wishes of the owner of the data. Then we could move onto the notions of use and appropriation.
- Personal data could be distinguished from corporate data. Personal data could become “data of personal nature” (echoing the European legal provisions). This would enable us to underline its opposition with corporate data, which are not a pre-existing legal category but must be created.
    - Proposal: replace “corporate data” by “data of organizational nature” which would cover all the data associated with operations in producing goods and services, strategy and R&T and R&D in that organization. IP data does not, in actual fact, completely correspond to the notion of corporate data. Thus any data that are not covered by IP but implemented by the company for its production of goods and services could be provided for.
- Total or part unavailability of a business service could become “total or partial obstacle to a business service”, because the notion of obstacle is more encompassing than unavailability. An obstacle can be placed by me. I can hinder without creating unavailability. Thus I create sufficient difficulty to slow or prevent production. Unavailability means to stop everything. It is the result.
- Fraud could become “use of an organization’s IS for illicit purposes”. Identity theft would then become “injury or loss arising from usurpation of identity”.

- Sabotage could become "harm caused to an IS and its physical components". The term of sabotage was actually defined in various ways, not least in the laws governing warfare.
  - The technical experts pointed out that in cyber language it is possible to "sabotage", to harm with no physical effects: to harm the integrity of intangible data, for instance.
- Harm to image (an injury as well as a cause) would become a direct and indirect injury or loss due to the detrimental effect on the image. This can cause direct injury or loss (if the image is an essential part of the value / goodwill, for instance for a law firm that offers intangible services), and indirect. The same goes for identity theft.,
- Failure to comply with an administrative rule is too restrictive. It could be changed to "direct and indirect harm due to preventing compliance with a unilateral or contractual rule".

Recommendations

Pursue the work to streamline the template.

Work must be continued with the actuaries, the certified accountants and the auditors in order to reach convergence.

Work should be done on quantifying cyber risk in order to understand subscription metrics (the value), what is to be paid, and what indemnification can be expected in the light of the premium paid out.

Issues currently under discussion

New situations[12] will need analysis and further specific study of the consequences, both substantive and procedural, of the legislative and regulatory provisions for the relevant administrative policies, the scope of cyber insurance and the way it is triggered. Such provisions are recent and innovative. The majority is based on mechanisms that are unprecedented in French law. They constitute a new legal and administrative ecosystem likely to have repercussions on the cyber environment and insurance cover.

Various questions arise:

- Ransomware. An FFA (French Insurance Federation) study is being conducted in-house. Its conclusions will be integrated into our work at a later date. From a technical and legal viewpoint, it is difficult to assign liability.
- Fraud. The intersection between fraud policies and cyber harm needs to be clarified. Its two-dimensional aspect should not obscure certain difficulties such as the fact that fraud is not of the same nature as the other insured events.
- Notification costs. The degree to which notification costs of tangible nature that cause injury or loss can be insured must be examined. This is because people whose personal data have been stolen must be notified; the nature of the theft is unknown (intangible loss) but it is due to the theft of a laptop (tangible loss). How can the contract be extended?
- Cyber terrorism. Similarly, should the risk of cyber terrorism be included in the table as of now? Should we deal with cyber terrorism in the light of the facts and the incident, rather than in the light of the insured event (by analogy with natural disasters), once the event has been qualified as "terrorist"? In the United States, this risk is covered by the underlying policy, but in Europe, most policies exclude terrorist acts (sponsored by States).

[12] Such as implementation of information-gathering techniques as provided by book VIII of the internal security code or administrative decisions to block and de-reference terrorist websites, pursuant to French law n° 2014-1353 dated 13 November 2014 on strengthening the combat against terrorism.

Three other points that are appreciated differently need to be discussed:

- Fines: only civil fines are currently insurable.
- Insurability of ransomware: this needs to be defined at European level. The UK is against…
- PCI-DSS : Currently no convergence on this technical subject.

VII. Subscription information

Blockages

In the absence of market statistics and given the existing insurance cover, how can the overall conditions for trusting dialogue between the insured party and the insurer be created? How should these conditions be defined?

Does the market need to institute trustworthy third parties that would enable data to be collected, validated and kept anonymous, and then used to make models?

Is it possible to create a joint organization defining the content and validation of a qualifying training course for cyber insurance experts?

VII.1. Confidential dialogue

What subscription information would be needed to guide and foster dialogue? Was a catalogue necessary? The AMRAE would supply examples of questionnaires.

Subscription information

For the risk manager, the questions asked have little to do with his main problem: how is his organization protected? IT exposure and a computerized organization exposure are often confused, although the latter is key when approaching cyber risk.

Few questionnaires deal with this. It is true that the insurer must ask the questions that will determine the insured party's subscription choice, but the substantive side of the subject is not dealt with.

Nor is the questionnaire based on any calculation table or set of statistics. It is not associated with metrics that would enable risk or loss ratio to be calculated, yet the insurance industry requires compliance with this.

The result of the initial work carried out by AMRAE on how subscription information in the field of cyber risk is gathered revealed the following constraints:

Companies are disinclined to describe their exposure to cyber risk. Those in sensitive activities remain cautious and communicate only at high levels.

AMRAE noted the lack of information on the positioning of medium size enterprises; Some SMEs are more open than others (high tech SMEs). Some groups, not least banks, communicate but only for the part of cyber risk governed by precise regulations.

In the cases where information was shared, it was only after a confidentiality agreement had been signed between the insurance company, the broker and the insured party.

The questionnaire was the simplest method for subscribing, in particular amongst very small enterprises, SMEs and intermediate size enterprises. However, questionnaires are increasingly rejected by clients, who no longer wish to answer yet another list of questions (cf. IT security audits etc.), all the more so as these questions are deemed intrusive.

Furthermore, in their current state, questionnaires are often ill-suited to the situation of multinational groups (several countries, what percentage of the enterprise, etc.) and also to SMEs. The latter do not feel concerned. They cannot answer the first questions if they have outplaced their IS, if they are not the owners of their information network or hardware, and if most of their data are with a host company.

So the insurer who needs to map the IS is not helped.

At the perimeter of the serious risks, dialogue with the market is thus usually via road shows. Risk managers present their overall cyber risk policy to their own company in house. The security and computer security departments demonstrate that they are covering the IS (goodwill). The company answers yes or no to the market's questions. No critical information is exchanged in respect of tool weakness, investment choices and risk control. There is nothing specific, only generalities.

Only few in house documents are revealed to the market.

What emerges is that insurers, backed by the broker, meet the client's needs on the basis of very little information. Conversely, the lack of exchange means that there is little chance of being covered should an event occur via the market.

Therefore

The market is currently content to accept this situation.

The information exchanged could therefore clearly be improved, but that supposes that organizations have in-house information on their exposure to cyber risk at their disposal for them to be able to exchange, in a form that remains to be determined.

The first condition for opening dialogue is for every organization to know its own exposure (as in the SPICE type approach).

Stakeholders' freedom must be weighed against the need to offer a consistent, effective approach so that the enterprise (via its risk manager informed by the cyber security teams) can enter into a dialogue with the market. However, a minimum framework or standard would be useful, in compliance with the provisions governing competition and individual freedoms, so that each stakeholder could address the risk in the way he chooses.

Recommendations

Have a common language, and on that basis build up a sufficiently objective and agreed metrics.

All stakeholders agree that dialogue must be improved so that more open examination of accidents (lack of information – Big Data) can be carried out.

Create a channel for dialogue so that future insured parties would have a clearer picture, a data base that would allow an actuarial study of real exposure, and a quantitative data base that would serve all interested parties.

Begin examining how very small and SMEs on the one hand, and large groups on the other, could ascertain the nature and necessary level of guarantee for the subscription information required by the market.

Work with the actuaries who know what type of information they need.

Work with Chief Data Officers and Digital Officers.

VII.2. Management of the insurance event

Data and information systems are now at the heart of corporate strategies and State concerns.

The legislator thus naturally took over this subject (2013 military planning law, LPM) and imposes confidentiality constraints on Operators of Vital Importance (OIVs).

In addition to this "statutory confidentiality", the strategic nature of cyber security also entails strict confidentiality rules in companies.

The confidentiality associated with cyber risks can appear to be in contradiction with insurance companies' rules for indemnification.

The latter have already been led to deal with this apparent contradiction in other fields (fires in sensitive sites, banks etc.). For there to be no problem after the insured event, transparent dialogue between the insured party and the insurer is paramount.

Once everyone is informed of the other parties' constraints, they must agree on the specific rules governing event management as of the subscription. This is all the more important where the constraints are legal (OIV, attorney-client confidentiality etc.). The insurance contract can then combine the constraints that bind the insurance company and the statutory requirement for the insured party to disclose the reality and amount of his loss in order to be indemnified.

The expert also plays an essential role in managing cyber events. He is trusted all the more as he is informed of sensitive facts.

Once the event has occurred, the insurance expert analyses the policy and ascertains the reality of the loss to trigger the guarantee and offer indemnification. His role is to help the parties resolve the issue.

For the expert to do a proper job in a highly sensitive environment of confidential data, the various cases where an expert is needed must be clearly provided for upstream in the contract.

Recommendations

There is a need for clarification. Perhaps it is here that an insurer can provide assistance or management in the event of a crisis, thus making his offer more convincing?[13]

[13] Jean-Laurent Santoni, *Le Ransomware est-il assurable ?*, Expertises
see http://www.expertises.info/droit-technologies-systemes-information/

VII.3. Conditions for confidentiality, the role of the public authorities

What can the public authorities offer to **develop trust for exchanges of subscription information?** What can it propose to ensure confidentiality? What should its role be now and in future? What means could ANSSI provide to establish the climate of trust needed for exchanges between the insured party and the insurer? For instance, could it be to provide qualifications for certified stakeholders? Or perhaps special forums for exchanging information? Or else to monitor insurance events? How should insurance claims and compensation be managed? What technical skills are required for checking the truth of losses and evaluating their amount?

The public authorities do not wish to be the go-between in the relationship between the insurer and the insured party (because they acknowledge the commercial nature of the relationship).

- **The public authorities may serve as a reference for good practices**

The public authorities' concern is to encourage organizations to adopt rules identical to those of Operators of Vital Importance (OIVs) and their subcontractors, and those imposed on the essential operators governed by the NIS Directive.

One of the most important sectorial decrees for application of the law on military planning (LPM) for operators of vital importance is provided for health. All decrees are built on the same template and provisions can be replicated. This decree lays down requirements: the security rules to apply, the types of IS to declare to ANSSI and the types of security incident to notify to ANSSI.

As regards personal data, the decree refers to the European General Data Protection Regulation (applicable from 25 May 2018). More generally, all the standards in the ISO 270XX category contain provisions for these good practices.

Another "virtuous" example in the field of health can be found in the Appendix to the PSSI template for health and medico-social structures: Cover for PSSIE rules (State information security policy) by the rules of the PSSI template[14].

A dedicated space for implementation of the cyber security and military planning decrees on the ANSSI website will set forth the catalogue of references to be used: what organizations must do and what documents are available. The catalogue emphasizes quality and steering.

The military planning decree (LPM) is part of a broader set of provisions concerning security and actions of vital importance (SAIV), itself based on the national security directives (DNS). It introduces the notion of an information system of vital importance (SIIV), in other words, the most critical IS of the vital importance operators (OIV), to which all the LPM obligations apply.

Sectorial decrees are publicly available, but certain appendices (those listing the typologies of attacks and the delays for applying the rules) will not be published. Most of the information exchanged between OIVs and the ANSSI during implementation of these provisions will be protected at Restricted Circulation (DR) or even Defence Secrecy (CD) level should the need for secrecy so require.

[14] See http://www.esante.gouv.fr/en/pgssi-s/espace-publication

Management of incidents reported to ANSSI under LPM will be in the charge of the COSSI (operating arm of the information security department). A secure network enabling DR information to be exchanged between ANSSI and the OIVs will be set up in 2017.

The idea of a public economic interest grouping (GIP) was mooted, a sort of national CERT to collect information on the threat, and link up with publishers, companies and users.

Recommendation

Possible avenues to explore have been indicated by public initiatives.

- **The projected assistance platform for victims of malicious cyber harm**

The National Strategy for digital security[15] announced the creation of this platform on 16 October 2015.

The ANSSI, in association with the Ministry of the Interior, is to set up an assistance platform for victims of malicious cyber harm. The purpose of this platform will be to assist all victims, from the private individual to any large corporation that is not an OIV (Operators of Vital Importance - which already benefit from ANSSI assistance in the event of cyber-attack). The platform will enable the victim to contact service providers and the police as the case may be.

Its possible role in cyber insurance is worth examining closely. The ANSSI and the Ministry have six months to define the structure and legal form for this project. A PPP (public-private entity) is envisaged.

The platform will thus deal with non-OIV stakeholders (SMEs and private individuals). It is very different from the LPM, which deals exclusively with OIVs that are in direct contact with ANSSI, more especially COSSI, which is informed of incidents.

Stakeholder qualifications: trustworthy experts

The goal is to encourage companies to call upon specialized service providers (like real estate agents) to audit and address the event. It could also apply to qualified insurance products. Qualification is based on two aspects: quality/skill and trust.

There will not be enough qualified service providers to cover all the needs for expertise. However, it seems important for insurers and insured parties to be able to rely on trustworthy experts. The client must be able, for instance, to recuse an expertise jeopardizing its business. This right of opposition should be contractual.

A new job will be required: that of “Third party trustworthy cyber expert”. This would be an addition to the PRIS basic qualification of “service provider in response to security events” already labeled by the ANSSI.

Lodging the claim – sealing order

This is not an easy question. The introduction of a lawsuit and the resultant sealing order is often detrimental to continuance of business. Many claims are not lodged because of the fear of sealing orders. However, there are legal obligations for claim lodging that must be complied with. Article 20b of the bill on a Digital Republic lays down the new conditions under which sworn public officers must intervene.

[15] http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

What is required is to synchronize the redress for the cyber incident and the investigation. One problem is to ensure that business can continue despite being affected by the needs of the investigation (document seizures, staff interrogations). These problems must be addressed when drafting and applying plans for resumption and continuation of business following insurance claims (PCA-PRA).

The new Cloud architectures obviously do not help in understanding attacks or who to accuse. Insurance contracts must provide for these aspects based on the clauses in theft contracts where the claim triggers the insurance mechanism.

There should be no link between a legal claim and reporting of the incident to the ANSSI platform. The ANSSI has no legal jurisdiction (a peculiarity of the French system). However the project does concern the ANSSI and the Ministry of the Interior and needs clarification.

The trustworthy third party in dialogue between the insurance and the insured over cyber security events

Two main problems need to be resolved:

- Guaranteeing security between the insurance company and the insured when sharing sensitive evidence , so that cyber risk can be properly qualified and quantified;
- Anonymous, relevant statistical data for calculating premiums and assisting actuaries.

Recommendations

One possible solution would be to set up a neutral platform for exchanging information between insurance company and insured party.

Idea for a platform

Study the possibility of setting up a neutral platform for exchanging information between insurance company and insured party. It could be operated by a trustworthy third party yet to be defined. This “mutualized secure platform for controlling and insuring against cyber risk” could be a non-profit making institution in the form of a public-private partnership set up jointly by the ANSSI and the insurance companies.

Further thought must be devoted to the operating process and running of this platform.

APPENDIX 1 – Invitation

Dear Sir or Madam,

You are invited to participate in an initial closed round table on the systemic aspects of cyber risk insurance.

We wish to invite private and public stakeholders interested in cyber risk and how to insure it, in the broader framework of "cyber security for tomorrow's systems". We will include the points of view of industrial clients, insurance or reinsurance companies and public regulation authorities as well as those of French and European professional associations.

The problems of controlling cyber risk throughout the value chain and its transfer to insurance will be examined during five closed seminars that will take place between November 2015 and June 2016. The goal will be to propose actions (white paper, legislative or regulatory recommendations).

They will provide an initial approach to our study so that set of European references can be drawn up for management of cyber risk. The purpose is to arrive at a standard: qualification of the insurance event from the standpoint of the industrial client and the insurer, common categories and methodology giving a sectorial framework to organizations, insurers and reinsurers that complies with legal and technical requirement; but that will also allow industrial activity to be continued in the event of attack, give a vision of the indemnification cycle, and support resumed or continued activity. On all these issues we would like to benefit from your opinions and thoughts.

We have contacted you on the recommendation of organizations and people that have already begun on these issues, and whose work is the basis of our analysis.

Our study is part of a finalized research project, EIC (Environment for interoperability and integration in cyber security) conducted at the SystemX Institute for technological research (IRT) which was set up to bring together interested public and private partners to implement the European cyber development plan. The work is funded jointly by industry, not least Airbus Group, and the General Secretariat for National Defence and Security/National Agency for Information System Security (ANSSI) The EIC project's technical goal is to develop a platform to simulate attacks on future systems. The project also has econometric and financial aspects (modelling the cost of a cyber attack and improving the insurance circuit). Its legal aspects in support of the economic development of the digital sector will conform to the European legal model.

The experts from Airbus Group, M. Philippe Cotelle (Insurance and Risk Management), Mme Bénédicte Suzan (posted to l'IRT-SystemX) with the support of M. Philippe Wolf (manager of the EIC program) will be charged with organizing and conducting the seminars and processing the results. Exchanges will be confidential.

We look forward to meeting you and remain,

Yours faithfully

Philippe WOLF

APPENDIX 2 – Participants

We consulted stakeholders in this subject via qualified persons recommended and invited to participate in our study for the first year of our research program. This list is not complete.

Insurers:

- AXA Entreprise.

Reinsurers:

- SCOR ;
- Munich-Re France.

Brokers:

- Clevercourtage ;
- Marsh.

Professional Associations:

- FERMA-AMRAE ;
- FFA ;
- CIGREF ;
- Institut des actuaires (actuaries).

Law firm

- KGA.

Risk prevention

- Bureau Véritas.

Industry, SMEs

- Airbus Group ;
- MBDA ;
- Lineon.

International Organization:

- OCDE (2 departments).

Ministry for the Economy, Industry and Digital activity

- General Directorate for enterprises (DGE) ;
- General Directorate for the Treasury, Insurance department;
- Legal Affairs Directorate (DAJ) ;
- General Council for the Economy (CGE) : Security and Risks section
- Ministry of Defence
- General Directorate for Procurement (DGA-ITE).

SGDSN / ANSSI

IRT-SystemX

- Director of EIC program;
- Researcher in charge of legal affairs.

APPENDIX 3 – Working Group

List of participant names.

Alain Ribera	alain.ribera[at]airbus.com
Bénédicte Suzan	benedicte.suzan[at]irt-systemx.fr
Cécile Vignial	cecile.vignial[at]oecd.org
Christian Daviot	christian.daviot[at]ssi.gouv.fr
Christophe Delcamp	c.delcamp[at]ffsa.fr
David Crochemore	david.crochemore[at]ssi.gouv.fr
Didier Parsoire	dparsoire[at]scor.com
Elettra Ronchi	elettra.ronchi[at]oecd.org
Elisabeth Rolin	elisabeth.rolin[at]ssi.gouv.fr
Florence Picard	florencepicard[at]aol.com
François Beaume	francois.beaume[at]bureauveritas.com
Françoise Roure	francoise.roure[at]finances.gouv.fr
Gilbert Canameras	gilbert.canameras[at]erametgroup.com
Gilbert Flepp	gilbert.flepp[at]acegroup.com
Isabelle Hirayama	isabelle.hirayama[at]irt-systemx.fr
Jean-François Pepin	jean-francois.pepin[at]cigref.fr
Jean-Laurent Santoni	jean-laurent.santoni[at]clevercourtage.com
Jean-Paul Defransure	jean-paul.defransure[at]mbda-systems.com
Laurent Bernat	laurent.bernat[at]oecd.org
Laurent Celerier	laurent.celerier[at]ssi.gouv.fr
Luc Vignancour	luc.vignancour[at]marsh.com
Laurent-Xavier Simonel	lx.simonel[at]kga.fr
Matthieu Bourgeois	m.bourgeois[at]kga.fr
Nathalie Convert	n.convert[at]ffsa.fr
Olivier Allaire	olivier.allaire[at]lineon.fr
Philippe WOLF	philippe.wolf[at]irt-systemx.fr
Philippe Cotelle	philippe.cotelle[at]airbus.com

Philippe Gaillard	philippe.gaillard[at]axa.fr
Philippe Laflandre	philippe.laflandre[at]airbus.com
Patrick Pouillot	ppouillot[at]munichre.com
Sébastien Heon	sheon[at]scor.com
Shirley Plumerand	shirley.plumerand[at]gmail.com
Stanislas Chapron	stanislas.chapron[at]marsh.com
Stéphane Spalacci	s.spalacci[at]ffsa.fr
Vincent Desroches	vincent.desroches[at]ssi.gouv.fr

APPENDIX 4 – IRT-SystemX

Labelled on February 1 2012, IRT SystemX completed the first three years of its work developing unique technological expertise and grounding via 17 research projects that bring together 61 industrial partners and 14 academic partners on its site. The objective for 2016-2020 is to develop 4 large research programs (systems engineering, autonomous transport, intelligent territories and trust-based Internet). It will also develop the use of the 7 platforms already created and increase its international presence. IRT SystemX has been set up as a foundation for scientific cooperation and future investment leverage.

The purpose is to develop market- and user-oriented applications to help industry in transforming to digital operation and production. It will thus confront the challenges of industry in design, modelling, simulation and testing of future innovations that increasingly use digital methods, via four programs:

Systems engineering: develop processes, methods and software tools for collaborative engineering for complex systems, in the broader context of big companies, while using the potential of digital technologies;

Autonomous transport: develop new, secure, safe architectures for autonomous vehicles and transport systems, integrating the new usages, critical embedded systems, and changing infrastructures and interactions.

- Trust-based Internet: develop the algorithms, protocols and architectures that will be the foundations of tomorrow's digital infrastructures and digital transformation.
- Intelligent territories: develop decisional aid tools for the optimization and operational planning of changing territories, via data collection and analysis.

The Institute operates on two main principles:

- Bringing together talent in the same place;
- Mutualizing skills and platforms.

IRT-SystemX, ANSSI and Airbus Group concluded a convention for research actions relating to protection and defence of information systems. This work concerns the economic and regulatory aspects of interactions between people and cyber security techniques. Their purpose is to promote trust in digital environment usage.

IRT research work is validated by the ANR (National research agency).

APPENDIX 5 – The EIC project

EIC : Environment for cyber security interoperability and integration. Work began on 2 February 2015. The research program was drawn up for five years. The overall cost of the project was estimated at €10M, 12 FTE (Full Time Equivalent, an increase is expected), 6 industrial partners to date (Airbus Group, Bertin, Engie, Gemalto, Prove&Run, Thalès), academic partners (UTT Troyes, IMT – Mines Télécom and CEA).

The protection of information systems and the data they transport requires complicated arbitrage between ease of use, cost of security, operating safety and compliance with constantly changing digital law so that the conditions for their deployment in an open market can be met and value can rapidly be created and the economic prosperity can be achieved.

CHESS Platform : Cybersecurity Hardening Environment for Systems of Systems funded in the amount of €1M over five years by ANSSI.

The EIC project deployed the CHESS platform for its first four applied research tasks, to assess combined cybersecurity technologies, based on innovative usage cases such as SmartGrids, Tomorrow's factory, Autonomous connected Transport and new services in the Internet of Things.

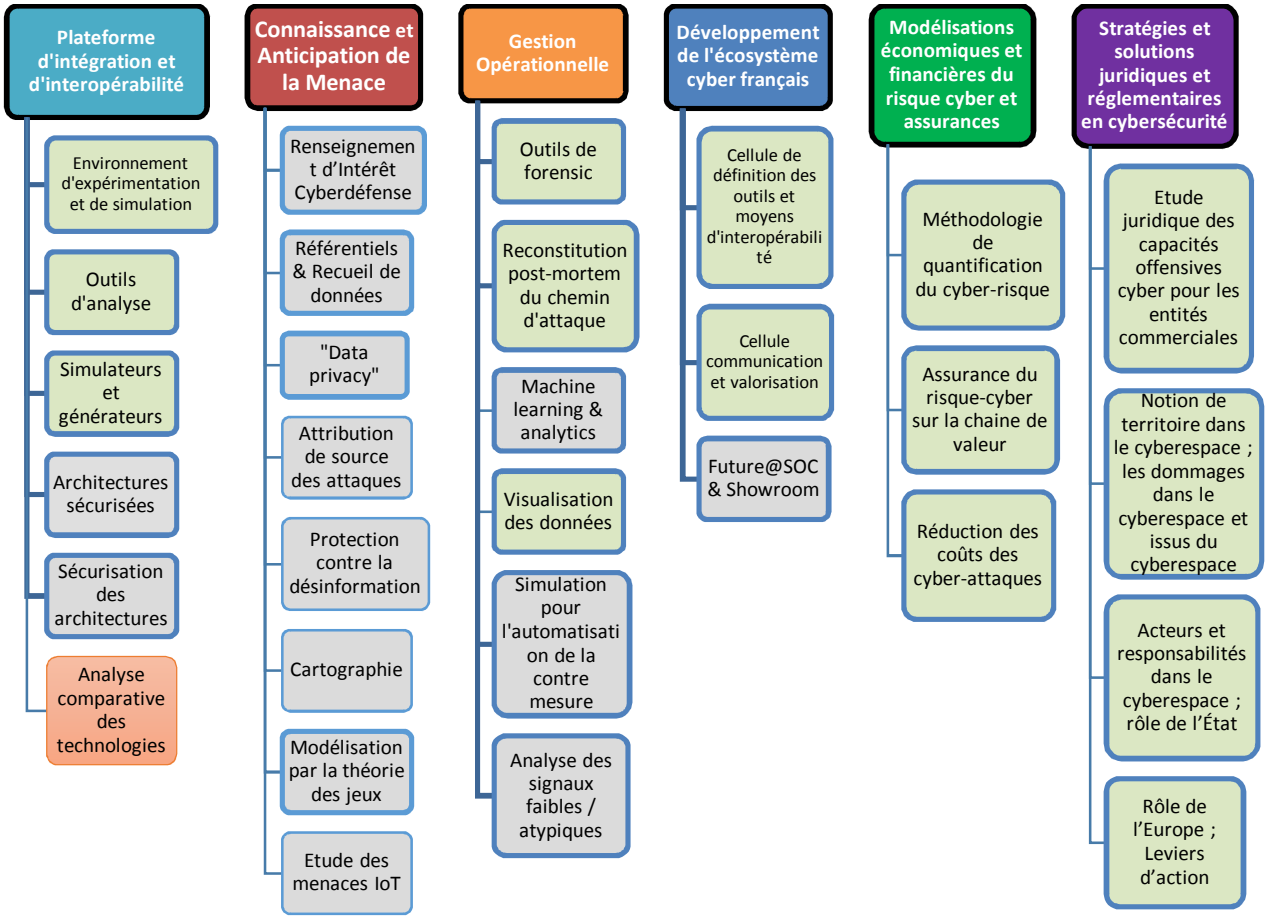


Figure 7 : Breakdown of EIC research program into tasks and sub-tasks (in French)

Since September 1 2015, Airbus Group has funded tasks 5 and 6 of EIC in continuation of tasks 2 to 4 which built up usage cases enabling insertion of these new technologies after development in the market. ANSSI also provides funding and is directly involved in defining research topics and organization. Funding of Tasks 5 and 6 has been opened to other private partners.

T5 and T6 deal with EIC tasks 1 -4 jointly and in collaboration, focusing on the economic/econometric, financial, insurance and legal aspects of cyber risk.

These two research topics are being studied by a public-private partnership that also calls upon external players whose skills and approval are indispensable *a priori*.

T5.1 is leading to innovative econometric modelling that provides quantification of the cyber risk and a representation mode that will enable corporate officers to prioritize investments in cyber assets and thus mitigate risk.

T5.2 involves the conditions required for acknowledging, managing and controlling cyber risk so that it can then be transferred to insurance. The goal will be to remove the obstacles to understanding cyber risk in an organization, and those blocking the development of the cyber security insurance market. The purpose of T5.2 is to identify the obstacles and produce recommendations for removing them in short order, via a plan of action synchronized to legislative and regulatory actions currently being taken (nationally and internationally).

The legal and regulatory work of T6 will enable EIC to introduce legal certainty by design so that the products of the applied research and innovation can be directly framed and promoted from the outset by effective provisions for industry in the European internal market, but also outside it (creating wealth and growth). Practical analysis of legal intelligence and national strategy are based on a practical analysis of law and State and industrial strategy working together at IRT SystemX.

The tools and methods of T6 will help back up T5.2 (cyber risk management /insurance) by providing expertise in legal assessment of cyber risk for industry, insurers and reinsurers, the State and the governing authorities. It will analyse the basic elements and sharing of liability to produce cyber insurance suited to the industry and the goals of national strategy in digital security.

T6 production must integrate a control and validation chain for its opinions and recommendations. The legal work will be carried out in close collaboration with the legal department of SGDSN/ANSSI. The results of the T5.2 research may thus be adopted by ANSSI, which has a national role in producing regulations and preparing bills for the French National Assembly, EU instances such as ENISA G29, and the international organizations such as the UN or the OECD.

APPENDIX 6 – Bibliography

This bibliography includes the main documents used during our work. The subject is vast and the list is not complete.

France

1. Denis Kessler, *Les sociétés modernes face aux risques extrêmes*, Risques n°76, December 2008.
2. AMRAE communicated documentation describing a "tool for cyber risk analysis and processing for insurance" drafted in partnership with CESIN. The method can be found at: http://www.cesin.fr/publications/document/download/20
3. Stéphane LIPSKI, Quantification du risque et du sinistre indemnisable : point de vue de l'expert, AFDIT, 14/04/2014, http://www.afdit.fr/media/pdf/3%20avril%202014/Probl%C3%A9matiques%20Juridiques.pdf
4. Jean-Laurent SANTONI, Loi de programmation militaire Contribution de l'assurance des cyber risques, Expertises - Avril 2014, http://www.cyberisques.com/fr/mots-cles-40-financement-cyber-risque/244-idees-jean-laurent-santoni-clever-courtage
5. Panorama d'actualités du droit de l'économie numérique, Paris 4 June 2015, AFDIT
6. Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées, L'évaluation des préjudices dans le monde numérique, Les liens de causalité au cœur de la démonstration, Colloquium 19 April 2013, http://www.lagbd.org/images/1/11/Colloque_CNEJITA_L'%C3%A9valuation_des_pr%C3%A9judices_dans_le_monde_num%C3%A9rique.pdf
7. FFSA, Panorama de la cyber-assurance, Conférence AMIECE dated November 30 2015, http://www.amiece.org/IMG/pdf/151130_AMIECE_-_Panorama_de_la_cyber-assurance.pdf
8. Grégoire Loiseau, Matthieu Bourgeois, *Du robot en droit à un droit des robots*, La Semaine Juridique, 24 November 2014, Weekly, n°48.
9. Alizée LETROSNE, Le droit des robots, Paper directed by Professeur William GILLES, 10 June 2015, Université Paris 1 Panthéon Sorbonne.
10. Jean-Laurent SANTONI, *Risques et assurances, Assurabilité des conséquences pécuniaires des cyber risques*, Expertises - April 2013.
11. Claire BERNIER, Jean-Laurent SANTONI, *L'assurance comme moyen d'indemnisation des nouveaux risques numériques de l'entreprise, Journal des Sociétés*, n°127 February 2015, http://www.clevercourtage.com/wp-content/uploads/2015/03/JSS-Lassurance-comme-moyen-dindemnis-ation-C.-Bernier-JL-Santoni.pdf
12. *L'APPLICATION DU PRINCIPE NE BIS IN IDEM DANS LA RÉPRESSION DES ABUS DE MARCHÉ Proposition de réforme*, AMF May 2015, http://www.amf-france.org/technique/multimedia?docId=workspace://SpacesStore/7cb9fffa-2fc6-45ad-babc-aee62d3f2a17_fr_1.0_rendition
13. ANSSI, *Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (cloud computing) - référentiel d'exigences*, Version 1.3 dated 30/07/2014, http://www.ssi.gouv.fr/uploads/IMG/pdf/cloud_referentiel_exigences_anssi.pdf
14. Bernard Spitz, *L'assurance face au cyberrisque*, Les échos, 27/10/2015.

15. APREF (Association of reinsurance professionals in France), *Étude sur les « cyber-risques » et leur (ré)assurabilité*, June 2016.

16. René-François BERNARD, Ilarion PAVEL, Henri SERRES, Rapport à Monsieur le Ministre de l'Économie, de l'Industrie et du Numérique, *Cyberassurance*, 20 April 2015.

17. Professional thesis by Julien Ménissez, Les cyber-assurances - Quels critères de décisions ?, Exécutive Mastère Spécialisé Management Stratégique de l'information et des Technologies, HEC Paris – MINES ParisTech, 2015.

18. FFSA, *Cyber-Risques et Protection des données personnelles*, 27 June 2016.

19. Banque de France, *Évaluation des Risques du Système financier Français*, December 2015, https://www.banque-france.fr/fileadmin/user_upload/acp/publications/ERS-001-20150715.pdf

20. Philippe Wolf, *Some considerations about privacy*, http://www.irt-systemx.fr/v2/wp-content/uploads/2015/11/privacy-pw-irt-systemx.pdf

21. Isabelle Hirayama, Bénédicte Suzan, Philippe Wolf, *Active and Proactive Defence in Cyberspace*, IRT-SystemX, 10 June 2016.

22. Decree dated 10 June 2016 on security rules and declaration methods for IS of vital importance and security incidents relating to the sub-sector of activities of vital importance: Health products, in application of articles R. 1332-41-1, R. 1332-41-2 and R. 1332-41-10 of the Defense Code, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032749532&dateTexte=&categorieLien=id

23. Decree dated 17 June 2016 on security rules and declaration methods for IS of vital importance and security incidents relating to the sub-sector of activities of vital importance: Water management , in application of articles R. 1332-41-1, R. 1332-41-2 and R. 1332-41-10 of the Defense Code, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032749580&dateTexte=&categorieLien=id

24. Decree dated dated 17 June 2016 on security rules and declaration methods for IS of vital importance and security incidents relating to the sub-sector of activities of vital importance: Food in application of articles R. 1332-41-1, R. 1332-41-2 and R. 1332-41-10 of the Defense Code,, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032749626&dateTexte=&categorieLien=id

25. Insurance Code 1 January 2016, http://www.cjoint.com/doc/16_01/FAioYVSo2cb_codedesassurances2016.pdf

EU

26. European Data Protection Supervisor, *Report Survey 2015, Measuring compliance with data protection rules in EU institutions*, 21 January 2016, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2016/16-01-21_Report_Survey_2015_EN.pdf

27. IAIS, *Global Insurance Market Report* (GIMAR) 2015, http://www.iaisweb.org/file/58465/2015-global

28. ENISA, *Big Data Threat Landscape and Good Practice Guide*, January 2016, https://www.enisa.europa.eu/publications/bigdata-threat-landscape/at_download/fullReport

29. DIRECTIVE 2009/138/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 on the *taking-up and pursuit of the business of Insurance and Reinsurance* (Solvency II), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:335:0001:0155:en:PDF

30. Regulation (UE) 2016/679 of the European Parliament and of the Council dated 27 April 2016 on protection of physical entities relating to personal data processing and free circulation of those data, repealing Directive 95/46/CE (General regulations on data protection) (of interest to the EEE) http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

31. DIRECTIVE 2016/280/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on protection of physical entities relating to personal data by the appropriate authorities for the purpose of preventing and detecting criminal offenses, investigations and claims or executing penal sanctions, and free circulation of these data, repealing the framework decision 2008/977/JAI of the Council

32. Marsh, *European 2015 Cyber Risk Survey Report*, https://www.marsh.com/uk/insights/research/european-2015-cyber-survey-report.html

33. ENISA, *ENISA Threat Landscape 2015*, https://www.enisa.europa.eu/publications/etl2015/at_download/fullReport

34. ENISA, *Threat taxonomy*, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/threat-taxonomy-2015/at_download/file

GB

35. HM Government, *Cyber Essentials Scheme: Assurance Framework*, January 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400914/bis-15-72-cyber-essentials-scheme-assurance-framework.pdf

36. Cambridge Centre for Risk Studies, Cambridge Risk Framework, Cyber Catastrophe: Stress Test Scenario, *SYBIL LOGIC BOMB CYBER CATASTROPHE SCENARIO*, June 2014, https://www.researchgate.net/profile/Scott_Kelly2/publication/263262710_Stress_Test_Scenario_Sybil_Logic_Bomb_Cyber_Catastrophe/links/0046353a45b383dfc8000000.pdf?inViewer=0&pdfJsDownload=0&origin=publication_detail

37. Cambridge Center for Risk Studies, Cambridge Risk Framework, *Cyber Accumulation Risk Management*, February 2016, http://cambridgeriskframework.com/getdocument/39

38. COI-TENANT-INSURANCE-REQUIREMENTS-2015, *LEASE AGREEMENT INSURANCE AND INDEMNIFICATION LANGUAGE*, http://230fifthave.com/wp-content/uploads/2015/08/COI-TENANT-INSURANCE-REQUIREMENTS-July-30-2015.pdf

39. Lloyd's *City Risk Index 2015-2025*, http://www.lloyds.com/cityriskindex/
Synthèse,
https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/city%20risk%20index/city%20risk%20exec%20summary_french.pdf

40. HM Government & Marsh, UK CYBER SECURITY, *THE ROLE OF INSURANCE IN MANAGING AND MITIGATING THE RISK*, March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf

Suisse

41. Zurich Insurance Group, *Zurich identifies seven cyber risks that threaten systemic shock*, https://www.zurich.com/en/media/news-releases/2014/2014-0422-01

42. Global Center for Digital Business Transformation, *Digital Vortex How Digital Disruption Is Redefining Industries*, June 2015, http://www.imd.org/uupload/IMD.WebSite/DBT/Digital_Vortex_06182015.pdf

43. Zurich Insurance Group, *Risk Nexus Beyond data breaches: global interconnections of cyber risk*, April 2014, https://www.files.ethz.ch/isn/182163/Zurich_Cyber_Risk_April_2014.pdf

USA

44. Ponemon Institute LLC, 2015 and 2016 Cost of Data Breach Study: Global Analysis, May 2015 et 2016 https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094wwen/SEL03094WWEN.PDF

45. Internet Security Alliance (ISA) / American National Standards Institute (ANSI), The Financial Management of Cyber Risk, 2010, http://www.isaca.org/chapters2/New-York-Metropolitan/membership/Documents/2011-12-15%20Adams%204.pdf

46. US Senate, Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, Hearing entitled "Examining the Evolving Cyber Insurance Marketplace.", Thursday, March 19, 2015, Written Testimony of Michael Menapace, https://www.hsdl.org/?view&did=765042

47. Senate Committee on Commerce, Science, and Transportation, March 19, 2015, Hearing "*Examining the Evolving Cyber Insurance Marketplace*", Testimony of Ben Beeson, Vice President, Cyber Security and Privacy, Lockton Companies, Ola Sage, Founder and CEO e-Management and Catherine Mulligan, SVP Zurich, https://www.hsdl.org/?view&did=765042

48. The Betterley Report, Cyber/Privacy Insurance Markey Survey, June 2016, https://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf

OCDE/OECD

49. OECD, Legal instruments in Digital economy policies, 2015, *Gestion du Risque de Sécurité Numérique pour la Prospérité Économique et Sociale*, https://www.oecd.org/fr/sti/ieconomie/DSRM_French_final_Web.pdf

Miscellaneous

50. Canadian Institute of Actuaries, Research Paper on Operational Risk, November 2014, http://www.cia-ica.ca/docs/default-source/2014/214118e.pdf

51. Airmic, *Review of Recent Developments in the Cyber Insurance Market*, https://www.scor.com/fr/sgrc/vie/risques-psychosociaux/item/1716.html?lout=sgrc

52. Garifova L.F., *Infonomics and The Value of Information in The Digital Economy*, 2nd GLOBAL CONFERENCE on BUSINESS, ECONOMICS, MANAGEMENT and TOURISM, 30-31 October 2014, Prague, Czech Republic, http://isiarticles.com/bundles/Article/pre/pdf/52169.pdf

53. Doug Laney , Infonomics: *The Economics of Information and Principles of Information Asset Management*, The Fifth MIT Information Quality Industry Symposium, July 13-15, 2011, http://mitiq.mit.edu/IQIS/Documents/CDOIQS_201177/Papers/05_01_7A-1_Laney.pdf

54. Ranjan Pal, Pan Hui, CyberInsurance for CyberSecurity, A Topological Take On Modulating Insurance Premiums, http://www.deutsche-telekom-laboratories.de/~panhui/publications/insrRP.pdf

55. PartnerRe, *CYBER LIABILITY INSURANCE, MARKET TRENDS: SURVEY*, October 2015, http://www.partnerre.com/assets/uploads/docs/PartnerRe_Cyber_Liability_Trends_Survey_2015.pdf

56. Institute of Insurance Economics, University of At. Gallen, INSURABILITY OF CYBER RISK: AN EMPIRICAL ANALYSIS, January 2015, http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf

57. InfoCyndinique, http://ifrei.org/tiki-index.php?page=InfoCindynique

58. Nassim Nicholas Taleb, *Silent Risk*, https://drive.google.com/file/d/0B8nhAlfIk3QIR1o1dnk5ZmRaaGs/view?pref=2&pli=1

APPENDIX 7 – Glossary (French and English)

This is a preliminary work to be consolidated. It does not commit the insurance market.

ASSURÉ

Personne qui est garantie par un contrat d'assurance. [Larousse]

THE INSURED

The person, group of people, or organization that is insured in a particular agreement [Cambridge Dictionary]

ASSUREUR

Personne qui s'engage, moyennant le paiement d'une prime ou d'une cotisation, à payer à l'assuré ou au bénéficiaire désigné un capital ou une rente en cas de survenance d'un risque déterminé. [Larousse]

INSURER

A person or company that insures someone or something [Cambridge Dictionary]

ATTEINTE AUX DONNÉES

En droit de l'informatique, ce que l'on nomme communément le piratage relève des atteintes aux systèmes de traitement automatisé de données (STAD). Issues initialement de la loi dite « Godfrain » ces infractions se retrouvent principalement sous les articles 323-1 à 323-7 du code pénal.

La définition ci-après n'est pas consolidée.

1. Toute altération, destruction, suppression, corruption, inutilisation, illisibilité, inaccessibilité, impossibilité de traitement des ***données***, résultant :

- de tout acte commis par un ***préposé*** de l'***assuré*** ou par un ***tiers*** visant à accéder ou se maintenir frauduleusement, dans tout ou partie du ***système d'information*** de l'***assuré*** ou à entraver ou fausser le fonctionnement du ***système d'information*** de l'***assuré,***
- d'une attaque en ***déni de service***,
- de la réception ou la transmission d'un ***code ou logiciel malveillant***,
- d'un incident technique affectant le système d'information de l'assuré,
- d'un dommage matériel affectant le système d'information de l'assuré,
- d'une erreur humaine ou erreur de programmation,
- d'une interruption non intentionnelle et imprévue du ***système d'information*** de l'***assuré.***

2. Toute divulgation ou transmission sans autorisation de ***données.***

3. Toute soustraction frauduleuse de ***données.***

4. Toute violation de la ***norme PCI DSS.***

INFRINGEMENT

An action that breaks a rule, law, etc. [Cambridge Dictionary]

CODE OU LOGICIEL MALVEILLANT

Programme ou application, notamment virus, logiciel espion, vers informatique cheval de Troie, ransomware, keyloggers, …, conçu aux fins d'accéder ou de se maintenir frauduleusement au sein du ***système d'information***, d'en surveiller, entraver ou fausser le fonctionnement ou d'introduire, altérer ou détruire des informations qu'il renferme. [ANSSI[16]]

MALWARE

Computer software that is designed to damage the way a computer works [Cambridge Dictionary]

CONSÉQUENCES PÉCUNIAIRES DE LA RESPONSABILITÉ CIVILE

Mise en jeu de la Responsabilité civile de l'assuré pour couvrir les dépenses nécessaires à l'indemnisation des préjudices subis par des tiers lorsque l'assuré en est civilement responsable. Ces préjudices sont :

- Dommages corporels subis par les tiers : un dommage portant atteinte à l'intégrité physique d'une personne autre que l'assuré (blessures, invalidité ou décès
- Dommages matériels subis par les tiers : toute détérioration ou destruction totale ou partielle d'un bien matériel appartenant à un tiers.
- Dommage immatériel : « tous dommages autres que corporels ou matériels » c'est-à-dire soit la réparation des dommages moraux (préjudices extrapatrimoniaux telles que les atteintes à la réputation, à la considération…), soit la réparation de dommages pécuniaires.

Les assureurs, dans leur définition des dommages immatériels, mettent généralement l'accent sur les dommages pécuniaires : « tout préjudice pécuniaire résultant de la privation de jouissance d'un droit, de l'interruption d'un service rendu par une personne ou par un bien ou de la perte d'un bénéfice ». Il s'agit de réparer le gain manqué par le tiers. On distingue :

- Dommages immatériels consécutifs à un dommage garanti: Dommage pécuniaire subi par le tiers victime et qui est la conséquence directe d'un dommage matériel ou corporel garanti par le contrat RC de l'assuré.
- Dommages immatériels consécutifs à un dommage non garanti : Dommage pécuniaire, subi par le tiers victime, qui n'est pas la conséquence d'un dommage matériel ou corporel garanti par le contrat RC de l'assuré.

Le tiers subit un dommage corporel ou matériel mais ce dommage n'est pas garanti par le contrat RC souscrit par l'assuré. Seules les conséquences pécuniaires (manque à gagner) de ce dommage initial sont garanties. Le dommage initial doit être susceptible de mettre en jeu la responsabilité de l'assuré (ex : vices cachées).

[définitions issues des conventions spéciales incendie de l'APSAD (Assemblée Plénière des Sociétés d'Assurances Dommages), 1982. Elles peuvent varier d'un assureur à l'autre]

MONETARY CONSEQUENCES OF LIABILITY

CYBER-EXTORSION

[non consolidé]

[16] Le glossaire de l'ANSSI définit l'ensemble des termes techniques relevant de la SSI, voir http://www.ssi.gouv.fr/entreprise/glossaire/

Toute action ou menace d'action sur les ***données*** ou sur le ***système d'information*** de l'***assuré*** dans le but d'obtenir une rançon.

La forme la plus répandue de cyber-extorsion consiste à demander une rançon contre la remise d'une clé permettant le décryptage des données[17].

CYBERSÉCURITÉ

État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre **la disponibilité, l'intégrité ou la confidentialité** des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. [ANSSI]

CYBERSECURITY

The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyberdefence. [ANSSI]

Ways of protecting computer systems against threats such as viruses [Cambridge Dictionary]

CYBER-TERRORISME

Dans le droit français, le terrorisme est « une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur ».

Toute action ou menace de destruction, dégradation, modification ou perturbation (y compris ***déni de service***) des ***données*** et/ou du ***système d'information*** de l'***assuré*** dans le but de causer des dommages et/ou d'intimider toute personne pour des raisons sociales, idéologiques, religieuses, politiques ou tout objectif similaire. [non consolidé]

CYBERTERRORISM

The use of the internet to damage or destroy computer systems for political or other reasons [Cambridge Dictionary]

DÉNI DE SERVICE

Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. [ANSSI]

Privation totale ou partielle d'origine malveillante du service des ***systèmes d'information*** de l'***assuré*** sans que les équipements informatiques, les équipements de télécommunication ou les installations d'infrastructure de l'***assuré*** subissent un ***dommage matériel*** ou une destruction. [non consolidé]

DENIAL OF SERVICE

A situation in which people intentionally prevent a website from operating by sending too many requests to use it [Cambridge Dictionary]

DOMMAGE CORPOREL

[17] Voir http://cyber-serenite.fr/cyber-lexique

Un dommage portant atteinte à l'intégrité physique d'une personne [APSAD].

BODILY INJURY

DOMMAGE MATÉRIEL

Toute détérioration d'un bien meuble ou immeuble, toute atteinte physique à des animaux [APSAD].

MATERIAL DAMAGE

DOMMAGE IMMATÉRIEL

Tous dommages autres que corporels ou matériels. C'est-à-dire soit la réparation des dommages moraux (préjudices extrapatrimoniaux telles que les atteintes à la réputation, à la considération…), soit la réparation de dommages pécuniaires [APSAD].

IMMATERIAL DAMAGE

DONNÉE

Représentation conventionnelle d'une information en vue de son traitement informatique [Larousse].

Toute information échangée, traitée et/ou stockée sous format électronique et/ou tout média digital, notamment les ***données personnelles*** et les ***données confidentielles,*** les logiciels et les supports de ***données***. [non consolidé]

DATA

Information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer [Cambridge Dictionary]

DONNÉES CONFIDENTIELLES

Toute information confidentielle appartenant ou confiée à l'***assuré***, tels que les procédures, les documents, les dessins, les formules ou les informations protégées par un secret professionnel institué par la loi, les règlements, les usages ou qui ne sont pas dans le domaine public. [non consolidé]

DONNÉES PERSONNELLES

Donnée à caractère personnel : « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne » [Art. 2 loi I&L].

Toute information identifiant ou permettant d'identifier une personne physique par référence notamment à un numéro, un nom, un mot de passe, des éléments ou critères qui lui sont propres (y compris les données médicales), appartenant ou confiée à l'***assuré***. [non consolidé]

PERSONAL DATA

Personal data shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. [EU Data Protection Directive (95/46/EC)]

ERREUR HUMAINE

Toute négligence ou erreur commise par un ***préposé*** de l'***assuré*** ou par un prestataire externe dans le cadre de l'exploitation, la maintenance et la mise à jour du ***système d'information***. [non consolidé]

ERREUR DE PROGRAMMATION

Toute erreur de conception, de développement ou d'encodage d'un logiciel, d'une application, d'un système d'exploitation ou d'un micro-code. [non consolidé]

FAIT DOMMAGEABLE

Le ***fait dommageable*** est celui qui constitue la cause génératrice du dommage ; un ensemble de ***faits dommageables*** ayant la même cause technique est assimilé à un ***fait dommageable*** unique. [non consolidé]

HARMFUL EVENT

FAUTE PROFESSIONNELLE

Toute faute ou tout acte fautif, tout manquement, toute négligence ou omission, toute déclaration inexacte ou trompeuse, toute infraction aux dispositions légales, réglementaires ou statutaires, commise dans le cadre des activités de l'***assuré***. [non consolidé]

MALPRACTICE

Failure to act correctly or legally when doing your job, often causing injury or loss [Cambridge Dictionary]

FRAIS DE COMMUNICATION ET DE NOTIFICATION

Frais liés à une violation de l'obligation de protection des données personnelles : dépenses engagées par l'assuré pour se conformer à ses obligations légales ou règlementaires à la suite d'une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles, ou l'accès non autorisé à de telles données.

Cette garantie porte sur :

- \- Les frais de notification aux instances administratives (CNIL, Premier ministre et ANSSI)
- \- Les frais de comparution (enquêtes administratives)
- \- Les frais de notification aux personnes concernées par la violation de ses données à caractère personnel [APSAD].

FRAIS DE DÉFENSE

Les honoraires et frais engagés par l'***assuré*** pour les besoins de sa défense, notamment :

- -les frais d'avocats,
- -les frais d'expertise,
- -les frais de procédure et de comparution. [non consolidé]

FRAIS DE MONITORING ET SURVEILLANCE

Frais engagés par l'***assuré*** avec l'accord préalable de l'***assureur*** pour détecter et contrôler en cas d'***atteinte aux données*** toute éventuelle utilisation inappropriée. [non consolidé]

FRAIS DE RESTAURATION

Les frais engagés par l'***assuré*** pour déterminer si les ***données*** peuvent ou non être restaurées ou reconstituées, pour décontaminer, nettoyer, restaurer, reconstituer les ***données*** et leur support.

Les frais d'adaptation, de reconfiguration de logiciels, le coût d'acquisition des licences de remplacement.

Le coût d'initialisation des systèmes de contrôle d'accès. [non consolidé]

FRAIS DE RESTAURATION D'IMAGE

Frais liés au rétablissement de l'E-réputation et à la communication : dépenses engagées pour rétablir la réputation/l'image de l'assuré auprès du public.

Sont compris, les frais de :

- Conseil en communication / relations publiques / Gestion de crise : frais liés aux conseils délivrés par des professionnels de la communication et de la gestion de crise.
- Nettoyage / noyage : technique consistant à développer sa présence sur le web (et donc sur les moteurs de recherche) dans le but de faire reculer les résultats gênants dans les toutes dernières pages de résultats. Pour que les informations négatives concernant l'entreprise visée soient les moins visibles possible des internautes, les informations négatives vont être noyées en créant de nombreux contenus.
- Frais de re-référencement : frais destinés à payer des informaticiens ou acheter un logiciel pour faire en sorte que le site web de l'entreprise soit à nouveau visible et en première page dans les moteurs de recherche.
- Plateforme téléphonique : Frais liés à la mise en place de frais de téléphonie supplémentaire afin d'informer et/ou de répondre à la clientèle [APSAD].

FRAIS ET PERTES CONSÉCUTIFS A LA VIOLATION DE LA NORME PCI DSS (Payment Card Industry - Data Security Standard)

Les frais engagés et pertes supportées par l'***assuré*** résultant de la violation par l'***assuré*** de la ***norme PCI DSS***, dont :

- Les honoraires d'expert mandaté en vue d'identifier l'origine de la violation de la ***norme PCI DSS***,
- Les pénalités contractuelles imposées à l'***assuré***,
- Les frais engagés en vue de l'obtention du renouvellement de la certification aux ***normes PCI DSS***,
- Les frais de réémission des cartes bancaires. [non consolidé]

FRAIS LIÉS A UNE MENACE DE CYBER-EXTORSION

Dommage pécuniaire : pertes de fonds ou de valeurs monétaires consécutives à des agissements à caractère délictueux tels que des escroqueries, extorsions, chantages, abus de confiance ou de biens sociaux.

Il s'agit d'obtenir de l'assureur :

- Le remboursement des fonds détournés, des rançons ou des sommes extorquées
- La prise en charge des frais de recours et de poursuite contre l'auteur du délit

Attention : la notion d'actifs financiers peut, là encore, prêter à confusion dans la mesure où ce terme désigne tout titre ou contrat, généralement transmissible et négociable sur un marché financier, qui est susceptible de produire à son détenteur des revenus ou un gain en capital, en contrepartie d'une certaine prise de risque. La notion est donc inappropriée pour l'assurance, il serait préférable de lui substituer celle de dommages pécuniaires puisqu'il s'agit de faire état d'une perte de fonds pour l'entreprise, d'une atteinte à sa trésorerie, consécutive à une infraction pénale appauvrissant le patrimoine de la victime [APSAD].

FRAIS SUPPLÉMENTAIRES D'EXPLOITATION

Les frais exposés par l'***assuré*** afin de limiter la durée d'interruption du ***système d'information***. [non consolidé]

FRANCHISE

Clause d'une assurance qui fixe un montant restant à la charge de l'assuré en cas de dommage ; ce montant lui-même. [Larousse]

INCIDENT TECHNIQUE

Défaillance ou panne mécanique des composants critiques du ***système d'information*** de l'***assuré*** qui détruit, altère, rend illisible ou inaccessible les ***données*** et résultant notamment des évènements suivants :

- Surcharge électrostatique ou perturbations électromagnétiques
- Surchauffe
- Action de l'électricité ou de la foudre [non consolidé]

MONTANT DE LA GARANTIE

Le montant maximal d'indemnisation, y compris les ***frais de défense***, par ***sinistre*** et par ***période d'assurance***. [non consolidé]

AMOUNT OF COVERAGE

NORME PCI DSS

Norme publiée de sécurité des données (DSS) pour l'industrie des cartes de paiement (PCI).

PÉRIODE D'ASSURANCE

La période comprise entre :

- la date d'effet du contrat et la première échéance principale,
- deux échéances principales, sans pouvoir être supérieure à 12 mois consécutifs,
- la dernière échéance principale et la date de cessation des garanties. [non consolidé]

PRÉPOSÉ

Toute personne physique salariée ou non de l'***assuré***, agissant sous la direction, les ordres et la surveillance de l'***assuré***, y compris les stagiaires rémunérés ou non, les apprentis, les auxiliaires de vacances, le personnel intérimaire, le personnel détaché.

Par dérogation à ce qui précède, toute société ou toute personne externe à l'entreprise de l'***assuré*** mandatée par l'***assuré*** pour fournir des services informatiques, étant précisé que l'***assureur*** se réserve expressément le droit d'exercer tout recours subrogatoire à l'encontre de ces sociétés ou personnes.

Les mandataires sociaux salariés de l'***assuré*** sont également considérés comme ***préposés***. [non consolidé]

ATTENDANT

Someone whose job is to be in a place and help visitors or customers [Cambridge Dictionary]

PRESTATAIRE D'EXTERNALISATION

Toute entité extérieure à l'assuré à l'exception du prestataire de service de cloud et qui lui fournit des services déterminés dans la limite des missions qui lui ont été confiées, notamment un service externalisé de gestion de la paie, d'hébergement web, de marketing ou de prospection, qu'elle agisse ou non en vertu d'un engagement contractuel exprès. [non consolidé]

RÉCLAMATION

Toute mise en cause expresse fondée sur une ***faute professionnelle***, réelle ou alléguée, à l'encontre de l'***assuré*** pendant la ***période d'assurance*** prolongée le cas échéant par la période de garantie subséquente.

Est assimilée à une ***réclamation*** toute déclaration faite par l'***assuré*** à l'***assureur*** concernant des dommages ou évènements susceptibles de relever des garanties du présent contrat. [non consolidé]

CLAIM

A written request asking an organization to pay you an amount of money that you believe they owe you [Cambridge Dictionary]

Depending on the context this term may refer to: (a) a demand made by a policyholder on his insurer(s) for payment or some other contractual benefit under an insurance policy; (b) a demand made by an insurer on its reinsurer(s) to be paid under a reinsurance contract; or (c) a demand made by a third party on a policyholder to be compensated for some injury, damage or loss for which the third party blames the policyholder. A claim is payable under an insurance or reinsurance contract if it is caused by an insured peril and it is not excluded under the terms of that contract [https://www.lloyds.com/common/help/glossary?Letter=C].

SANCTION ADMINISTRATIVE

Amendes et pénalités : sanctions d'ordre pécuniaire encourues par l'assuré à la suite d'une méconnaissance de ses obligations légales, réglementaires ou prudentielles, de nature civile, pénale, administrative ou contractuelle.

- Amendes civiles (ou à des dommages et intérêts pour action dilatoire ou abusive (article 32-1 CPC) ou pour appel dilatoire ou abusif (article 559 CPC) : elles ne sont pas assurables. Il s'agit de la condamnation à des dommages intérêts pour procédure abusive (application particulière du droit de la responsabilité civile pour faute). Il s'agit de sanctionner l'abus d'exercice du droit d'ester en justice ou d'interjeter appel.
- Amendes pénales : elles ne sont pas assurables et proviennent d'une condamnation prononcée par une juridiction répressive.
- Amendes administratives : elles ne sont pas assurables. Sanctions pécuniaires prononcées par des autorités administratives indépendantes ayant un pouvoir de sanction et après constatation du non-respect de règles prudentielles, légales ou règlementaires [APSAD].

Toute sanction pécuniaire assurable infligée à l'***assuré*** par un organisme gouvernemental, un organisme officiel, une instance administrative, institué en application des règlementations de protection des ***données*** (notamment la CNIL en France), en conséquence d'une violation de la règlementation sur la protection, conservation, confidentialité des ***données***.

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre **la disponibilité, l'intégrité ou la confidentialité** des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. [ANSSI]

Information systems security

All technical and non-technical protective measures enabling an information system to withstand events likely to compromise the availability, integrity or confidentiality of stored, processed or transmitted data and of the related services that these systems offer or make accessible. [ANSSI]

SERVICE DE CLOUD

Tout accès à des infrastructures ou plates-formes informatiques hébergées chez un prestataire informatique avec lequel l'***assuré*** a passé une convention à cet effet. [non consolidé]

CLOUD SERVICE

A cloud service is any resource that is provided over the Internet. The most common cloud service resources are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

SINISTRE

Garantie pertes et frais :

- La connaissance par l'***assuré*** d'une ***atteinte aux données***.

Garantie responsabilité civile :

- Toute ***réclamation*** adressée à l'***assuré*** ou à l'***assureur***.

Constitue un seul et même ***sinistre*** tout dommage ou ensemble de dommages causés à des ***tiers*** engageant la responsabilité de l'***assuré***, résultant d'un ***fait dommageable*** et ayant donné lieu à une ou plusieurs ***réclamations***. [non consolidé]

DISASTER?

SYSTÈME D'INFORMATION

Ensemble organisé de ressources (**matériels, logiciels, personnel, données et procédures**) permettant de traiter et de diffuser de l'information. [ANSSI]

Matériel, équipement informatique, logiciels (et leurs composants) qui font partie intégrante d'un système ou d'un réseau accessible par internet ou réseau intranet ou connecté à une plateforme de stockage ou tout appareil périphérique exploité par l'***assuré*** ;

Tout ordinateur ou système électronique d'un ***tiers*** utilisé pour accéder au ***système d'information*** ou aux données stockées dans le ***système d'information.***

Toute plate-forme de stockage ou de traitement et tout autre appareil périphérique ou ***système d'information*** appartenant à, contrôlé, exploité ou loué par un ***prestataire d'externalisation***.

Les ***services de cloud*** utilisés par l'***assuré***. [non consolidé]

INFORMATION SYSTEM

Organised set of resources (hardware, software, personnel, data and procedures) used to process and circulate information. [ANSSI]

TIERS

Toute personne autre que le ***souscripteur*** et, dans l'exercice de leurs fonctions, ses représentants légaux et ses ***préposés***. [non consolidé]

THIRD PARTY

A third person or organization less directly involved in a matter than the main people or organizations that are involved [Cambridge Dictionary]

-_-_-_-_-