ASSOCIATION DES **PROFESSIONNELS**
DE LA **RÉASSURANCE** EN **FRANCE**

JUIN 2016

# Etude sur les « cyber risques » et leur (ré)assurabilité

Délégation Générale : B. DOLLFUS – tél +33 (0)1 42 47 90 10
Secrétariat Général : J-M. SZMARAGD - tél +33 (0)1 58 44 76 41
Siège : 26 boulevard Haussmann – 75009 Paris France - Site : www.apref.org

# SOMMAIRE

# TABLE DES MATIERES

# RESUME

*Une transformation radicale affecte aujourd'hui profondément, sur une échelle planétaire, l'ensemble des sociétés comme les divers volets de l'économie :* ***la révolution numérique****. L'économie mondiale est désormais interconnectée par des moyens et à travers des réseaux électroniques, d'immenses masses de données et d'informations collectées, souvent confidentielles, transitent ou sont stockées dans des espaces virtuels, tandis que production, gestion, transactions, infrastructures…sont toujours davantage commandées et contrôlées à distance, et automatisées.*

*Il en résulte un* ***système extrêmement vulnérable*** *aux intrusions, attaques, erreurs humaines, accidents… qui se multiplient en dépit des parades mises en œuvre de façon permanente par les professionnels. Un nouveau risque a surgi, le « cyber risque », qui pourrait devenir l'un des risques majeurs du monde d'aujourd'hui et, au fur et à mesure d'avancées technologiques en progression fulgurante, encore bien davantage de celui de demain. De par la concentration des systèmes d'exploitation informatique et des logiciels, le « cyber risque » a un caractère multiplicatif, qui en fait un risque potentiellement* ***systémique et international.*** *Il s'est dès lors imposé au cœur des préoccupations des différents acteurs au niveau national comme à l'échelon mondial et est devenu un des principaux risques pour les entreprises, les collectivités et les pouvoirs publics, ainsi qu'un des thèmes centraux de défense nationale.*

*Ce risque appelle un* ***besoin fondamental de protection*** *pour les acteurs de la vie sociale et économique, dont le fonctionnement, les moyens financiers, la réputation, voire la survie même pour les entreprises ou, pour les individus, en cas de dysfonctionnement entrainant des dommages corporels, peuvent être menacés. C'est notamment le rôle de l'assurance et de la réassurance de contribuer à cette protection, et le marché (ré)assurantiel du cyber- risque est en plein essor. Son taux de pénétration toutefois reste faible. Les capacités potentielles ne peuvent se développer de façon pérenne que si les acteurs parviennent à mieux appréhender ce risque et donc à limiter ses effets grâce en particulier à une connaissance des expositions et des sinistres survenus, permettant de le modéliser et d'établir les cumuls éventuels d'exposition. Il n'est aussi assurable que si tous les moyens de prévention sont mis en œuvre pour en limiter la survenance et l'impact, tant au plan technique qu'en termes d'encadrement réglementaire.*

*L'APREF souhaite par cette note contribuer à une* ***réflexion sur le « cyber risque » qui favorise son assurabilité et permette une meilleure protection des acteurs****. L'illustration du risque par des exemples de sinistres connus permet de mieux encadrer sa définition et favorise sa compréhension. L'APREF s'appuie par ailleurs sur l'approche du CRO Forum (Forum des « Chief Risk Officers » des grandes sociétés d'assurance et de réassurance européennes) pour proposer une* ***définition objective du « cyber risque ».***

*Nombre d'organismes se penchent sur la* ***problématique assurantielle du « cyber risque »,*** *dont l'OCDE qui vient de lancer une enquête par le biais d'un questionnaire adressé aux entreprises d'assurance et de réassurance, destiné à la publication de rapports correspondant à différentes facettes et enjeux du marché. Le marché se développe, mais de façon encore*

*souvent hétérogène rendant plus complexe son accessibilité. La profession cherche des garanties adaptées à ce nouveau risque, vulnérable entre autres aux pertes immatérielles. Cette note s'efforce de faire un* ***état des lieux des couvertures assurantielles disponibles,*** *qu'elles préexistent –parfois de façon simplement implicite- dans des contrats traditionnels ou soient proposées dans le cadre de contrats nouveaux, dédiés spécifiquement au « cyber risque », ainsi que de faire des préconisations en faveur du développement d'un marché sécurisé, auquel devraient contribuer les nouvelles directives européennes et différentes réglementations nationales et internationales. Il reste un différentiel entre besoins de protection et offres de garanties, sachant toutefois que de plus en plus de compagnies offrent en sus à leurs assurés une panoplie de services tendant à faciliter l'analyse et la maitrise de risques et à améliorer la prévention. Compte-tenu de l'ampleur des enjeux, la réassurance est appelée à jouer un rôle central dans la protection du marché qu'elle peut faire bénéficier de son expérience internationale.*

*L'APREF oriente ses recommandations d'abord sur* ***l'information et la prévention*** *qui doivent être au cœur de la réglementation future et des remontées d'expérience des différents acteurs car il est important que le cadre législatif et règlementaire, comme le marché, contribuent à l'élaboration et l'amélioration de bases de données anonymisées et sécurisées, en particulier en termes de sinistralité. Ensuite sur la* ***prévention et la limitation du potentiel de destruction*** *qui doit être encouragée par tous les moyens non réglementaires en coopération avec les organismes spécialisés et les pouvoirs publics. Enfin en proposant une première approche du* ***risque cumulatif potentiel*** *s'appuyant sur divers scenarios de cumuls, ce qui entraine pour des raisons de sécurité la limitation de garanties découlant de cette crainte d'un évènement majeur affectant l'ensemble de la chaine.*

# INTRODUCTION

A la révolution industrielle succède la révolution numérique, porteuse de vastes opportunités mais aussi de risques, voire de menaces. En 2015, le cyber risque figure au 1er rang des risques technologiques identifiés dans le Panorama 2016 des risques globaux du Forum de Davos. Il est en général cité parmi les trois premiers risques dans les classements des entreprises ou du grand courtage.

Il s'agit en effet d'un risque dont la présence, la fréquence en termes d'actes de malveillance, et la complexité s'accroissent au fur et à mesure d'avancées technologiques en accélération constante, de l'interconnexion des réseaux et maintenant des objets, de la mondialisation des échanges, de la technicité des délinquants et des terroristes avec une possibilité relativement aisée d'intrusion et de prise de contrôle à distance. L'entreprise, comme le citoyen, ou les organes de l'Etat sont aujourd'hui de plus en plus dépendants de la sécurité, des performances et de l'efficacité de leur système informatique, et des réseaux connectés.

Prévention, information et collaboration en termes de sécurité informatique, sont des éléments essentiels de protection contre le cyber- risque. Certaines attaques ont eu une large résonnance dans le monde, telles que Target (2013) ou Sony (2014) en ce qui concerne le vol de données, ou l'attaque très médiatisée sur les centrales nucléaires iraniennes (2010) par le virus Struxnet, virus suffisamment complexe pour entrainer des dommages irrémédiables sur des installations industrielles de pointe et très protégées. Elles ont contribué à sensibiliser les industriels sur la vulnérabilité des données ou les risques d'attaque des systèmes, comme les systèmes SCADA (télégestion industrielle), utilisés pour des installations industrielles y compris sensibles (centrales hydro-électriques ou nucléaires, distribution d'eau potable, oléoducs...)

Dans le contexte actuel d'**absence de données et de statistiques significatives**, le cyber risque demeure un risque très difficile à cerner, en particulier de par son caractère cumulatif et universel, et pose problème pour la protection des biens, voire dans certains cas des personnes (prise de contrôle de moyens de transport ou d'installations industrielles). Les solutions (ré)assurantielles existent mais s'avèrent encore complexes à mettre en œuvre au niveau des entreprises, tout d'abord faute d'un consensus sur ce que recouvre exactement le risque cyber, mais aussi du fait des problématiques d'accès à des données fiables sur l'étendue et le coût des cyber- attaques et/ou évènements ayant endommagé des systèmes informatiques avec des conséquences parfois importantes. S'ajoute la problématique de la transversalité des dommages susceptibles d'être causés. Il en découle la difficulté de recours à des méthodes statistiques traditionnelles et de modélisation du risque.

Enfin, l'ampleur des dommages potentiels est difficile à évaluer au niveau d'une entreprise ou d'un marché. Les Lloyd's ont ainsi présenté un scénario de 1000 Mds$ impliquant une cyber-attaque sur le réseau électrique américain, tandis que l'ENISA (agence européenne chargée de la sécurité et des réseaux) estime à 260/340 Mds€ le montant des pertes annuelles mondiales

estimées qui sont engendrées par des attaques cyber, lesquelles se sophistiquent chaque jour davantage.

Aux USA, le Président Obama, qui définit la cyber sécurité comme « l'un de défis les plus importants auxquels nous sommes confrontés en tant que nation », vient de lancer un plan de 19 Mds$, le CNAP (Cyber-security National Action Plan), ayant pour objectif de doter les Etats-Unis d'outils de sécurité, testés et certifiés, destinés à protéger citoyens, entreprises et gouvernement des cyber- attaques et des atteintes aux systèmes informatiques et vols de données.

Le marché assurantiel européen s'est développé plus tardivement que le marché américain, mais couvre déjà, soit par des polices spécifiques, soit par absence d'exclusions sur les polices traditionnelles, un certain nombre d'aspects du cyber- risque. Il appartient à la (ré)assurance de contribuer à résoudre, dans la mesure du possible, des défis structurels d'assurabilité. Toutefois, en l'état actuel des connaissances et compte-tenu de la progression constante du risque, de l'évolution de sa nature et de son caractère potentiellement systémique, certains réassureurs considèrent aujourd'hui qu'il est encore trop tôt pour savoir si le risque cyber constitue une opportunité ou une menace pour la profession, ou se situe entre les deux.

Les réassureurs sont engagés sur les risques extrêmes et désireux de participer à l'amélioration des couvertures et à la réduction des risques. Soucieuse de contribuer à une meilleure protection du marché, particulièrement en France, l'APREF souhaite par cette Note aider à la réflexion sur le cyber risque, ainsi que sur les possibilités de développer plus largement les couvertures et de repousser les limites de l'assurabilité par des solutions de place (voir 2e partie). Une 3$^{e}$ partie fera le point d'un environnement règlementaire en pleine évolution.

Cette démarche s'inscrit d'abord dans la recherche de définition du cyber risque selon l'extension du périmètre considéré, qu'il s'agisse de « tout risque émanant de l'utilisation de données électroniques et de leur transmission, incluant des outils technologiques comme Internet et les réseaux de télécommunications [..]» (approche CRO Forum) [1], ou d'une approche dédiée plus étroitement centrée sur la cyber criminalité, l'essentiel étant que les différents acteurs aient la même vision et compréhension du risque concerné (voir 1e partie).

L'assurabilité de ce risque devrait passer par des schémas faisant appel à une coopération étroite entre assureurs, réassureurs… au niveau du marché d'une part et à l'Etat d'autre part, pour mettre en œuvre des mécanismes de prévention, d'accès aux connaissances, de partage des informations y compris sur les menaces de sinistres ou les sinistres survenus, de protection et de couvertures. Il convient dans ce cadre de s'interroger sur l'aspect systémique et les risques de cumul importants et de réfléchir à des expositions potentielles par branches et à des scénarios de mutualisation, dépendant du degré de protection. (voir 4e partie).

Ceci nous conduira à des préconisations, tant en matière réglementaire et d'accès aux données, qu'en termes de prévention et de couverture, s'appuyant sur une meilleure vision de l'aspect transversal et cumulatif du risque.

[1] CRO (Chief Risk Officers) Forum. Cyber resilience – The cyber risk challenge and the role of insurance . December 2014

# 1. ANALYSE DE RISQUES, ILLUSTRATIONS ET PROPOSITION DE DEFINITION

En France comme ailleurs :

- les opérateurs d'importance vitale (OIV) sont victimes chaque jour de plusieurs millions d'attaques informatiques via internet (mais également sans connectivité)
- les entreprises subissent aussi des attaques innombrables, à des degrés divers selon leur importance et leur secteur économique.

La plupart sont détectées et stoppées avant de réussir à toucher les cibles. Certaines toutefois arrivent à contourner les mesures de protection et échappent à la vigilance des équipes de sécurités informatiques.

Pour mieux cerner le risque, nous décrivons ci-dessous 3 scenarios parmi les plus connus de manifestation du risque cyber, à savoir :

1) compromission et vol de données,
2) attaques cyber et cyber espionnage sur installations sensibles (APT),
3) attaques des systèmes Scada/ICS et réseaux d'infrastructures.

Ils serviront de référence à la définition d'un cadre du cyber risque.

## 1.1. SCENARIO 1 : Compromission de données privatives / personnelles

### 1.1.1. Généralités

Détenant des données (privatives, commerciales, confidentielles, bancaires…) de leurs clients personnes physiques ou morales/ co-contractant/ sous-traitants, ayant une valeur marchande ou permettant de réaliser un gain, les sociétés se voient exposées à des attaques malveillantes dont le but est de compromettre, détourner, manipuler, divulguer ou détruire ces données.

Que l'auteur de l'acte malveillant soit interne ou externe, le processus de l'attaque sera généralement le suivant :

- **Intrusion initiale** : accès à l'infrastructure cœur du réseau via Internet (ou hors connectivité), en contournant les mesure de protection de l'instant T, profitant éventuellement **d'une erreur humaine, d'une panne, d'un problème technique / défauts dans une mise à jour** conduisant le système à se retrouver infiltré
- **Reconnaissance** : l'accès à l'infrastructure permet aux voleurs de développer une compréhension des contrôles de sécurité et d'identification des applications ou des processus à cibler.

**Attaque** sur :

- les données personnelles (exemple références comptes clients avec données privatives et financières),
- les données confidentielles (y compris message entre dirigeants), secrets d'affaires, brevets, les données sensibles, exfiltration : suppression des informations pour ne pas être détecté.

Il est important de comprendre que le **timing d'une telle attaque peut varier considérablement** en fonction de sa sophistication et, dans de nombreux cas, peut s'étaler sur des mois voire des années.
En effet**, la reconnaissance initiale et l'intrusion peuvent être effectuées plusieurs mois avant une réelle attaque**, fournissant ainsi une opportunité plus grande de maximiser le volume de données sensibles recueillies. Cela met en évidence la particularité de ces attaques organisées selon une approche « lente » et méthodique pouvant durer des jours, des mois voire des années afin de **contourner les systèmes les plus sophistiqués de surveillance et les mécanismes de détection.**

### 1.1.2. Illustrations

Entre Novembre et Décembre 2013, **Target**, l'un des plus importants acteurs de la distribution aux USA, s'est fait subtiliser plus de 40 millions de données bancaires, auxquelles s'ajoutent 70 millions de données personnelles.[2]
Les motivations des attaquants sont purement financières. En effet, une donnée personnelle se vend sur le marché noir entre 0,25$ et 2$ environ, tandis qu'une donnée bancaire peut rapporter plusieurs dizaines de dollars.

En juin 2014 **Domino's Pizza** a été victime d'une cyber-attaque. C'est sur Twitter que la chaîne de restaurants Domino's Pizza a annoncé le piratage de son site. Les données personnelles de 600 000 clients ont été dérobées par des « hackers »: adresses mails, postales, noms et mots de passe. Les données bancaires n'auraient pas été touchées. Toutefois, les auteurs réclament une rançon de 30 000 euros, menaçant de rendre publiques les données personnelles de 600 000 clients, Belges et Français, Domino's PIZZA a refusé de payer.

Un article du Figaro en date de janvier 2015 annonçait l'attaque de la partie **"abonnement presse" du site d'une chaine de télévision française leader, sur lequel il est possible de s'abonner à différents journaux**. Les pirates ont exploité une faille technique permettant de mettre la main sur les coordonnées des acheteurs et sur leur RIB, avec pour objectif la revente des bases de données volées à d'autres pirates pour des milliers d'euros. L'intrusion pourrait donc conduire à des usurpations d'identité ou à des malversations.

[2] Plus de détails en annexe 1

### 1.1.3. Application au secteur de la distribution

| Description | Activités touchées | Impacts |
|---|---|---|
| **Utilisation d'une vulnérabilité du site dédié aux contrats de particuliers** et au règlement des factures avec exploitation d'injection SQL au travers d'un proxy afin d'appréhender et d'extraire des données.<br><br>Les données concernées sont des **références de contrats de particuliers, leurs adresses et les références de leurs comptes bancaires.** | - **sites e-commerce**<br>- **magasins**<br>- **centrale d'achat**<br>- **centre de logistique** | -Compromission de données clients.<br>-Notification auprès des clients.<br>-Notification à la CNIL.<br>-Réclamation éventuelle des clients.<br>-Rupture de la chaine d'approvisionnement<br>-Perturbation des livraisons magasins ou clients |

En annexe 1 figure un tableau des principales violations de données recensées en 2014-2015 et des causes principales de violation en fonction du nombre de victimes [Source : Verizon 2013].

## 1.2. SCENARIO 2 : Attaques Cyber (Advanced Persistent Threat ou APT*), mode de piratage informatique furtif et continu

### 1.2.1. Généralités

Le vol d'informations, l'espionnage industriel, l'atteinte à l'image, la déstabilisation sont des attaques qui ont toujours existé dans le monde de l'entreprise et de l'industrie.

Aujourd'hui, leur forme a changé, et l'une des plus redoutées par les activités industrielles est **l'Advanced Persistent Threat (APT).** Cet acronyme*, apparu dans les années 2000 au sein des agences d'intelligence américaines, qualifie une vague d'attaques de cyber espionnage contre les industries de défense US.

Les impacts d'une telle attaque s'avèrent nombreux et variés. **Principalement financiers, ils peuvent aussi porter atteinte à la réputation de l'entreprise, voire à sa crédibilité**. De plus, si les attaques visent des secteurs vitaux de l'économie tels que le nucléaire ou l'énergie, elles peuvent avoir de **graves répercussions à l'échelle étatique, voire régionale ou mondiale**.

### 1.2.2. Illustrations

Lorsque des acteurs comme RSA ou ADOBE font l'objet d'une attaque, les entreprises clients sont potentiellement exposées.

Rapport Verizon 2013
Objectifs des fuites de données constatées :

- 75% des cyber attaques ont des motivations financières
- 20% du cyber espionnage est motivé par le vol de propriété intellectuelle ou d'information concurrentielle

**Un article de L'Express de septembre 2011 citait le cas d'un groupe français, cible d'une attaque de grande ampleur**. Ces intrusions lancées plus de deux ans avant leur découverte auraient touché aussi bien les sites en France que les filiales à l'international du groupe. Les hackers auraient réussi à s'introduire dans le réseau informatique du groupe et à prendre le contrôle d'ordinateurs. **Des préjudices "sur le plan stratégique" sont évoqués, ce qui pourrait signifier le vol de secrets industriels.** Nous ignorons aujourd'hui si les activités militaires de cette entreprise ont été touchées.

**Lors de l'été 2012, le quotidien Le Monde rapportait qu'une cinquantaine d'entreprises, appartenant au secteur de la défense et de l'industrie chimique, avaient été victimes d'une série d'intrusions informatiques.** Ces intrusions étaient coordonnées : les ordinateurs des dites sociétés auraient été infectés par un programme malveillant, utilisé pour dérober des informations. Les informations volées étaient protégées par la propriété intellectuelle L'espionnage industriel semble bien être le mobile de cette vaste attaque.

Inculpation de huit personnes soupçonnées d'appartenir à une cellule de pirates établie à New York. Celle-ci ferait partie d'un réseau qui s'étendrait au total sur 26 pays ! Ces hackers ont agi lors de deux opérations, en décembre 2012 et février 2013.

En amont, un groupe de hackers avait pénétré le système informatique de groupes bancaires, piraté les numéros et les codes secrets de cartes prépayées (cartes pour les entreprises et ONG) puis supprimé leur plafond de retrait. Le jour J, plusieurs personnes ont alors retiré au même moment une certaine somme d'argent dans plusieurs distributeurs.

La banque Rakabank, basée aux Émirats, a été la première victime enregistrant 4 500 débits effectués à travers 20 pays pour un total de 5 millions de dollars. Puis la Bank of Muscat, basée à Oman, avec 36 000 retraits en 10 heures dans 24 pays pour un total de 40 millions de dollars. Aux US, ce sont 400 000 dollars qui ont été retirés fin décembre puis 2,4 millions en février par 3 000 retraits séparés.

**Le groupe russe Kaspersky Lab a publié un rapport en février 2015 qui révèle l'attaque d'une centaine de banques par un cyber gang Carbanak. Le montant exact des pertes enregistrées par ces banques n'est pas encore connu mais pourrait se situer entre 300 millions et un milliard de dollars, indique pour sa part le Financial Times. Une enquête est en cours, menée par Interpol et Europol.**
La liste des banques victimes de ces attaques n'est pas connue, mais d'après The New York Times la plupart des établissements bancaires ciblés se situeraient en Russie, au Japon, aux Etats-Unis et en Europe. Selon Kaspersky Lab, le cyber gang aurait pénétré à l'intérieur des systèmes en utilisant une technique appelée spear phishing[3] ou harponnage qui consiste à envoyer des mails à des employés de banque, mails qui contiennent des logiciels malveillants.
Un autre exemple est le sabotage des algorithmes de Trading Haute Fréquence par des hackers.

[3] Voir annexe 5.5.3

### 1.2.3. Application aux secteurs des OIV et industries critiques

| Description | Activités touchées | Impacts |
|---|---|---|
| Un tel scénario pourrait être la conséquence d'une attaque via l'hameçonnage ciblé (Spear Phishing).<br><br>Cette technique consiste à envoyer un courriel à un individu ou à un groupe ciblé en s'assurant que le sujet du courriel sera d'intérêt pour la victime afin que cette dernière ouvre un lien ou une pièce jointe ayant un contenu malveillant. Toute la sécurité informatique (pare-feu, reverse proxy) de la société visée est ainsi contournée et l'attaquant peut accéder à de nombreux documents sensibles (commerciaux, industriels, R&D) pour les extraire, les détruire ou les crypter. | - L'ensemble du réseau interne.<br>- Les messageries.<br>- Un grand nombre de postes utilisateurs. | - Compromission de données confidentielles<br>- Perte d'avantage et de compétitivité,<br>- Perturbation d'infrastructure critique<br>- destruction de données avec un coût de décontamination important,<br>- cryptage de données avec demande de rançon. |

## 1.3. SCENARIO 3 : Atteinte des systèmes SCADA / ICS

### 1.3.1. Généralités

Les infrastructures critiques (électricité, pétrole, gaz, eau, déchets, etc.), s'appuient fortement sur des équipements électriques, mécaniques, hydrauliques et autres types d'équipements, contrôlés et supervisés par des systèmes informatiques dédiés appelés contrôleurs et capteurs. Ces systèmes sont raccordés à des systèmes de gestion, et forment ensemble des réseaux utilisant les solutions **SCADA** (système de télésurveillance et d'acquisition de données) et ICS (système de contrôle industrie), permettant la collecte et l'analyse des données, ainsi que le contrôle automatique des équipements tels que pompes, vannes et relais.

Cependant, si les réseaux et les dispositifs SCADA/ICS ont été conçus pour offrir un contrôle fiable, ils n'intègrent souvent pas de mécanismes de sécurité permettant d'empêcher les accès non autorisés, ou capables de faire face aux menaces de sécurité en constante évolution provenant des réseaux externes ou internes. Un pirate qui a réussi à infiltrer un réseau SCADA est en mesure d'envoyer des commandes malveillantes pour bloquer ou freiner les dispositifs et interférer avec les processus industriels critiques et spécifiques qu'ils contrôlent, tels que l'ouverture et la fermeture de vannes par exemple.

**Les scénarios d'attaques les plus communs sont** :

- L'utilisation d'un port d'accès à distance habituellement réservé à un fournisseur de services de maintenance,
- Le piratage d'un canal légitime entre les systèmes informatiques et les systèmes SCADA/ICS,
- L'hameçonnage d'un utilisateur interne incitant à cliquer sur un lien depuis un poste de travail connecté au réseau SCADA/ICS et à Internet,
- L'infection des ordinateurs portables et/ou des supports amovibles à l'extérieur du réseau SCADA/ICS, contaminant les systèmes internes lorsqu'ils se connectent au réseau pour collecter de données, mettre à jour le contrôleur/les capteurs...,
- L'exploitation des erreurs de configuration de la sécurité ou des dispositifs connectés.

### 1.3.2. Illustrations

Il s'agit de paralyser l'entreprise pour une durée indéterminée par la gestion d'une crise majeure, **de provoquer des dommages matériels et immatériels, voire corporels**, ou bien encore de collecter des données stratégiques en vue d'en retirer un gain ou un avantage compétitif

A titre d'exemple, en décembre 2014 un industriel allemand, spécialiste de la production d'acier, a été victime d'une attaque informatique réussie ayant conduit à la compromission de son système informatique avec un résultat concret : l'impossibilité de procéder à l'arrêt maîtrisé d'un haut fourneau, avec pour conséquences d'importants dégâts sur le site.

Dans son rapport, le ministère précise que l'attaque a commencé par une infiltration du réseau administratif de l'entreprise visée par hameçonnage ciblé et ingénierie sociale. De là, les pirates auraient réussi à compromettre le réseau de contrôle des installations industrielles.

En 2012, le groupe pétrolier Saoudien Aramco a révélé avoir fait l'objet d'une attaque informatique de grande ampleur. 30 000 postes de travail ont été infectés par un virus informatique provenant de l'extérieur. Cette cyber attaque n'aurait cependant pas affecté les données industrielles du groupe, isolées du réseau bureautique[4]

[4] Voir annexe 1

### 1.3.3. Application à des secteurs critiques

| **Description** | **Activités touchées** | **Impacts** |
|---|---|---|
| - L'infiltration d'un logiciel malveillant dans un système de commande industriel (SCADA) via une clé USB/ Internet fournit aux attaquants la capacité de contrôler à distance les processus infectés.<br>- **Une augmentation de pression** (ou l'arrêt de système de refroidissement) **en raison de l'atteinte malveillante** par les pirates informatiques **mène à l'arrêt du site et/ou à une contamination nucléaire de l'environnement.**<br>- Une modification des configurations nominales des installations peut provoquer des dégradations physiques avec le plus souvent des conséquences matérielles – mais parfois aussi humaines. | - Une entreprise de traitement des eaux perd le contrôle de ses centres de traitement.<br>- Un site nucléaire et toute industrie qui en dépend<br>- Inhibition d'alarme de surveillance de produits dangereux sur un site) | - Catastrophe industrielle, humaine ou écologique.<br>- Intoxication,<br>- Dégâts matériels sur un site nucléaire<br>- Interruption de l'activité après feu / explosion<br>- Interruption d'autres sites industriels ou activités dépendant(e)s<br>- Dommages corporels<br>- Dégâts sur biens de tiers<br>- Dommages environnementaux<br>- Pertes d'exploitation<br>- Réclamations d'actionnaires<br>- Coupure de courant de plusieurs raffineries / usines, d'une zone géographique intégrant des habitations |

Ces différentes illustrations nous amènent à la question de la définition du risque cyber. Elle se situe dans un environnement en plein développement dont il convient de tenir compte.

**1.4. Evolution des facteurs de risques** :

- L'augmentation du nombre de données stockées par les entreprises dans le cadre de leurs activités et quelles que soient ces activités :
  - Données clients/donneurs d'ordre/prospects
  - Données fournisseurs et tout autre partenaire
  - Données propres
  - L'augmentation de l'immatérialité du capital des entreprises,
  - L'augmentation exponentielle du rôle des SI dans les processus industriels ou de gestion
- L'externalisation des systèmes d'informations (« outsourcing », « cloud computing », …)
- L'augmentation des risques liés à l'ouverture « planétaire » des réseaux d'entreprises sur l'internet et les réseaux sociaux

Et, parallèlement,

- Une nouvelle forme de criminalité, la « cybercriminalité » et les « cybercriminels » professionnels.

**Le CRO Forum**, qui réunit les Chief Risk Officers des grandes sociétés d'assurance et de réassurance européennes, a consacré en décembre 2014 une étude très approfondie sur le cyber risque. Pour ses participants, **le risque cyber, au sens large, recouvre les risques de faire des affaires [..] dans un environnement digital ou « cyber »** [5]. C'est donc l'environnement qui conditionne le risque. L'étude poursuit en soulignant que la nature évolutive du risque, […] et le manque de clarté sur l'étendue du champ de couverture contribuent à l'importance d'une « codification » du cyber risque. […].. Pour circonscrire toutefois plus spécifiquement le risque cyber par rapport aux autres types de risques dans l'univers digital, elle précise **: « le cyber risque couvre tout risque émanant de l'utilisation de données électroniques et de leur transmission, incluant les outils technologiques comme Internet et les réseaux de télécommunication. Il inclut aussi les dommages physiques qui peuvent être causés par des cyber attaques, la fraude commise par l'utilisation abusive de données, toute responsabilité née du stockage de données, et la disponibilité, l'intégrité et la confidentialité des informations électroniques, qu'il s'agisse d'individus, d'entreprises ou de gouvernements »[6].**

Ainsi, la survenance d'un risque cyber signifie toute destruction, perte, altération, divulgation ou accès non-autorisé à des systèmes d'information ou données informatiques. Cette définition comprend l'indisponibilité due à l'altération d'un système [informatique ou digital ou « cyber »], celui-ci étant lui-même constitué de données.

Ce faisant, on doit distinguer les menaces cyber de nature **intentionnelle** (malveillance) des risques cyber de nature **accidentelle**. En effet, la cyber sécurité ne se limite pas à la protection vis-à-vis de la cybercriminalité, qui agit majoritairement à travers la connectivité des réseaux (mais pas exclusivement), elle concerne aussi les dysfonctionnements fortuits pouvant affecter les SI industriels ou de gestion, ainsi que les éléments physiques de « hardware », équipements, câbles, chaines de production des sites industriels, aux intelligences artificielles de « trading » de haute fréquence, sites industriels.

Il ne s'agit donc pas d'une approche proprement assurantielle mais de la définition du cadre dans lequel évolue le cyber risque, permettant de comprendre expositions et besoins de protection qui en découlent. Une 2e démarche consiste à déterminer les risques déjà assurés d'une part, et/ou assurables par les contrats dits « cyber ».
En effet, comme le souligne également l'étude du CRO Forum qui promeut par ailleurs un partage plus large d'informations de qualité sur les sinistres recensés, une partie des dommages ici décrits, notamment ceux subis (ou causés) par l'entité ou ses employés,

[5]. Op. cit. « As a term, cyber risk covers the risks of doing business, including managing and controlling data, in a digital or "cyber" environment" page 3

[6] Cyber risk covers any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cyber attacks, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments.

relèvent généralement des contrats d'assurance traditionnels pour autant qu'ils n'excluent pas les conséquences des atteintes à des systèmes d'information ou à des données informatisées. **La frontière entre contrats traditionnels et contrats « cyber » est éminemment variable d'un acteur à l'autre.**

C'est à partir d'une vision globale de ce risque, qui permet de définir les besoins de protection, que les opérateurs du marché – courtiers, assureurs et réassureurs – pourront mieux appréhender leurs expositions et offrir des protections adaptées, conçues soit sur mesure, soit sous forme de produits plus standardisés pour des acteurs de taille moyenne ou intermédiaire, selon des critères éventuellement à déterminer. Ces couvertures peuvent intégrer et/ou compléter les risques bien identifiés déjà couverts par les polices traditionnelles.

### 1.5. DEFINITION DU CYBER RISQUE

**Pour toute personne morale ou physique, ci-après désignée comme « l'entité »**

**Toutes atteintes à :**

- **des systèmes électroniques et/ou informatiques [de production, d'exploitation, de gestion d'informations et de télécommunication] sous le contrôle de l'entité ou de ses prestataires et/ou**
- **des données informatisées (personnelles, confidentielles ou d'exploitation) appartenant à ou sous le contrôle de l'entité, qu'elles soient transférées ou stockées chez elle ou chez ses prestataires**

**Consécutives à :**

- **un acte malveillant ou de terrorisme**
- **une erreur humaine, une panne ou des problèmes techniques**
- **un évènement naturel ou accidentel**

**Ayant pour conséquences :**

- **des dommages corporels, matériels, et/ou immatériels (frais ou pertes financières), subis par l'entité et/ou ses employés**
- **une mobilisation de ressources internes ou externes**
- **des dommages corporels, matériels, et/ou immatériels, frais ou pertes financières causés par l'entité à des tiers (y compris chaines logistiques / sous-traitants)**
- **une atteinte à la marque et/ou à la réputation de l'entité**

En annexe 1 est également proposée une liste de risques cyber répondant à cette approche.

# 2. ETAT DES LIEUX DU MARCHE (RE) ASSURANTIEL – SPECIFICITES DU CYBER RISQUE ET PROBLEMATIQUES DE COUVERTURE

## 2.1. Le marché de l'assurance cyber

### 2.1.1. Généralités

Les origines de l'assurance des cyber-risques remontent aux années 1990 avec le début de la « dot-com » économie, principalement aux Etats-Unis.

Toutes les entreprises, quels que soient leurs secteurs d'activité et leur taille, sont exposées aux risques liés aux incidents de sécurité informatique, même si certaines le sont plus que d'autres.

Aux Etats Unis les polices Cyber possèdent 3 volets :
1 - **'First party'** : dommages matériels et immatériels subis par l'entreprise,
2 - **'Third party'** : dommages causés aux tiers,
3 - Garantie des frais engagés dans le cadre de la gestion de crise.

En France, il existe une multitude de produits et de wordings spécifiques à chaque compagnie d'assurance qui, en l'absence d'analyse exhaustive des garanties existantes, sont susceptibles de comprendre des doublons d'assurance. Le marché est aujourd'hui à la fois compétitif et hétérogène sur un risque en croissance constante encore difficile à cerner, sans que l'offre soit forcément adaptée à la demande.

La couverture des cyber-risques peut être également donnée par une section spécifique dans la police d'assurance dommage ou la police d'assurance Responsabilité Civile. Actuellement, en France, les garanties des polices d'assurances restent assez larges et n'excluent pas toujours tous les risques liés à des incidents de sécurité informatique ou restent silencieuses sur ces problématiques.

Les Risk managers sont de plus en plus sensibilisés aux cyber- risques et la demande croît. Le marché de l'assurance et de la réassurance en France répond aux sollicitations en mobilisant des capacités importantes.

### 2.1.2. Les principaux acteurs du marché de l'assurance et de la réassurance

**Sur le marché mondial les principaux acteurs sont :**
ACE, AIG, Arch, Argo, Aspen, Allianz AGCS, Allied World, AXA, Axis, Beazley, Chubb, CNA, Crum and Forster, Endurance, Hannover Re, Hartford, HCC, Hiscox, Lloyds, Munich Re, Novae Re, QBE, Scor, Swiss Re, Transatlantic Re, Travelers, XL, Zurich.
Ces acteurs opèrent sur le marché français en proposant des couvertures en assurance ou en réassurance. Les assureurs utilisent les réseaux de courtage pour se développer ainsi que leur réseau d'agents lorsqu'ils en possèdent.
De nouveaux acteurs s'intéressent à ce type de risques et de nouvelles capacités devraient émerger prochainement sur le marché.

Les capacités recherchées vont de quelques dizaines de milliers d'euros pour des petites structures jusqu'à quelques centaines de millions d'euros pour les plus grands groupes mondiaux. On estime aujourd'hui à environ 500 Millions d'euros la capacité théorique par

risque offerte par des couvertures spécifiques cyber sur le marché français, en croissance rapide, Lloyd's inclus. Les freins à l'offre de capacités plus importantes à ce jour paraissent être la difficulté d'appréhension du risque de cumul, comme l'impossibilité en l'état actuel des connaissances de « modéliser » le risque.

Les protections en réassurance sont proposées soit via des montages en 'Facultative' assuré par assuré, soit par la mise en place de traités dédiés couvrant l'ensemble des risques cyber de l'assureur, lorsqu'elles ne ressortent pas de l'absence d'exclusions sur les traités traditionnels. La structure la plus fréquemment rencontrée est le traité en Quote-part où le réassureur partage le sort de la cédante, selon un pourcentage fixé à l'avance. Cependant il existe également des solutions en 'Excédent de sinistre par risque et par événement' ainsi que des 'Stop Loss' sur rétention, qui interviennent au-delà d'un certain seuil de sinistralité.

### 2.2. **Les spécificités du cyber risque et les problématiques de couverture**

Les couvertures proposées par le marché répondent à des besoins de couvertures tant en dommage qu'en responsabilité civile. Cette note ne traite pas de la branche Transport, très exposée toutefois, qui pourra faire l'objet d'une étude complémentaire. Certaines de ces garanties peuvent être déjà implicitement couvertes dans les polices Dommages aux Biens et les polices Responsabilité Civile Générale des entreprises. En l'absence d'exclusion des risques cyber, un assuré pourrait se voir indemnisé certains préjudices au titre de ses polices d'assurance existantes. Pour repérer ci-dessous les garanties déjà accordées dans le cadre des polices d'assurance classiques, nous avons ajouté la mention suivante : *(couverture existante).*

Les principales **garanties dommages** rencontrées sur le marché de l'assurance cyber sont les suivantes :

1 - Frais de restauration du réseau et des données de l'Assuré suite à un accès non autorisé, à un virus informatique, à une attaque par déni de service.

2 - Pertes d'exploitation et dépenses supplémentaires suite à une interruption d'activité due à l'inaccessibilité totale ou partielle du système informatique de l'Assuré –non consécutives à des dommages matériels-.

3 - Cyber vol : pertes d'argent, de valeurs ou de marchandises de l'Assuré par vol électronique.

4 - Cyber extorsion : Extorsion de fonds subie par l'Assuré afin d'éviter des pertes ou des dommages occasionnés à son réseau, divulgation d'informations confidentielles ou dégradation de son site Web.

Les principales **garanties responsabilité civile** recensées sur le marché de l'assurance cyber sont les suivantes :

1 - Prise en charge (dommages et intérêts et frais de défense) des préjudices liés à la publication ou diffusion de données numériques portant atteinte aux Données personnelles non publiques (violation du droit à la vie privée ou au droit à l'image d'une personne).

2 - Prise en charge des préjudices liés à la divulgation non autorisée de Données confidentielles (clientèle, CA, business plan…) (couverture existante).

3 - Pertes ou dommages occasionnés à des données tierces sur le réseau de l'Assuré. (couverture existante)

4 - Atteinte au fonctionnement des services / communications internet ou dommages occasionnés à des réseaux tiers.

5 - Transmission de virus informatique.

6 - Frais de notification des clients à la suite d'une violation de données.

Au rang des principales **garanties annexes** accordées actuellement sur le marché de l'assurance cyber figurent :

1 - Sanctions pécuniaires assurables prononcées par une autorité administrative – exclusivement- à l'encontre de l'assuré suite à une enquête en raison de tout manquement à la réglementation relative aux données.

2 - Protection juridique en cas d'atteinte à l'e-réputation de l'Assuré (dénigrement, diffamation, atteinte à la marque / entreprise exprimée via internet).

Certaines compagnies offrent, en complément de leur couverture standard, un panel de services à leurs Assurés. Les plus fréquemment rencontrés sont :

1 - Mise à disposition d'une équipe spécialisée d'avocats et de spécialistes informatiques afin de soutenir l'Assuré en amont dans l'analyse des risques (pre-breach), et en aval dans la maitrise et le suivi de ses risques pendant la survenance du sinistre et après une cyber-attaque (post-breach),

2 - Accompagnement avant et après la souscription pour prévenir et sensibiliser les entreprises face aux risques liés à la gestion des données (audit possible de la sécurité informatique de l'entreprise, accès gratuit à une solution d'information globale sur la protection des données personnelles) [7],

3 - Possibilité pour les Assurés d'offrir aux personnes physiques affectées un service de data monitoring, réalisé par un prestataire spécialisé tiers,

4 - Mise à disposition de consultants en relations publiques et gestion de crise,

5 - Aide spécialisée et juridique apportée par divers experts pour déterminer la portée de la violation et les mesures devant être adoptées afin de se conformer à la législation.

Enfin certaines garanties paraissent plus rarement données sur le marché de l'assurance cyber. Il s'agit des couvertures :

1 - Dommages matériels consécutifs à une atteinte au système ou aux données

[7] Noter que l'ANSSI propose aujourd'hui des certifications d'experts qualifiés, cf page 20

2 - Dommages corporels & décès

3 - Vol de propriété intellectuelle et industrielle, brevets,

4 - Perte d'exploitation « contingente » due à carence de fournisseur(s) et/ou de client(s)

5 - Dommages environnementaux (quoique inhérents à certaines couvertures, comme RC nucléaire)

6 - Cyber-terrorisme

Les exclusions dépendent de chaque assureur, du domaine d'activité de l'assuré et de sa taille.

Un tableau répertoriant les scenarii possibles d'attaques, les impacts pour l'assuré au niveau de son activité ou des dommages occasionnés à des tiers, ainsi que les garanties existantes (ou non) en assurance, figure en Annexe 2.

Il est très difficile à ce jour pour le marché de l'assurance et de la réassurance d'évaluer l'impact potentiel d'un sinistre systémique, comme de déterminer des scenarios catastrophe ayant pour conséquence l'agrégation de multiples polices originales dans un même évènement. Une réaction à cette incertitude consiste en l'introduction de limites annuelles de couvertures dans les traités de réassurance y compris sur des structures en Quote-part.
Les définitions de l'événement cyber dans les traités de réassurance permettant à la Cédante d'agréger des sinistres cyber n'ont pas encore fait leurs preuves face à des sinistres de grande ampleur. Il y a là une source d'insécurité pour un assureur qui choisirait de se couvrir en réassurance par un traité en excédent de sinistre par événement.
La 4e partie de cette étude s'attache à décrire ou reprendre certains exemples de scenarios systémiques susceptibles d'aider à une meilleure appréhension des risques de cumul. Les offres de couvertures pourront bénéficier de l'évolution de l'expérience de la sinistralité et de sa meilleure connaissance, permettant de mieux cerner ce risque.

En ce sens, il est essentiel pour la profession d'avoir accès à un maximum d'informations sur les sinistres et menaces de sinistres, comme nous le recommandons dans la 3e partie.

# 3. CADRE LEGISLATIF ET REGLEMENTAIRE

La réglementation est appelée à jouer un rôle central dans la prévention et la connaissance du risque cyber. Par l'introduction de nouvelles exigences en termes de protection, de règles renforcées pour l'administration des systèmes, d'extension du pouvoir de l'Etat en matière de contrôle et de sanctions, et d'obligations de notification d'incidents, elle devrait également contribuer au développement de l'assurance. Ce sont pour le moment principalement les secteurs considérés comme « vitaux » qui sont concernés. Sans introduire de contraintes injustifiées, l'extension de ces règles et l'assistance par des certifications de spécialistes au niveau national ou international pourraient aider à étendre l'offre.

Nous étudions ci-dessous le cadre normatif en France, aux Etats-Unis, et au sein de l'Union Européenne, étant entendu que sur un risque qui a priori ne connait pas de frontière, une étroite coopération internationale et une approche concertée du risque devraient prévaloir.

## 3.1. CADRE REGLEMENTAIRE EN FRANCE

Le cyber risque est une atteinte à des systèmes électroniques ou à des données informatisées sous le contrôle d'une identité ou de ses prestataires. La France s'est dotée peu à peu de normes afin de lutter au mieux contre ces atteintes, qu'elles soient consécutives à un acte malveillant ou terroriste, à une erreur humaine, à une panne, etc. Deux grands groupes d'entités ont été identifiés comme spécialement concernés par les cyber-risques et sont visés par des textes particuliers à leurs activités :

### 3.1.1. LOI INFORMATIQUE ET LIBERTE et OPERATEURS TELECOM (Loi du 6 janvier 1978, ordonnance du 24 août 2011 « Paquet Télécom ») :

La loi « Informatique et Libertés » du 6 janvier 1978 donne une définition d'une donnée à caractère personnel dont la protection est le principal enjeu normatif. Il s'agit de « 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 ».

La loi « Informatique et Libertés » a notamment créé la Commission Nationale de l'Informatique et des Libertés ou **CNIL**.

Le champ d'activités de la CNIL, qui est la protection et le traitement des données à caractère personnel, rejoint plus ou moins directement les problématiques de cyber-sécurité. Le rôle et le pouvoir de la CNIL sont amenés à s'accroitre, suite au vote du Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, avec un pouvoir de sanction accru et une coopération entre les autorités de protection nationale en Europe mieux coordonné, et organisée autour d'un nouvel organe européen, le Comité Européen de la Protection des Données (CEPD).

La CNIL a pour missions d'informer et protéger en mettant à la disposition des particuliers et des professionnels des outils pratiques et pédagogiques (https://www.cnil.fr/fr/les-missions) ,

d'accompagner et conseiller (autorisations pour les traitements de données les plus sensibles, autorisations..), de contrôler et sanctionner, et enfin d'anticiper. Pour ce faire la CNIL met en place une veille pour détecter et analyser les technologies ou les nouveaux usages pouvant avoir des impacts importants sur la vie privée.

Le **responsable du traitement informatique** des données telles que définies par ailleurs dans la Loi précitée est celui qui (art. 3 de la loi) :

1) décide de la finalité du traitement ;
2) décide des moyens du traitement.

Il s'agit du **dirigeant** ou **de certains employés** explicitement désignés (le RSSI, le DSI ou le CIL) ou de **tiers autorisés ponctuellement** et de manière motivée (police, fisc…).

Tout responsable de traitement informatique des données personnelles a comme obligations :

- Sécurité des fichiers : sécurité logique, physique et adaptée à la nature des données et aux risques ;
- **Confidentialité des données** : seules les personnes autorisées peuvent y accéder ;
- Durée : les données personnelles ont une date de péremption fixée par le responsable en fonction de l'objectif du fichier ;
- **Finalité du traitement** : un fichier doit avoir un objectif précis. Les informations exploitées dans un fichier doivent être cohérentes par rapport à son objectif ;
- **Autorisation** : les traitements de données personnelles présentant des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en œuvre, être soumis à l'autorisation de la CNIL.

Les fournisseurs de services de communication électronique ont également plusieurs obligations :

- **Obligation de notifier**, sans délai (24h), les violations de données à caractère personnel à la CNIL et aux personnes concernées par la violation, grave ou non. La CNIL a **2 mois** pour se prononcer.
  → ***Si pas de violation*** : les mesures de protection prises permettent de rendre les données incompréhensibles à toute personne non autorisée. La CNIL clôture le dossier.
  → ***Si violation*** **:** la CNIL peut contraindre le fournisseur à avertir l'intéressé. En cas de silence de la CNIL pendant 2 mois : le fournisseur doit considérer que les mesures prises ne sont pas appropriées et il doit informer les personnes concernées par la violation.
- Obligation à l'égard du sous-traitant : La CNIL impose aux entreprises de réaliser un audit auprès de leurs sous-traitants sur l'application des mesures de sécurité et de confidentialité des données. Sinon, elles sont responsables du fait de leurs sous-traitants.

En cas de non-respect, les responsables de traitements sont soumis à des sanctions :

→ ***Pénales*** **(code pénal) :**

- **L'obligation de sécurité** (art. 226-17: 5 ans et 300.000€ d'amende)
- **Communication d'information à des personnes non autorisées** (art. 226-22 : 5 ans et 300.000€ d'amende, sauf imprudence ou négligence : 3 ans et 100.000€ d'amende).
- **Détention des données d'une durée supérieure à celle déclarée** (art. 226-20 : 5 ans et 300.000€ d'amende).

- **Refus ou entrave à l'information** (art. 131-13 : 1500€ d'amende par infraction et 3000€ si récidive).
- **Non-accomplissement des formalités** auprès de la CNIL (art. 226-16 : 5 ans et 300.000€ d'amende).
- **Détournement de finalité** des données (art. 226-21 : 5 ans et 300.000€ d'amende).

→ ***Administratives :***

La CNIL peut sanctionner tout manquement à la Loi « Informatique et Libertés » après enquête. Les sanctions prononcées doivent être proportionnelles à la gravité des manquements et des avantages tirés de ces manquements. La CNIL peut prononcer un avertissement, une astreinte, une amende (150.000€ maximum, 300.000€ en cas de récidive).

**3.1.3. LOI de PROGRAMMATION MILITAIRE et OPERATEURS D'IMPORTANCE VITALE** (Arrêté du 3 juillet 2008, loi de programmation militaire (LPM) du 18 décembre 2013) :

Ce terme désigne tout opérateur ayant une activité d'importance vitale : activités civiles de l'Etat ; activités militaires de l'Etat ; activités judiciaires ; espace et recherche ; santé ; gestion de l'eau et de l'alimentation ; énergie ; communications ; électronique ; audiovisuel et information ; transports ; finances et industrie.

Les OIV sont eux aussi soumis à des obligations :
- **Mettre en œuvre, à leurs frais, les règles de sécurité nécessaires** à la protection de leurs systèmes d'information (L. 1332-6-1 Code de la défense).
- **Informer sans délai le Premier ministre des incidents** (L. 1332-6-2 Code de la défense)
- **Soumettre leurs systèmes d'information à des contrôles** pour vérifier le niveau de sécurité, à leurs frais (L. 1332-6-3 Code de la défense). Audits effectués par l'ANSSI (avec éventuellement des experts externes)
- **En cas de crise majeure**, le Premier ministre peut décider des mesures à mettre en œuvre par les OIV (L. 1332-6-4 Code de la défense).
- **Les sous-traitants** qui participent aux systèmes d'information des OIV doivent respecter les mêmes niveaux et règles de sécurité. Les OIV doivent répondre de la défaillance de leurs sous-traitants.

Les dirigeants des OIV sont également soumis à des sanctions (L. 1332-7, Code de la défense) :
- Pour les dirigeants personnes physiques : amende de 150.000€. Sanction prononcée après mise en demeure, sauf concernant l'information sans délai du Premier ministre
- Pour les dirigeants personnes morales : amende maximum de 150.000€ x 5 (art. 131-38 du Code pénal).

### 3.2. CADRE REGLEMENTAIRE AUX ETATS-UNIS

Aux Etats-Unis le cadre réglementaire distingue entre les lois fédérales et les lois des différents États.

Au niveau fédéral, les risques cyber jouent un rôle important dans le contexte du vol d´identité touchant les consommateurs (Fair and Accurate Credit Transactions Act 2003) et dans le contexte de l´utilisation des informations de santé protégées (Health Information Technology for Economic an Clinical Health Act 2009). Les obligations en vertu de lois fédérales comprennent la protection de données, l´information des individus, l´alerte du gouvernement et les programmes de prévention.

En l'absence de cadre juridique fédéral protégeant les données personnelles identifiables en général, différentes législations ont été adoptées dans 47 États obligeant les entités privées, gouvernementales ou éducatives à informer les personnes des atteintes à la sécurité des informations impliquant des informations personnellement identifiables. Les obligations en vertu des lois de l'Etat varient d'un État à l'autre et comprennent certaines mesures de sécurité, les délais et les modes de notification.

Les sanctions en cas de violation de la loi varient aussi, mais peuvent atteindre jusqu'à 1.500.000 $ dans certains cas.

Au niveau fédéral il existe certaines initiatives d´harmoniser la protection des données et l´obligation de notifier des cyber-attaques au gouvernement.

Dans ce contexte, aussi le Department of Homeland Security (DHS) explore les possibilités de supporter le marché de l´assurance cyber par la **création d´une base de données (Incident Data Repository) qui garantit un environnement sécurisé pour faciliter l´échange anonyme des informations sensibles.**

Actuellement, le DHS mène toujours des discussions avec les Chief Security Officers des entreprises et les assureurs pour déterminer comment une base de données pourrait aider à améliorer les meilleures pratiques en cyber-sécurité, mais aussi à **développer des nouvelles couvertures cyber qui « récompensent » l´implémentation de ces pratiques**

### 3.3. DIRECTIVE EUROPEENNE DU 18/12/2015 (NIS)

Au niveau européen, la directive vise à renforcer et uniformiser le **niveau de la sécurité des réseaux et des systèmes d'information au sein de l'Europe**. Elle est prévue pour entrer définitivement en vigueur 21 mois après son vote et s'articule autour des objectifs suivants :

- l'adoption d'**une stratégie de sécurité officielle par Etat**. Ces stratégies définissent en particulier les politiques de prévention de gestion et de réparation des accidents.
- la création de réseaux européens de **CSIRTs (équipes de gestion d'incidents informatiques).**

- la mise en place d'un niveau de sécurité élevé et d'un système de notification pour les organismes d'Importance Vitale (OIV) d'une part et pour les fournisseurs de services digitaux d'autre part
- la désignation précise, par Etat-membre, **d'autorités administratives compétentes et de points de contacts uniques** pour gestion de la sécurité des réseaux et des systèmes d'information. Si l'autorité administrative compétente désignée est unique, elle se confond avec un point de contact unique.

Le suivi des incidents au niveau national, la diffusion des alertes, la prise en charge des incidents, l'animation du réseau des CSIRT et des échanges avec le secteur privé sont clairement affectés aux CSIRTs.

Il est également prévu la création :

- d'une Agence de sécurité des réseaux et des systèmes d'information **(ENISA).**
- d'un **groupe de coopération** composé de représentant des états membres, de la commission européenne et de l'agence ENISA.

**Par OIV** on entend opérateur dans les secteurs de l'énergie (électricité, pétrole, gaz), des transports (aérien, ferré, par voie d'eau, routier) de la banque, des infrastructures de marchés financiers, des services de santés (hospitaliers) de la distribution d'eau potable, des infrastructures digitales. Les opérateurs OIV doivent être identifiés par les Etats dans les 6 mois suivant la prise d'effet de la directive. Plusieurs critères permettent d'identifier les OIV en fonction des impacts potentiels d'une interruption de leur service.
Par fournisseur de services digitaux on entend vente en ligne, moteur de recherche en ligne, service de cloud computing.
Tous les organismes non-OIV ou non- fournisseurs de services digitaux ont la possibilité **(sans avoir l'obligation)** de notifier des incidents.

Les États membres veillent à ce que les **OIV notifient sans délai** aux autorités compétentes ou aux CSIRTs tout incident ayant un impact significatif sur la continuité des services fournis. Les autorités compétentes agissant en commun au sein du groupe de coopération sont incitées à développer des guidelines décrivant les circonstances dans lesquelles les notifications doivent être effectuées.
Les États membres veillent également à ce que les fournisseurs de services digitaux notifient tout incident ayant un impact substantiel sur la fourniture d'un service aux autorités compétentes ou aux CSIRTs.

Sanctions : les États membres fixent les règles relatives aux sanctions applicables aux violations des dispositions nationales prises en application de la présente directive et prennent toutes les mesures nécessaires pour veiller à ce qu'elles soient mises en œuvre. Les sanctions prévues doivent être efficaces, proportionnées et dissuasives.

### 3.4. PREVENTION EN MATIERE DE CYBER RISQUE :

#### LE ROLE DE L'ANSSI (FRANCE)

**Description :**
L'ANSSI est l'Agence Nationale de la Sécurité des Systèmes d'Information.

Service français créé par décret le 7 juillet 2009, elle est rattachée au Secrétaire général de la Défense et de la sécurité nationale.
L'ANSSI emploie 500 personnes et a traité près de 30 attaques informatiques majeures en 2015.
L'agence a évolué plus récemment vers le conseil et a développé une expertise plus large à destination des OIV et orientée sur la cybersecurité du pays. Son champ d'activité principal reste la protection des services de l'Etat.

**Missions :**
L'ANSSI a une mission d'autorité nationale en matière de sécurité et de défense des systèmes d'information et joue un rôle central. Pour ce faire, elle déploie un large panel d'actions normatives et pratiques, depuis l'émission de règles et la vérification de leur application, jusqu'à la veille, l'alerte et la réaction rapide face aux cyberattaques. Elle doit :

- détecter et réagir au plus tôt en cas d'attaque informatique, grâce à un centre de détection chargé de la surveillance permanente des réseaux sensibles et de la mise en œuvre de mécanismes de défense adaptés aux attaques ;
- prévenir la menace par le développement d'une offre de produits de très haute sécurité ainsi que de produits et services de confiance pour les administrations et les acteurs économiques ;
- jouer un rôle de conseil et de soutien aux administrations et aux opérateurs d'importance vitale.

La Loi de programmation militaire promulguée le 19 décembre 2013 a renforcé les missions de l'ANSSI. Son article 22 prévoit l'adoption de mesures de renforcement de la sécurité des opérateurs d'importance vitale : au nom du Premier ministre l'ANSSI peut imposer aux OIV des mesures de sécurité et des contrôles de leurs systèmes d'information les plus critiques. De plus, l'article 22 rend **obligatoire la déclaration des incidents constatés par les OIV sur ces systèmes. Le principe de notification obligatoire vaut y compris pour des menaces potentielles.**

Des arrêtés sectoriels sont prévus à partir de juillet 2016 ; ces arrêtés vont permettre la mise en place d'un suivi statistiques de déclarations d'incidents par grands secteur (communications électroniques, approvisionnement en énergie électrique, gaz, hydrocarbures pétroliers, gestion de l'eau, transports, produits de santé, espace, alimentation, finances…). Une partie de ces statistiques sera normalement disponible (sous condition de respect des critères de confidentialité, d'anonymat et/ou de diffusion restreinte).
Les notifications d'incidents seront effectuées sans délais. Des sanctions pécuniaires et pénales seront prévues pour chef d'entreprise ne respectant pas ses obligations déclaratives.
Une directive nationale de sécurité sera par ailleurs rédigée par le ministère visant entre autres à la pérennité de la mission OIV.

**L'ANSSI qualifie des prestataires de service sur la prévention et la gestion des crises**.
Le principe mis en avant est celui de l'auto évaluation ou de l'évaluation par un prestataire externe sur le degré de maturité de protection SI. Parmi ceux-ci on peut citer :
-Les PASSI Prestataires d'Audit de Sécurité de Systèmes d'Information, menant principalement une action de prévention, permettent la remontée de l'information
-Les PDIS sont des Prestataires de Détection des Incidents de Sécurité
-Les PRIS sont des Prestataires de Réponse aux Incidents

Enfin, les CERTs (Computer Emergency Response Team) sont des organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ces sont des centres d'alerte et de réaction aux attaques informatiques, destinés aux entreprises et/ou aux administrations, mais dont les informations sont généralement accessibles à tous.

**L'ANSSI et l'industrie financière :**
Quelques contacts ont été établis entre l'ANSSI et l'assurance/réassurance. En 2012 un groupe de travail autour d'un scenario de place mené avec la Fédération Bancaire Française a abouti à la rédaction d'un rapport. (http://www.fbf.fr/fr/files/92HJ84/Rapport-exercice-de-place-2012.pdf).
Des échanges périodiques avec l'APREF pourraient avoir lieu lorsque l'ANSSI disposera de chiffres consolidés et d'une typologie des incidents déclarés, notamment à compter de la deuxième partie de l'année 2016. Une réunion préliminaire avec l'ANSSI a posé les jalons d'échanges avec l'APREF. Une prochaine réunion est prévue pour la fin l'année 2016.

Les éventuelles informations fournies par l'ANSSI seront en tout état de cause anonymisées.
Les requêtes de l'APREF devraient porter en priorité sur les sinistres les plus importants.
L'objectif de l'APREF est de contribuer dans la mesure du possible à fournir aux porteurs de risques du marché une base d'information professionnelle permettant une meilleure connaissance du risque et une amélioration du transfert de risque.

**L'ANSSI à l'international** :
Conformément aux orientations du livre blanc sur la défense et la sécurité nationale 2013, l'ANSSI contribue à **l'orientation de la recherche nationale et européenne en matière de sécurité des systèmes d'information**. Elle entretient et développe ainsi des relations bilatérales avec un grand nombre d'agences homologues sur tous les continents.

**Recommandations de l'APREF** :
L'ANSSI a un rôle privilégié dans la prévention des risques et la mise en œuvre de bonnes pratiques de sécurisation des systèmes d'information. Elle intervient également dans la gestion des crises. Les réassureurs ont un rôle potentiellement très important dans l'indemnisation des sinistres.
L'ANSSI propose à tous des offres de certification de produits de sécurité matériels ou logiciels et certifie des prestataires.
Toutefois, les organismes non-OIV et les non-prestataires de services digitaux n'ont pas d'obligation de déclarer les incidents de sécurité et n'ont pas d'obligation d'utiliser ces organismes de certification reconnus par l'ANSSI. Ces mesures de certification pourraient potentiellement servir de critère d'assurabilité, le label ANSSI permettant aux assureurs et aux réassureurs de considérer le risque comme mieux encadré. Ces réflexions doivent être approfondies.

Il apparait donc très important que l'ANSSI et le monde de l'assurance et de la réassurance travaillent dans un esprit de collaboration.
La dimension internationale des risques est gérée de facto au sein de l'Europe, par le règlement européen sur la sécurisation des systèmes d'information. En dehors de l'Europe, elle peut être gérée par le contrôle des liens entre l'assuré potentiel et les différents organismes locaux.

En règle générale, plus la réassurance dispose d'informations détaillées, plus elle est enclin à offrir facilement sa couverture. Le système est globalement plus efficace et plus accessible si davantage d'informations sont partagées.
Les assureurs et les réassureurs pourraient, par réciprocité, également être amenés à partager leurs informations anonymisées avec l'ANSSI dans le but de renforcer la qualité de la base de données à constituer.

Parmi les pistes explorées en première approche par l'APREF figurerait l'allègement à moyen ou long terme des exclusions dans les polices dédiées exclusivement au risque cyber mais également dans les autres polices pouvant couvrir partiellement ces risques, au fur et à mesure que la connaissance progresse et que sont mieux appréhendés les risques d'agrégation.

## 4. RISQUES SYSTEMIQUES

Le risque systémique peut être défini comme le risque qu'un événement particulier entraine par réactions en chaîne des effets négatifs considérables sur l'ensemble du système pouvant occasionner une crise générale de son fonctionnement.
Quelles sont les caractéristiques qui rendent le risque cyber sensible à un effet systémique :

- Dépendance accrue de l'utilisation des technologies de l'information et de la communication (ICT-TIC)
- Interconnexion accrue des systèmes de communication à l'échelle mondiale : Le système d'information de l'entreprise est déployé dans un contexte d'entreprise étendue permettant un travail en réseau avec ses clients ou usagers, ses fournisseurs, ses donneurs d'ordre, ses partenaires ou les représentants de l'administration. Ces interconnexions génèrent des vulnérabilités nouvelles pour les systèmes d'information de l'entreprise.
- Généralisation des outils nomades (smartphones, tablettes, ordinateurs portables...) et le passage au tout numérique gomment la frontière entre espace professionnel et espace privé, accentuant très significativement les risques.
- Inter connectivité accrue des appareils et des entreprises qui se déploie via internet avec le développement de l'Internet des Objets « IoT »
- Forte dépendance de la plupart des Infrastructures critiques dans le monde (énergie, transport, etc…) au mode de fonctionnement M2M (« la communication de machine à machine ») qui utilise les télécommunications et l'informatique pour permettre des communications entre machines, et ceci sans intervention humaine
- Dépendance aux systèmes d'exploitation et logiciels standards de quelques sociétés informatiques dans le monde.

Quelles sont les difficultés inhérentes à l'élaboration d'un scénario systémique cyber ?

- Origine de l'incident : Forces de la Nature, Défaut technique, erreur humaine ou acte criminel.
- Diversité des dommages : dommages aux biens propres de l'entreprise, pertes d'exploitation, dommages causés à des tiers,
- Absence de limites géographiques : incidences possibles sans limitation de frontière.
- Absence de limites temporelles : le temps de latence d'un virus est très variable.
- Méconnaissance des relations entre les parties. Deloitte identifie 672 profiles de scénarios en fonction de sept types de secteur industriel, cinq types de contrôle et trois types d'organisations de compagnies.
- Législation évolutive : les législations nationales ne sont pas encore arrivées à maturité et des changements sont à prévoir.

- Historique sinistres récent et absence de base de données centralisée

Ces scénarios sont par nature différents de ceux déjà connus par notre industrie pour les catastrophes naturelles mais peuvent dans une large mesure s'en inspirer. Or, les recherches sur les phénomènes d'accumulation en matière de risques cyber sont encore récentes, elles sont cependant au cœur des préoccupations des assureurs et des réassureurs. Apporter des réponses permettra le développement de solutions assurantielles et de réassurance dédiées.

Aussi, les travaux de recherche se multiplient notamment :

- Etudes menées par le centre de recherche de Cambridge[8]
- Etude par l'université de St Gallen en avril 2016.[9]
- AIR et RMS ont élaboré des scénarios[10][11]
- Les Lloyd's ont chiffré les conséquences économiques d'une attaque cyber de type Stuxnet sur un certain nombre de villes dans le monde, par un virus qui infecterait par le biais d'une clé USB des systèmes industriels. Pour la France, les Lloyds donnent, à titre d'exemple, les estimations suivantes [12]:
    - Paris : $8.93 milliards
    - Lyon : $1.09 milliards
    - Marseille : $0.82 milliards

Nous avons retenu pour illustrer le risque systémique en matière de Cyber quelques scénarios parmi les plus démonstratifs et aboutis. Le chiffrage reste à ce stade un exercice périlleux.

1 - Sybil
2 - Blackout
3 - Les risques de cyber-attaques contre les centrales nucléaires
4 - Cloud
5 - Les Banques

*Un scenario aviation pourrait être étudié dans l'avenir.*

[8] Cambridge Center for Risk Studies, Managing cyber insurance accumulation risk
[9] University of St . Gallen, Cyber Risk : Too big to insure ? Risk Transfer Options for a Mercurial Risk Class, April 2016, http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf
[10] http://www.verisk.com/press-releases-verisk/2016/april-2016/air-releases-industry-s-first-open-source-cyber-scenario.html
[11] http://www.rms.com/cyber
[12] http://www.lloyds.com/cityriskindex/

## 4.1. SCENARIOS

### 4.1.1. SYBIL

Le centre d'étude des risques de l'Université de Cambridge a réuni en juillet 2013 des experts en sécurité informatique et des chercheurs de l'Université afin d'établir un scénario plausible de risque systémique lié à des problèmes informatiques. Ce scénario est d'une particulière sévérité et de fréquence centennale, selon ce centre d'étude.
Dans un premier temps, ils ont défini le scénario puis dans un second temps, en ont étudié l'impact sur les différents acteurs économiques.

**La définition du scénario :**
La compagnie Sybil Corporation est le leader dans l'édition de logiciel de système de gestion de base de données. Etabli depuis 1970, son système est utilisé dans la plupart des secteurs économiques. Une employée de Sybil, responsable de la codification, s'oppose de plus en plus à son employeur et décide de modifier des sources, ce code modifié sera incorporé dans la prochaine version.
La modification du code entraîne des erreurs de calculs de plus ou moins 10% par rapport à la valeur correcte. Ces erreurs n'apparaitront pas dans des transactions car cela serait alors facilement détecté, mais uniquement dans des algorithmes système. Le fait que les erreurs soient de peu d'importance rend sa détection difficile.
Sybil incorpore le code corrompu dans sa mise à jour et le diffuse à l'ensemble de ses utilisateurs. La plupart des entreprises mettent à jour rapidement leur système d'autres le font avec délai. Commence alors une phase de latence dans lequel le fichier corrompu est présent mais non détecté. Les erreurs s'accumulent et affectent le design, la conception, les instruments de décisions et de reporting causant différents incidents :

- défaut dans un système de sécurité d'une usine, 3 employés décèdent
- une banque utilise un taux d'intérêt erroné et perd des sommes importantes, les dirigeants sont mis en cause
- un laboratoire pharmaceutique doit rappeler des produits en raison d'erreurs dans la formulation
- une société électrique n'arrive plus à fournir de l'électricité pendant 24 heures,
- etc….

Au fil du temps, les utilisateurs notent des erreurs, font des vérifications, se tournent vers leur département informatique qui se retourne vers Sybil qui finit par incorporer un rectificatif dans une mise à jour.

L'équipe définit deux scénarios : l'un pendant lequel il s'écoule une période de 15 mois pendant laquelle le virus est actif mais non diagnostiqué et un autre plus sévère où cette période est de 24 mois. Les mises à jour destinées à réparer le système sont installées avec plus ou moins de rapidité par les utilisateurs. Les entités affectées auditent leur système et prennent les mesures nécessaires

**Impact économique et assurantiel**
Vient le temps de mesurer les effets financiers du virus : quelques rares entreprises avaient des polices cyber. Certaines sociétés ont perdu des sommes supérieures à plusieurs centaines de millions de dollars…

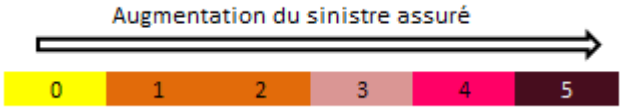
Selon les hypothèses retenues, l'impact macro-économique est évalué entre 5 et 15 000 milliards de dollars, sans limite de frontière[13]. En comparaison, la crise financière de 2008 à 2014 serait évaluée à 20 000 milliards de dollars

Quelles seraient les branches d'assurance impactées ?

**Impact sur les sinistres assurés**

| Branches | | |
|---|---|---|
| Incendie | Vie privée | 1 |
| | commercial | 1 |
| | Construction et engineering | 0 |
| | Commercial facultative | 2 |
| | Binding authorities | 2 |
| R.C. | Mandataires sociaux | 5 |
| | Institutions financières | 4 |
| | RC générale | 5 |
| | RC médicale | 3 |
| | RC professionnelle | 4 |
| Auto | privé | 0 |
| | flottes | 0 |
| Transport | Cargo | 0 |
| | Corps | 0 |
| | RC | 0 |
| | Specie | 0 |
| Aviation | Compagnie | 0 |
| | Aéroport | 2 |
| | RC produits | 2 |
| | Aviation générale | 1 |
| | Espace | 0 |

| Branches | | |
|---|---|---|
| Energie | Downstream | 2 |
| | RC | 2 |
| | Onshore | 2 |
| | Upstream | 0 |
| Autres | Individuelles accide | 0 |
| | Film et événement | 1 |
| | Frais de retrait | 5 |
| | crédit | 5 |
| | Agro | 0 |
| | Kidnapping | 0 |
| | Risque politique | 1 |
| Vie | Vie | 0 |
| | Santé | 0 |
| | Protection revenu | 2 |




L'essentiel des réclamations seraient basées sur la responsabilité, notamment celle des mandataires sociaux : le virus était présent mais n'a pas été détecté.

**Exemples de réclamations :**
Ces cas cités par l'étude s'inspirent de faits réels.

| | | |
|---|---|---|
| Banque | Pendant 2 ans, la banque a fait des transactions sur la base de mauvais taux d'intérêt. Perte de $1.75 billion. | Perte de valeur. RCMS |
| Compagnie d'assurance | Erreur de référencement dans l'archivage électronique. | Perte de données, perte de confiance du client, frais de restauration |
| Laboratoire Pharmaceutique | Rappel de produits. Des erreurs de formulations ont été faites au stade des essais cliniques | Perte de revenue, perte financière |
| Services de distribution d'eau | Dysfonctionnement du système SCADA au niveau du retraitement d'eaux polluées. | Amendes, pollution |

[13] Cambridge Centre for Risk Studies, Cambridge Risk Framework Cyber Catastrophe: Stress Test Scenario "SYBIL LOGIC BOMB CYBER CATASTROPHE SCENARIO"- Octobre 2014
https://urldefense.proofpoint.com/v2/url?u=http-3A__cambridgeriskframework.com_downloads&d=CwIFaQ&c=ZeRjgwCO0jrp4rkAtCoSKyq8f3EgikGx7r3AUiZ_4i0&r=MngchEtLMGRvtD_N4Fs4Q54WEEq4b7mL2QTbRZbpQHk&m=FZ5p0gOMxVTLotTY9vKhatJ8NlNeaRI5PTza1KITHHI&s=aPq8uRE-szYT-uSXn3ZIEBuqEiCn4hCXnrGBpf2RgH8&e

### 4.1.2. BLACKOUT (USA)

Les Lloyd's et le Centre de Recherche des Risques de l'université de Cambridge ont réalisé une étude en 2015[14] sur les effets assurantiels d'une coupure d'électricité dans le Nord des Etats-Unis suite à une attaque Cyber de systèmes d'exploitation. Cette région regroupe 93 millions d'habitants et génère un PIB d'environ 4,97 billions de dollars. En comparaison, l'Ile de France compte 12 millions d'habitants pour un PIB d'environ 623 milliards d'euros en 2012 (Insee).

Les principales conclusions de l'étude sont les suivantes :

- Les attaques provoquent des dommages physiques à cinquante générateurs distribuant de l'électricité dans le Nord Est des Etats-Unis, incluant les villes de New York et de Washington DC.

- Les effets sont multiples :
    - Conséquences sur la santé humaine, accidents de la circulation, décès prématurés dus à l'absence de climatisation, accidents médicaux dans les hôpitaux.
    - Baisse de la productivité dans l'industrie, le commerce, le transport et les moyens de communication. Après la consommation de panique des premiers jours, suit une baisse due notamment au manque d'argent liquide.

- L'impact total sur l 'économie américaine est selon les scénarios de 243 milliards de dollars à 1000 milliards dans le scénario extrême.

- Le sinistre assurantiel est selon les scénarios de 21,4 milliards de dollars à 71,1 milliards. Les réclamations portent sur trente branches différentes d'assurance, notamment :
    - Incendie et pertes d'exploitations
    - Responsabilité civile, mise en cause des fournisseurs d'électricité, des constructeurs des générateurs, développeurs des systèmes, etc
    - Responsabilité civile des mandataires sociaux
    - Tous risques habitation
    - Annulation d'évènements
    - Automobile
    - Assurance-crédit
    - Vie

Il est difficile de chiffrer l'impact qu'aurait un tel scénario sur l'Ile de France, dont le PIB représente 14% de la région objet de l'étude par les Lloyds.

### 4.1.3. LES RISQUES CYBER-ATTAQUES CONTRE LES CENTRALES NUCLEAIRES

Fin mars 2016, alors que la sécurité des sites nucléaires belges est pointée du doigt, Gilles de Kerchove, le coordinateur de l'Union européenne pour la lutte contre le terrorisme, estime qu'une prise de contrôle d'une centrale nucléaire par des mouvements djihadistes pourrait devenir une réalité "avant cinq ans", notamment en prenant le contrôle du "centre de gestion d'une centrale nucléaire, d'un centre de contrôle aérien ou l'aiguillage des chemins de fer", dans une interview au quotidien La Libre Belgique.
En Avril 2016, dans la centrale nucléaire de Gundremmingen en Allemagne, plusieurs malwares ont été détectés sur certains ordinateurs participant au système de manipulation de combustible nucléaire d'un des deux réacteurs. Les malwares ont aussi été retrouvés sur plusieurs clés USB laissant penser qu'elles ont été le vecteur d'insertion dans le système informatique. Ce procédé n'a rien de surprenant ;

[14] Business Blackout : The insurance implications of a cyber-attack on the US power grid - https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf

ces menaces internes ont été identifiées par les puissances nucléaires. Plusieurs journaux affirment que les postes de contrôle de la centrale n'ont pas de connexion internet, disposent tous d'un logiciel antivirus et que les machines les plus sensibles, celles en contact direct avec des éléments radioactifs, ne sont pas pilotées par de l'informatique. Dans le cas présent, il ne semble pas s'agir d'un acte malveillant mais plutôt d'un acte involontaire et accidentel mais cet exemple illustre bien le fait qu'Internet n'est plus le seul vecteur d'attaque pour les systèmes industriels.

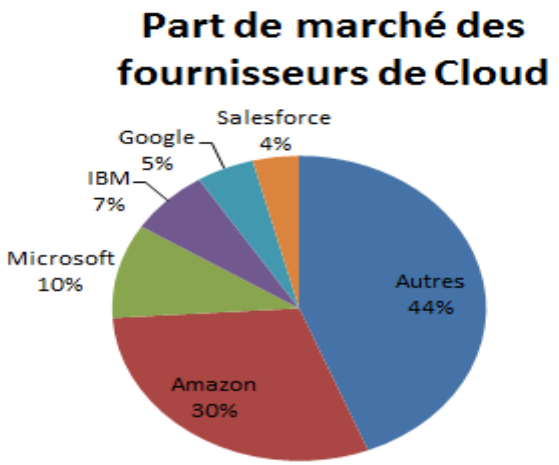
### 4.1.4. CLOUD

Le Cloud pourrait-il être un risque systémique ?

**Définition de Cloud** :
Le Cloud (ou cloud computing) est une technologie qui permet de mettre sur des serveurs localisés à distance des données de stockage ou des logiciels qui sont habituellement stockés sur l'ordinateur d'un utilisateur, voire sur des serveurs installés en réseau local au sein d'une entreprise.
Le cloud computing ou informatique en nuage est une infrastructure dans laquelle la puissance de calcul et le stockage sont gérés par des serveurs distants auxquels les usagers se connectent via une liaison Internet sécurisée. L'ordinateur de bureau ou portable, le téléphone mobile, la tablette tactile et autres objets connectés deviennent des points d'accès pour exécuter des applications ou consulter des données qui sont hébergées sur les serveurs. Le cloud se caractérise également par sa souplesse qui permet aux fournisseurs d'adapter automatiquement la capacité de stockage et la puissance de calcul aux besoins des utilisateurs.

**Principaux Cloud**

SalesForce a été la première offre CRM online.
Amazon Web Service est une collection de produits étiquetés Cloud Computing avec notamment Amazon Elastic Compute Cloud (Amazon EC2), qui permet d'exécuter des applications dans un environnement dont la puissance s'adapte automatiquement aux besoins du moment et Amazon Elastic MapReduce, système de bases de données non transactionnelles utilisées pour de très grosses quantités de données.
Google offre une liste impressionnante de services.
Microsoft avec Windows Azure qui est un ensemble de solution avec une approche type PAAS.



Les différents types de « As A Service »
Il y a différents degrés dans l'externalisation en fonction du niveau de maîtrise et de responsabilité que l'on souhaite conserver :
L'IAAS (Infrastructure As A Service): il s'agit d'un modèle dans lequel un client sous-traite uniquement les équipements nécessaires au fonctionnement d'une partie ou de l'intégralité de son SI (serveurs, firewall, baies de stockage, etc …) et s'en remet au prestataire pour leurs gestions.
Le PAAS (Platform As A Service): Dans le PASS on ajoute à l'IAAS le système d'exploitation ainsi que le serveur d'application, de base de données et les outils de gestion attachés. Mais la maîtrise de l'application et des données restent à la charge du client.
Le SAAS (Service As A Software): un degré au-dessus de PAAS, le SAAS consiste à proposer une solution applicative complète et pour laquelle le client paie en fonction de son utilisation. L'un des exemples le plus connu est Sales Force (une application CRM en ligne). Dans ce cas de figure, les utilisateurs ainsi que la DSI ne gère absolument rien et n'interviennent qu'au début du projet pour la mise en place fonctionnelle.
Le STAAS (Storage As A Service): particularité par rapport aux 3 précédents, le STAAS n'offre que le stockage. Ce type service est généralement utilisé pour de l'échange de fichier ou comme espace de stockage secondaire pour sécuriser des sauvegardes par exemple

**Sécurité du Cloud**
Avec le développement rapide du SaaS, les entreprises se posent légitimement la question de la sécurité de leurs données dans le Cloud. Ces craintes concernent à la fois le stockage des données mais aussi le transfert de ces dernières. Le problème est toutefois souvent examiné en termes techniques, s'attachant particulièrement à la sécurité physique des données, aux architectures techniques ou encore à la politique de sécurité des infrastructures.
Dans bien des domaines, les données peuvent constituer les actifs les plus précieux. Parfois placées au cœur du processus économique, de ces données peut dépendre l'activité de l'entreprise mais aussi son développement. C'est pourquoi il faut également tenir compte de la sécurité juridique des données, qui peuvent être considérées comme très sensibles. C'est le cas notamment des données de santé à caractère privé, des données bancaires, ou encore la protection du capital intellectuel de l'entreprise dans le cadre du secret industriel par exemple.
L'affaire de cyber surveillance Prism a révélé le danger pour les entreprises françaises de stocker leurs données dans des Datacenter en dehors de la France et de l'Europe, notamment aux Etats-Unis. Par la loi « anti-terroriste » baptisée le Patriot Act, le gouvernement américain peut, en effet, avoir accès à des données sur les serveurs installés dans des Datacenter aux USA, et ce, quel que soit la nationalité du fournisseur. De ce fait, il est donc conseillé pour une entreprise de s'orienter vers un acteur reconnu et bien implanté, car l'entreprise qui confie ses données et ses applications à un opérateur tiers doit être certaine que ce service sera hébergé et opéré en France ou en Europe (leurs données informatiques sont hébergées dans les Datacenter du fournisseur) et qu'il dépendra, de ce fait, des législations françaises et européennes sur la sécurité des données. Selon le droit français, et a fortiori européen, les données confiées à un tiers restent ainsi la propriété du client et la loi interdit au prestataire de les divulguer.
Comme toutes les infrastructures IT, le Cloud Computing est vulnérable et peut être soumis à des attaques classiques externes (virus, logiciels espions, intrusions, déni de service, etc). Pour y faire face, l'entreprise utilisatrice doit s'assurer que le fournisseur dispose, bien sûr, de tous les outils de sécurité informatiques nécessaires (des firewalls aux systèmes de détection d'intrusion logicielle en passant par des solutions d'automatisation et de surveillance du réseau) pour garantir la sécurisation des données. Mais, elle doit aussi s'assurer que le fournisseur est également prêt à répondre aux nouvelles menaces notamment celles que l'on qualifie de « persistantes » menées par des groupes organisés. Ces derniers exploitent, en effet, des systèmes très sophistiqués et sont ainsi capables de repérer et de manière répétée toutes les failles des équipements et des applications existants dans le Cloud. L'entreprise cliente doit donc être vigilante en s'assurant que le fournisseur sait détecter en temps réel, via une cellule de veille, toutes les menaces persistantes ciblant les services délivrés.

La tendance nouvelle, dans les déploiements de solutions Cloud, est effectivement de privilégier une « protection fine » des données elles-mêmes -notamment grâce à un chiffrement à la source et à une authentification renforcée- plutôt que de continuer à ériger des murs de protection à base de 'firewalls', qui risquent toujours d'être débordés, à mesure que l'on s'ouvre à l'extérieur. On voit ainsi se développer des plateformes de sécurité des accès au Cloud (ou Cloud Access Security Protection). Elles impliquent une nouvelle gouvernance et des dispositifs de protection renforcés.

**Etude de l'Université de Cambridge et RMS, Février 2016** [15]
L'étude est basée sur un scénario d'accumulation de baisse et/ou de perte de fonctionnalité d'un grand nombre d'opérations d'entreprises qui utilisent toutes un même prestataire de services à distance (Cloud). Il s'agit dans l'exemple d'une défaillance technique mais ce pourrait être d'une attaque cyber. Pour l'évaluation de la sévérité et de la fréquence, différents scénarios ont été construits et leurs conséquences évaluées sur les différentes branches d'assurance et les différents secteurs industriels (Annexe 1).

**Etude du Ponemon Institute, Juin 2014 (Etats-Unis)** [16]
Sondage sur 613 spécialistes IT aux US.
L'augmentation de l'utilisation de Cloud entraine un effet démultiplicateur et donc une augmentation de la fréquence et du coût de la violation de données sensibles.
Ponemon considère deux types de données dans son étude. Ils estiment que la violation de 100 000 données ou plus, le coût moyen peut alors passer de $2.37 millions à $5.32 millions. La violation de données à forte valeur informative entraîne une augmentation de $2.99 millions à $4.16 millions. (Annexe 2)
Ces estimations concernent une entreprise donnée, on peut aisément imaginer quel serait l'impact d'une attaque touchant un grand nombre de clients d'un prestataire de Cloud (cf scénario Scor développé ci-après).

**Scénario CLOUD (source SCOR Global P&C)**
Ce scenario vise à estimer l'impact d'une attaque informatique de grande ampleur sur l'ensemble des clients d'un prestataire de Cloud qui représente **un coût assuranciel de plusieurs milliards de dollars.**
Un groupe de hackers bien structuré et coordonné est spécialisé dans les activités criminelles dont le vol de données, la fabrication de fausses cartes de paiement et l'extorsion. Ils décident de lancer une campagne d'extorsion cyber contre un grand nombre d'entreprises dans tous les segments d'activité. Cette opération demande une longue période de préparation et beaucoup d'experts pour maximiser ses chances de succès. L'objectif est de cibler les clients d'Amazon Web Services (AWS) qui est le plus important prestataire de solutions Cloud.
Pour ce faire, le groupe criminel va commencer par voler la liste des clients d'AWS en pénétrant le réseau informatique d'un de ses sous-traitants. Une fois la liste récupérée, ils lancent une campagne d'attaque informatique de type phishing à l'encontre de l'ensemble des clients d'AWS.
Lorsque l'attaque fonctionne, elle leur permet de chiffrer et potentiellement d'effacer toutes les informations de l'entreprise stockées dans le Cloud d'AWS sans possibilité de les restaurer. Les criminels demandent alors une rançon à chaque entreprise touchée contre la récupération de leurs données.

[15] Managing Cyber insurance accumulation risk, cambridge Center for risk Studies risk Managment solutions, cambridgeriskframework.com/getdocument/39
[16] Data Breach : The Cloud Multiplier Effect, Ponemon Institute sponsored by Netskope, June 2014, https://www.netskope.com/reports/ponemon-2014-data-breach-cloud-multiplier-effect/

**Hypothèses**
Nous avons choisi l'exemple d'Amazon Web Services (AWS) qui est le leader du marché avec 2.1 millions de clients corporate et 30% de parts de marché en 2015. L'attaque est une extorsion cyber à grande échelle qui touche des entreprises :

- Aux États-Unis (PME et grandes entreprises)
- Hors États-Unis (PME et grandes entreprises)

L'attaque a une probabilité de succès qui dépend de la taille de l'entreprise et de son niveau de connaissance (awareness) des risques cyber. Parmi les entreprises touchées, certaines choisiront de payer la rançon, d'autres non. Quoiqu'il en soit, quand l'attaque est réussie, les impacts suivants ont été considérés :

- Montant de l'extorsion
- Dommage à la réputation de l'entreprise
- Frais de réponse à l'incident et d'enquête
- Perte de données et de logiciels
- Amendes
- Perte d'exploitation
- Responsabilité civile

### 4.1.5. LES BANQUES

En France, les établissements ne sont pas épargnés, le secteur bancaire apparait comme particulièrement vulnérable aux attaques ciblées. « Le nombre d'attaques est phénoménal. Entre 2011 et 2014, leur occurrence a été multipliée par 12 », explique Raymond Bunge, directeur systèmes d'information des réseaux de banque de détail en France à la Société Générale. Plus nombreuses, les attaques sont aussi plus virulentes, puisqu'elles peuvent cibler, via des sites localisés à l'étranger, plusieurs points centraux des établissements de façon simultanée. - Source : les Echos, 24/07/2014

Les attaques de phishing (envoi de courriels frauduleux à des clients pour obtenir leurs données bancaires) ont augmenté de 67% entre 2012 et 2013, passant de 62 à 104 millions d'attaques. Les établissements bancaires sont les plus touchés +128% comparé aux sites d'e-commerce (+40%) et système de paiement sur internet eux en légère diminution.
Récemment des cyber-attaques ont pénétré le système de transactions financières internationales Swift, que 11,000 banques utilisent pour transférer des fonds et qui traite 25 millions d'ordres de virement par jour pour des milliards de dollars.

Un scénario qui aurait un impact systémique serait une cyber-attaque simultanée et sévère de banques françaises. Plusieurs impacts pourraient être envisagés, dont des difficultés financières sérieuses, sans exclure une faillite.

En 2012 les banques et infrastructures de marché d'importance systémique se sont livrées à un test de crise qui portait cette année sur une simulation de cyber-attaque des plateformes de transactions financières. Le scénario cette année concernait une cyber-attaque des plateformes internes d'échange de transactions financières des institutions impliquées "de nature à provoquer une paralysie de certains processus opérationnels critiques, avec des effets collatéraux, notamment sur les paiements interbancaires, les back-offices et la comptabilité des établissements, mais aussi sur les chambres de compensation", précise la Banque de France. Une quinzaine de banques et institution y ont participé. Plusieurs exercices similaires sont régulièrement lancés à ce sujet aux États-Unis et en Europe. Les résultats ont été concluants jusqu'ici.

Les impacts d'un tel scénario sont nombreux et peuvent aussi affecter les activités d'assurance. Un crash financier associé à la dévaluation de l'EURO créant l'impossibilité d'échanges interbancaires, et d'utilisation de cartes bancaires peut concerner les branches suivantes :

- Cyber
- Crédit/Caution défaut de paiement/faillites
- Responsabilité dirigeant (D&O) / Responsabilité professionnelle (E&O) ex : Faillites de PME, responsabilité en cas d'attaque et de défaillance des systèmes de protection informatique
- RC dommage si la détermination du tiers est possible.

En annexe figure un exemple de fonctionnement d'une attaque APT (Advance Persistent Threat) dite Carbanak. Il s'agit d'un mode de piratage informatique furtif et continu qui exige un haut niveau de dissimulation sur une longue période.[17]
Sur ce schéma,

- La banque HSBC a été attaquée 4 fois entre aout 2015 et janvier 2016 rendant les services de ses clients en lignes impossible en Grande-Bretagne. HSBC assure qu'aucune transaction n'é été affectée et que le service a repris normalement.

- RBS en juin 2015 a subi une interruption de 600,000 transactions de paiement.

Les branches impactées restent cependant limitées. Le test de 2012 montre que les banques sont préparées à ce genre de scénario et devraient donc réagir assez rapidement ce qui limiterait les pertes assurantielle (Pertes d'exploitations, faillites, …). À l'échelle de la France, les banques et assureurs semblent les entreprises les mieux préparées à ce genre de scénarios car la loi les oblige à se prémunir de ces attaques informatiques. Cependant, l'interdépendance accrue entre les banques et les autres acteurs du système financier renforcent le risque systémique potentiel des cyberattaques.

A notre connaissance, il n'existe pas de données chiffrées sur l'impact assurantiel de disponible, le sujet reste assez discret.

Un autre scenario majeur pourrait impliquer une prise en main du système de contrôle du trafic aérien.[18]

[17] Evaluation des Risques du Système Financier Français.pdf, banque de France, Décembre 2015.
[18] http://resources.infosecinstitute.com/cyber-threat-analysis-aviation-industry/

## Recommandations APREF

*Le marché de l'assurance et de la réassurance du cyber risque se développe mais la pénétration de l'assurance reste faible. La raison en est d'abord un besoin d'information et de compréhension : une enquête a révélé en 2015 que moins d'un cinquième des entreprises au Royaume Uni ont une vision claire au niveau de leur conseil d'administration de l'exposition de leur société au cyber risque. Une autre raison est la crainte d'une défaillance majeure de l'ensemble de la chaîne, ou d'une prise de contrôle d'une installation sensible ayant des conséquences difficiles à quantifier aujourd'hui.*

***Pour une meilleure protection du marché**, s'agissant d'un sujet de Place, **l'Apref préconise** :*

- *Un **consensus sur la définition objective du cyber risque** (page 16), centrée sur l'analyse du risque lui-même, étant entendu qu'il revient aux intervenants de déterminer le type de garanties qu'ils souhaitent délivrer en fonction de leur stratégie et des besoins du marché, dans le cadre du libre jeu de la concurrence*

- *Une réflexion dans le cadre du marché sur un « **produit socle »** destiné aux autres acteurs que les grandes entreprises qui disposent d'une offre sur- mesure, éventuellement par secteur d'activités, reposant sur des garanties explicites*

- *Une amélioration de la **prévention des risques,** s'appuyant sur :*
  - *Une **large information**, entre autres par la profession, pour favoriser la connaissance du risque cyber, et les menaces qu'il représente*
  - *Une **définition claire** de la chaîne de responsabilités (sous –traitants…)*
  - *Une **assistance accrue** pour aider les acteurs à réduire les risques en procédant à un inventaire en amont de leur profil de risques, et en aval à identifier, maitriser le sinistre et le limiter.*
  - *Une **généralisation de la certification** des prestataires et des produits de sécurité matériels ou logiciels que propose l'ANSSI.*
  - *Une **réglementation adaptée**, s'inspirant sans contraintes inutiles des secteurs « vitaux » : secteur financier, transport, énergie, santé…, incluant des exigences en termes de protection, des règles renforcées pour l'administration des systèmes, et surtout une **obligation de notification de tout incident**.*

- *A l'instar de la démarche du Department of Homeland Security, il semble essentiel à l'APREF de **créer** une **base de données d'incidents** (Incident Data Repository) qui garantit un **environnement sécurisé** pour faciliter l'échange d'informations anonymisées sensibles. Une coopération avec l'ANSSI et les pouvoirs publics doit être poursuivie en ce sens par la profession.*

- *Une réflexion en amont sur des **scénarios catastrophe,** la prévention de sinistres majeurs, et sur le processus de leur prise en charge au niveau national comme international, avec d'éventuels **Partenariats de Place**.*

# 5- ANNEXES

## 5.1 ANNEXES 1 – SCENARIOS DE RISQUES

### 5.1.1. Sinistre TARGET (Scenario 1 – Page 6)

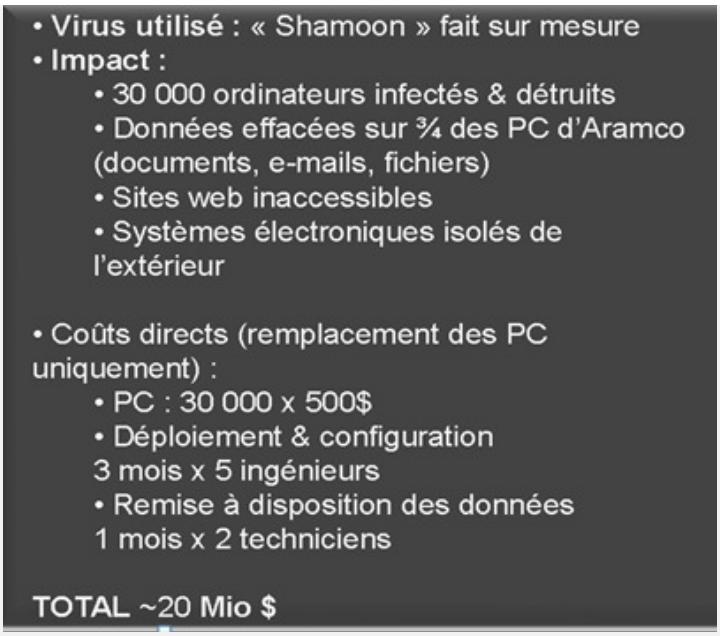
Entre le 27 Novembre 2013 et le 15 Décembre 2013, Target l'un des plus importants acteurs de la distribution aux USA, s'est fait subtiliser plus de 40 millions de données bancaires, auxquelles s'ajoutent 70 millions de données personnelles.

Les attaquants ont en premier lieu piraté un sous-traitant du distributeur chargé de la surveillance à distance des systèmes de chauffage et de climatisation. Le système de facturation externe de Target auquel le sous-traitant avait accès n'étant pas complétement isolé du réseau interne, les cybercriminels ont réussi à s'y infiltrer, à voler 70 millions de données personnelles, et à installer un logiciel malveillant sur quelques terminaux de paiements.

Après des tests concluants sur les magasins concernés, ils ont décidé, peu avant Noël où l'affluence est la plus forte, de déployer leur malware sur la plupart des terminaux de paiements des magasins du territoire américain.

Les motivations des attaquants sont purement financières. En effet, une donnée personnelle se vend sur le marché noir entre 0,25$ et 2$ environ, tandis qu'une donnée bancaire peut rapporter plusieurs dizaines de dollars.

### 5.1.2. Sinistre ARAMCO (Scenario 3 - page 10)




*source Airbus Défense*

### 5.1.3. Hitparade des violations de données 2014-2015

| ENTREPRISES | DONNÉES DÉROBÉES | TYPE DE DONNÉES |
|---|---|---|
| **PREMERA BLUE CROSS**<br>Date d'annonce : 18 mars 2015 | **11 M** | Numéro de compte bancaire<br>Numéro de sécurité sociale |
| **ANTHEM**<br>Date d'annonce : 05 février 2015 | **80 M** | Numéro de sécurité sociale<br>Adresses email<br>Adresses physique |
| **SONY**<br>Date d'annonce : 25 novembre 2014 | **47 000** | Information de l'entreprise<br>Données d'employés |
| **HOME DEPOT**<br>Date d'annonce : 02 septembre 2014 | **109 M** | Numéro de carte de crédits<br>Adresse email |
| **JP MORGAN**<br>Date d'annonce : 27 aout 2015 | **83 M** | Adresses email<br>Adresses physique |
| **Ebay**<br>Date d'annonce : 21mai 2014 | **145 M** | Adresses email<br>Adresses physique<br>Identification de connexion |
| **TARGET**<br>Date d'annonce : 13 décembre 2013 | **110 M** | Numéro de carte de crédits |
| ADOBE | 2014 | 150 M |

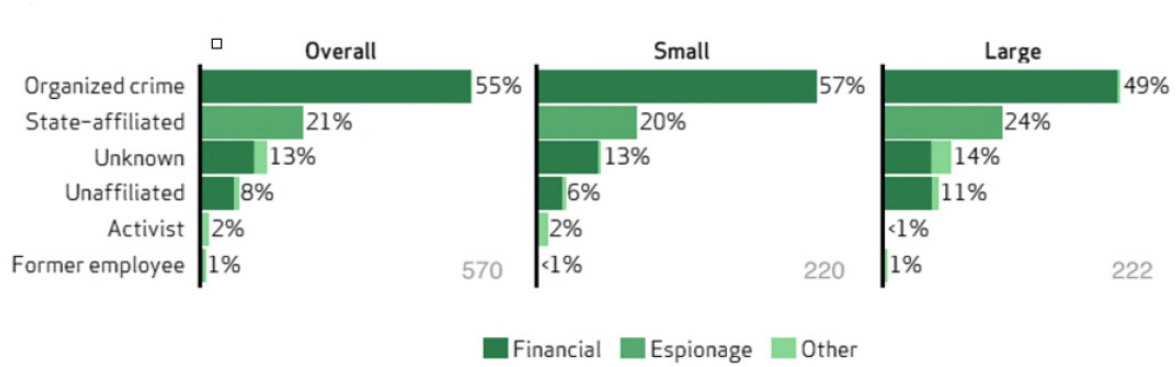
## Top Causes for Data Breaches by Number of Identities Exposed

Source: Norton Cybercrime Index

| Cause of Breach | Number of Identities Exposed | Percentage of Identities Exposed |
|---|---|---|
| Hackers | 408,432,788 | 74.0% |
| Insider theft | 112,435,788 | 20.4% |
| Accidentally made public | 22,350,376 | 4.1% |
| Theft or loss of computer or drive | 6,231,790 | 1.1% |
| Fraud | 2,417,320 | 0.4% |
| Unknown | 150,477 | 0.03% |

**Symantec report 2014*

### 5.1.4. ATTAQUANTS




** Verizon 2013*

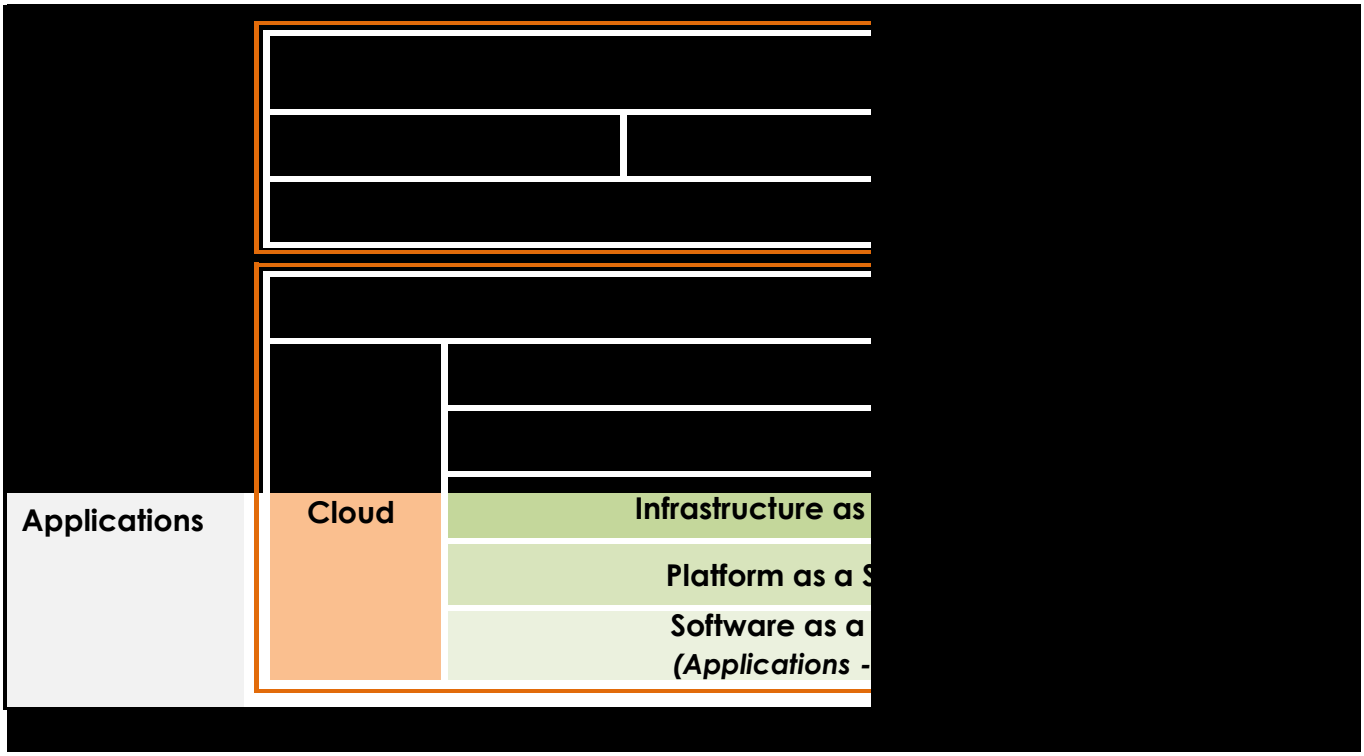
### 5.1.5. LES RISQUES CYBER D'ORIGINE MALVEILLANTE/CRIMINELLE

| Acteur Malveillant | Motivations | Cibles | Impacts |
|---|---|---|---|
| **Nation**  | • Economique, politique, et militaire | • Secrets, brevets,<br>• Information sensible,<br>• Technologique nouvelle/émergente<br>• Infrastructure critique<br>• Carence de fournisseur(s) stratégique(s) | ▶ Perte d'avantage et de compétitivité,<br>▶ Perturbation d'infrastructures critiques<br>▶ Conflits politiques/diplomatiques |
| **Organisation criminelle**  | • Gain financier immédiat<br>• Collecte d'informations pour de futurs gains financiers | • Systèmes de règlement financiers/de paiement/ Serveur Terminal Caisses<br>• PCI (« Payment Card Information »)<br>• Information employés identifiable<br>• Information / données clients, cartes bancaires | ▶ Enquêtes et sanctions réglementaires coûteuses<br>▶ Poursuites engagés par les clients et actionnaires<br>▶ Perte de confiance du consommateur |
| **Organisation Terroriste**  | • Politique, idéologique ou religieuses afin d'entrainer une désorganisation générale et susceptible de créer la peur et la panique | • Tout système d'informations : les media, les entreprises, les sites gouvernementaux, les systèmes SCADA, les particuliers | ▶ Menace la paix et la sécurité et de la sureté nationale par des actions ayant pour conséquence des :<br>• dommages matériels<br>• atteintes aux personnes |
| **Hacktiviste**  | • Influence politique et/ou au changement social/sociétale<br>• Pression sur les entreprises pour changer leur pratiques | • Secret industriel ou commerciaux<br>• Information commerciale sensible/ politique des prix/références fournisseurs<br>• Informations relatives aux principaux dirigeants, personnel, clients et partenaires | ▶ Perturbation des activités de l'entreprise, perte de marché<br>▶ Marque et réputation<br>▶ Perte de confiance du consommateur |
| **Insiders Initiés**  | • Avantage personnel, gain financier<br>• Vengeance professionnelle<br>• Patriotisme | • Ventes, offres, marchés stratégiques<br>• Secret industriels et commerciaux y compris des partenaires, et dans une moindre mesure brevet, R&D,<br>• Opération, stratégie commerciale<br>• Information personnel | ▶ Divulgation de secrets professionnels, brevets,<br>▶ Perturbation des opérations,<br>▶ Marque et réputation,<br>▶ Impact sur la sécurité |

### 5.1.6. Les risques cyber d'origine accidentelle

| Incidents accidentels | Nature de l'évènement | Conséquences | Impacts financiers |
|---|---|---|---|
| **Erreur humaine**  | • **Erreur de programmation,**<br>• **Erreur d'implémentation,**<br>• **Erreur d'utilisation,**<br>• **Erreur de maintenance** | ► **Arrêt des systèmes d'informations**<br>► **Responsabilité en cas d'erreur opération client, délivrance de bien ou services,**<br>► **Perte ou altération de données client, de données confidentielles, ou de données d'exploitation**<br>► **Procédure réglementaire** | ► **Frais supplémentaires d'exploitation**<br>► **Frais de défense / Dom*m*ages et intérêts**<br>► **Frais de reconstitution de données**<br>► **Pertes d'exploitation**<br>► **Cout du matériel de remplacement**<br>► **Frais et sanction administrative** |
| **Panne/problèmes techniques**  | • **Défaut de maintenance**<br>• **Problème de mise en production d'un logiciel**<br>• **Problème d'interopérabilité des systèmes avec fournisseurs, tiers, client**<br>• **D'origine industrielle électrique : commutation de contacts, fonctionnement de thyristors, etc.**<br>• **Electronique :** réseau **de distribution, problème de relais,** | | |
| **Evènement naturel**  | • **Incendie,**<br>• **Inondation,**<br>• **Dégât des eaux**<br>• **Tempête**<br>• **Foudre et surtension électriques liées** | | |

### 5.1.7. Atteintes aux systèmes d'information




### **5.1.8.** Atteintes aux données détenues, collectées, hébergées, exploitées**, …**

La sécurité des données doit répondre à trois objectifs principaux :

1. La disponibilité
   - L'information doit être accessible à tous ceux qui en ont besoin (et y sont autorisés)
2. La confidentialité
   - L'information doit rester accessible uniquement aux personnes autorisées
3. L'intégrité
   - 'information ne doit pas être corrompue ou rendue incomplète.

Deux autres objectifs permettent d'élargir les premiers pour définir la sécurité du système d'information :

1. La non-répudiation et l'imputation
   - Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur
2. L'authentification
   - L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

| | Données personnelles | Données confidentielles | Données d'exploitation |
|---|---|---|---|
| **Type de données de Tiers ou propriété de la société** | **Données réglementées, données de clients, données personnelles**<br>**Secrets industriel, secrets commerciaux, R&D,**<br>**Big Data**<br>**Données concurrentielles**<br>**Référencement fournisseurs et politique des prix**<br>**Données stratégiques et financières**<br>**Marques**<br>**Données d'archives**<br>**Données logistiques**<br>**Données de consommateurs, d'employés, RH**<br>... | | |

5.1.9. Impacts financiers :

La norme **ISO 27005** définit le capital à protéger concernant la sécurité de l'information :

1. **Les actifs primaires :**

- Les processus et l'activité
- L'information

2. **Les actifs de support :**

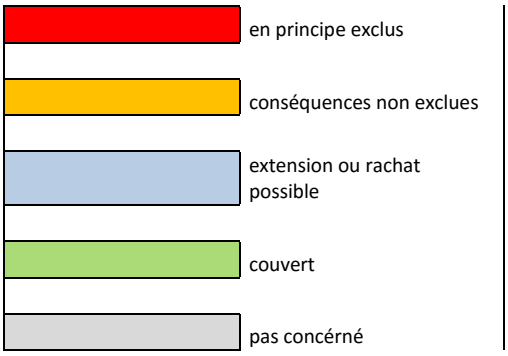
- Le matériel
- Les logiciels
- Les réseaux
- Le personnel
- Les sites
- Le support organisationnel (autorités de tutelle, maison-mère, département, agences, etc.)

On peut également distinguer les pertes que l'entreprises subit et celle qu'elle cause aux tiers.

| Pertes subies | Impacts financiers potentiels |
|---|---|
| **Pertes ou dommages aux données** | Perte ou détérioration de données ou de logiciels, entrainant des coûts de restauration, de mise à jour, de reconstitution ou de remplacement de ces actifs |
| **Interruption d'activité ou indisponibilité du réseau** | Perte d'exploitation en cas d'interruption, dégradation du service ou ralentissement du réseau, qui entraînent une perte de revenus, une augmentation des coûts de fonctionnement et/ou des frais d'atténuation et d'investigation |
| **Atteinte à la réputation** | Découlant d'une violation de la protection des données qui entraîne une perte de la propriété intellectuelle, une perte de revenus, une perte de marché |
| **Investigation par le régulateur sur le non-respect de la vie privée** | Enquête, procédure réglementaire (CNIL) ; frais de défense, amendes résultant d'une enquête ou d'exécution d'une régulateur en raison de la sécurité et de la responsabilité de la vie privée |
| **Frais de notification** | Frais juridique, frais de poste et de communication dans les pays où il y a une obligation légale ou réglementaire d'informer les individus d'une violation de sécurité ou de confidentialité, y compris les frais de réputation liés |

## 5.2. ANNEXE 2 – TABLEAU DES GARANTIES EXISTANTES

| Scenarii | Impacts | | Programmes d'assurance concernés | | | |
|---|---|---|---|---|---|---|
| **Descriptif** | **Impacts directs subis par l'organisation** | **Impacts causés aux tiers** | **Police RC** | **Police Dommage/PE** | **Police FRAUDE** | **Police CYBER** |
| Lancement d'attaques contre des entreprises tierces par un pirate via les systèmes d'information de l'organisation | Perte d'image et de chiffre d'affaires | Réclamation en RC pour mauvaise sécurité des systemes | possibilité d'une couverture spécifique | | | Spéciciquement couvert y compris pertes propres |
| Compromission de données stratégiques confidentielles de l'organisation suite à APT (Advanced Persistent Threat) | Arrêt d'activité, Perte d'exploitation, Frais supplémentaires d'exploitation, concurrence. | | | Non couvert en principe | | |
| Compromission de données stratégiques confidentielles de tiers | Réclamation client, pénalités contractuelles, frais supplémentaire d'exploitation, perte d'exploitation, | Atteinte à la confidentialité des données et éventuellement utilisation frauduleuse des données | Exclusion divulgation de secret professionnels | Non couvert en principe | Si détournement d'actifs ou de biens | Spéciciquement couvert y compris pertes propres |
| Indisponibilité du SI et du service fourni par l'infogérant à l'organisation suite évènement malveillant (y compris DOS) | Perte d'exploitation, frais supplémentaires d'exploitation, pénalités contractuelles | Non exécution ou retard dans l'execution de services, PE, réclamation clients, | | Non couvert en principe | | |
| Indisponibilité du SI et du service fourni par l'infogérant à l'organisation suite évènement accidentel ou naturel sur équipement | Perte d'exploitation, frais supplémentaires d'exploitation, pénalités contractuelles | Non exécution ou retard dans l'execution de services, PE, réclamation clients, | Conséquences RC non exclues | Non couvert en principe | | |
| Erreur d'un info-gérant ou de ses employés générant une compromission de la sécurité des données confidentielles de tiers | Perte financière, pour l'organsiation ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification aux clients et à la CNIL | Destruction ou altération des données de tiers | Exclusion virus + exclusion secrets professionnels | | | Spécifiquement couvert après analyse de la supply chain info gérance |
| Erreur de l'organisation ou ses employés générant une compromission de la sécurité des données confidentielles de tiers | Perte financière, pour l'organisation ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification aux clients et à la CNIL | Destruction ou altération des données de tiers | Exclusion virus + exclusion secrets professionnels | | | Spéciciquement couvert y compris pertes propres |
| Erreur de programmation de la part de l'infogérant | Perte financière, pour l'organisation ou ses clients | Non exécution ou retard dans l'execution de services, PE, réclamation clients, | | | | |
| Demande de rançon pour éviter une attaque sur le SI ou pour éviter de divulguer des informations ou obtenir la clé de chiffrement | Montant de la rançon, mise en cause client | Perte de données de tiers par cryptage = mise en cause | | | | Rachat d'exclusion possible |
| Virus informatique affectant les systèmes d'information de l'orgsanition (bombe logique, déni de service) | Perte financière, pour l'organisation ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification<br><br>Prise de contrôle des systèmes d'exploitation et production (SCADA) avec dommage à l'outil de | Non exécution ou retard dans l'execution de services, PE, réclamation clients, compromission des systèmes de CLIENTS. Atteintes aux bien ou aux personnes suite à incendie, explosion | Exclusion virus partiellement rachetée | Exclusion virus , Pas de garantie PE, doute sur la garantie des dommages matériels. | | Doute sur la portée de l'exclusion des dommages matériels. |



## 5.3. ANNEXE 3 - TABLEAU COMPARATIF DES ENVIRONNEMENTS REGLEMENTAIRES FR UK DE US EU

| | FRANCE | GRANDE BRETAGNE | ALLEMAGNE | U.S. | E.U. |
|---|---|---|---|---|---|
| **Opérateurs télécom** | **La CNIL (Commission Nationale Informatique et Libertés)**<br>***Loi « Informatique et Libertés », 6 janvier 1978 créant La CNIL***<br>***Ordonnance du 24 août 20 11 « Le Paquet Télécom »*** | **ICO (Information Commissioner's Office)**<br>***Data Protection Act 1998 (DPA)*** | **BfDI (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit),**<br>**Andesdatenschutzbeauftragte, Bundesnetzagentur**<br>***Bundesdatenschutzgesetz (BDSG)***<br>***Telekommunikationsgesetz (TKG*** | **Federal Trade Commission (FTC), Consumer reporting agencies,**<br>**State Attorney General and others….**<br>***Fair and Accurate Credit Transactions Act (FACTA) 2003***<br>***The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009,***<br>***47 state breach notification laws*** | ***Directive 95/46/CE du 24 oct.1995***<br>***et***<br>***Proposition de Règlement du parlement européen et du conseil du 25 janvier 2012***<br>***Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Unione***<br>***2015 december 18th*** |
| | • **Définition de « 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* | • **Définition de « donnée à caractère personnel »** : *« donnée concernant un individu vivant qui peut être identifié grâce à cette donnée, ou à partir de cette donnée et d'autres informations qui sont en possession du contrôleur* | • **Définition « donnée à caractère personnel » : «** toute information concernant la situation personnelle ou matérielle [...] d'une personne physique identifiée ou identifiable » | • **Définition des « informations personnelles identifiables » (PII) :** données ou agrégation de données, nom ou numéro pouvant être utilisé, seul ou en conjonction | • **Données à caractère personnel:** toute information concernant une personne physique identifiée ou identifiable ("personne concernée"); est réputée identifiable une personne qui peut être identifiée directement ou indirectement (…), |

| | | | | | |
|---|---|---|---|---|---|
| | *d'identification ou à un ou plusieurs éléments qui lui sont propres*. » (art. 2, al. 2, Loi Informatique et Libertés) | *de données* (data controller)*, ou pourraient être en possession du contrôleur de données*». | | avec toute autre information pour identifier une personne spécifique. | notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation, ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. |
| | □ | **• Définition de « donnée sensible à caractère personnel » :** données personnelles concernant des informations à caractère racial ou ethnique, des informations portant sur des opinions politiques, sur des croyances religieuses ou d'autres croyances de nature similaire, sur l'appartenance à un syndicat, sur la santé mentale ou physique, sur la vie sexuelle, sur l'éventuelle commission d'une infraction, sur toute procédure engagée relative à la commission d'une infraction ou sur toute sanction de cette infraction. | □ | **• Définition des « informations médicales personnelles » (PHI) :** informations concernant l'état de santé, la prestation de soins de santé, ou le paiement de soins de santé pouvant être lié à un individu spécifique.<br>• Définition de l' « information sur les consommateurs » : toute collecte concernant un individu, que ce soit sous forme papier, électronique ou toute autre forme, qui constitue un rapport concernant un consommateur ou qui est dérivé d'un tel rapport.<br>• Définition d' "atteinte aux données " / " atteinte à la sécurité " : perte, vol, ou tout autre accès non autorisé, autre que ceux qui ont trait à la portée de son travail, à des données contenant des informations personnelles sensibles, sous forme électronique ou imprimée, qui a pour conséquence la potentielle altération de la confidentialité ou de l'intégrité des données. | **Données à caractère personnel concernant la santé :** les données se rapportant à l'état de santé d'une personne concernée qui comportent des informations sur la santé physique ou mentale passée, présente ou future de la personne concernée, y compris des informations relatives à l'enregistrement du patient pour la prestation de services de santé (…), un numéro ou un symbole attribué à un patient, destinés à l'identifier de manière univoque à des fins médicales, (…) des informations obtenues lors d'un contrôle ou de l'examen d'un organe ou d'une substance corporelle, y compris des données génétiques et des échantillons biologiques, (…) ou toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'une épreuve diagnostique in vitro |

| | | | | | |
|---|---|---|---|---|---|
| | | · **Champ d'application de la loi** : concerne tout traitement de données personnelles, à l'exception du traitement pour un usage domestique (par l'individu concerné lui-même, par sa famille ou son ménage) et du traitement réalisé pour sauvegarder la sécurité nationale. | · **Champ d'application de la loi** : la collecte, le traitement, la transmission et l'utilisation de données à caractère personnel par des autorités et des personnes privées, à l'exception du traitement pour un usage domestique. Il existe des exceptions légales. | | |
| | **• Définition du responsable du traitement informatique des données personnelles** (art. 3, Loi) :<br><br>→ 2 critères : 1). décide de la finalité du traitement ; 2). décide des moyens du traitement.<br>→ Il s'agit du dirigeant ou de certains employés explicitement désignés (le RSSI, le DSI ou le CIL) ou de « tiers autorisés » ponctuellement et de manière motivée (police, fisc…). | **• Définition du responsable de traitement des données personnelles** : pas de critère. Vise toutes les personnes qui traitent des données entrant dans le champ d'application de la loi. | **• Définition du responsable de traitement des données personnelles** : pas de critère. Vise toutes les personnes qui traitent des données entrant dans le champ d'application de la loi ou font traiter des données par des tiers. | **Aucune définition du responsable de traitement des données personnelles.**<br><br>• 47 États, le District de Columbia, Guam, Porto Rico et les îles Vierges ont adopté une législation obligeant les **entités privées, gouvernementales ou éducatives** à informer les personnes des atteintes à la sécurité des informations impliquant des informations personnellement identifiables.<br>• FACTA s'applique à toute organisation qui recueille, stocke ou transmet de l'information concernant les consommateurs.<br>• Loi HITECH s'applique à des entités qui accèdent, maintiennent, modifient, enregistrent, stockent, détruisent, détiennent, utilisent ou divulguent de façon non sécurisée des informations de santé protégées | **• Définition du responsable du traitement:** La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités (…) et les moyens du traitement de données à caractère personnel<br><br>**• Traitement de données à caractère personnel:** Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion (…), ainsi que la limitation, l'effacement ou la destruction; |

| | | | | | |
|---|---|---|---|---|---|
| | · **Obligations pesant sur tout responsable de traitement informatique des données personnelles** :<br><br>- Sécurité des fichiers (sécurité logique, physique et adaptée à la nature des données et aux risques présentés par le traitement).<br>- Confidentialité des données (seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier).<br>- Durée de conservation des données : les données personnelles ont une date de péremption. Cette date est fixée par le responsable d'un fichier en fonction de l'objectif du fichier.<br>- Finalité du traitement : un fichier doit avoir un objectif précis. Les informations exploitées dans un fichier doivent être cohérentes par rapport à son objectif. Les informations ne peuvent pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées.<br>- Autorisation de la CNIL : les traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en œuvre, être soumis à l'autorisation de la CNIL. | · **Obligations pesant sur toute personne traitant des données personnelles** : le Data Protection Act pose 8 principes résumés ci-dessous :<br><br>- Sécurité des fichiers : des mesures de sécurité appropriées doivent être prises afin de protéger les données personnelles contre leur traitement illégal ou non autorisé et contre leur perte accidentelle ou leur destruction ; les données personnelles ne peuvent pas être transférées en dehors de l'EEE, sauf si le pays concerné applique un niveau adéquat de protection des données ;<br>- Confidentialité des données<br>- Durée de conservation des données : les données personnelles ne doivent pas être conservées plus longtemps que nécessaire.<br>- Légitimité nécessaire du traitement : le traitement des données doit être fait soit avec le consentement de l'intéressé, soit être exigé par la loi ou être nécessaire pour l'exécution d'un contrat, la protection des intérêts vitaux de l'intéressé, la réalisation de toute fonction de nature publique ;<br>- Nature des données : les données personnelles doivent être adaptées, pertinentes et proportionnées aux objectifs poursuivis ; les données personnelles doivent être précises et mises à jour.<br>- Enregistrement sur le registre des contrôleurs de données (Register of Data Controllers) : registre tenu par l'ICO (et disponible sur son site internet).<br>- Autorisation de l'ICO : chaque organisation manipulant des données personnelles doit en informer l'ICO. Il appartient ensuite à | • **Obligations pesant sur toute personne traitant des données personnelles** :<br><br>Sécurité des fichiers : mettre en place une organisation interne appropriée et des mesures techniques et organisationnelles appropriées, en particulier :<br>-contrôle d'accès (physique et logique)<br>- contrôle de transmission<br>- contrôle de l'enregistrement des données<br>- contrôle des sous-traitants<br>- protection contre la perte accidentelle et la destruction (disponibilité)<br>Les données personnelles ne peuvent pas être transférées en dehors de l'EEE, sauf si le pays concerné applique un niveau adéquat de protection des données.<br>- Confidentialité des données : seules les personnes tenues de respecter la confidentialité des données peuvent accéder aux données personnelles.<br>- Durée de conservation des données : les données personnelles ne doivent pas être conservées plus longtemps que nécessaire. - Notification aux personnes concernées sur le stockage des données personnelles<br>- Information sur les données stockées aux personnes concernées (sur demande)<br>- Rectification, effacement ou verrouillage des données (sur demande de la personne concernée)<br>- contrôle par l'autorité compétente chargée de la protection des données<br>Obligation de notifier, sans délai, à l´autorité compétente et aux personnes concernées le transfert non autorisé ou la violation de données personnelles à caractère sensible. | · **Obligations en vertu des lois de l'Etat (applicable à toute personne ayant une activité commerciale ou toute entité gouvernementale ou éducative) :**<br>- Information : aviser les personnes touchées par des atteintes de leurs informations personnelles sensibles ;<br>- Sécurité / Confidentialité des données : dans certains cas, mettre en œuvre des programmes de sécurité de l'information pour protéger la sécurité, la confidentialité et l'intégrité des données.<br>Ces obligations s'appliquent en particulier lorsqu'il existe une possibilité raisonnable que l'atteinte cause des dommages, des blessures, une fraude ou un vol d'identité.<br>- Notification : notifier dans un délai opportun (délai variable : « 10 jours», « 45 jours», « sans délai »)<br>- Mode de notification (variable : courrier, e -mail, prévenir les nouveaux médias)<br>- Certains Etats (Californie, Connecticut) exigent qu'un service soit fourni.<br>- Certains Etats (Massachusetts) exigent une politique écrite pour la sécurité de l'information.<br>- Certains Etats exigent que le bureau du Procureur général de l'Etat soit informé. | Stratégie NIS : Chaque État membre doit adopter une stratégie nationale NIS (sécurité des Réseaux et Systèmes d'Information) définissant des objectifs stratégiques et des politiques appropriées et des mesures réglementaires en vue d' atteindre et de maintenir un niveau élevé de sécurité des réseaux et systèmes d'information<br>Autorité nationale compétente : chaque État membre désigne une ou plusieurs autorités nationales compétentes sur la sécurité des systèmes d' information et des réseaux ( «l'autorité compétente ») couvrant au moins les secteurs referencés à l'annexe II (OIV) et les services numériques visés à l'annexe III (Opérateurs de Services Digitaux) . Les États membres peuvent désigner ce rôle à une ou plusieurs autorités existantes. Les autorités compétentes doivent surveiller l'application de la présente directive au niveau national.<br>CSIRT : Chaque État membre désigne une ou plusieurs équipe de réponse aux incidents de sécurité informatiques (ci-après : « CSIRTs ») couvrant au moins les secteurs visés à l'annexe II (OIV) et les types de fournisseurs de services numériques visés à l'annexe III (Opérateurs de Services Digitaux), responsable de la gestion des incidents et des risques en fonction d'un processus bien défini.<br>Les États membres veillent à ce que les autorités compétentes ou CSIRT reçoivent les notifications d'incidents d'incidents soumis en application de la directive . |

| | | | | | |
|---|---|---|---|---|---|
| | | l'organisation - après avis de l'ICO - de mettre en place les mesures appropriées pour protéger les données personnelles et être en accord avec le texte de loi et ses 8 principes.<br><br>- Notification à l'ICO : en cas de violation ou de perte de données, il n'existe pas d'obligation légale de notifier à l'ICO. Cependant, le Guide de l'ICO indique que si un nombre important de personnes est affecté ou si la violation est particulièrement sérieuse, alors l'ICO doit être informé.<br>Dans des certains secteurs spécifiques (comme la finance), il existe une obligation de notifier la violation de données à l'autorité compétente (ex : the Financial Conduct Authority). | | | Points de contact unique : afin de permettre aux points de contact uniques de présenter un rapport de synthèse sur les notifications au Groupe de coopération, les États membres veillent à ce que les autorités compétentes ou CSIRTs informent les points de contact unique sur les notifications d'incidents présentés en application de la directive.<br>Groupe de coopération : un groupe de coopération doit être composé de représentants des États membres , la Commission et le Réseau européen d'information et de l'Agence de sécurité ( " ENISA ») . |
| | **• Obligation pesant sur les fournisseurs de services de communication électronique :**<br>Obligation de notifier, sans délai (24h), les violations de données à caractère personnel à la CNIL et aux personnes concernées par la violation, peu important leur niveau de gravité.<br>La CNIL a 2 mois pour se prononcer.<br>→ Soit pas de violation constatée : les mesures de protection ont été prises, permettant de rendre les données incompréhensibles à toute personne non autorisée, pas besoin de prévenir l'intéressé. La CNIL clôture le dossier.<br>→ Soit violation constatée : la CNIL peut contraindre le fournisseur à avertir l'intéressé. >> En cas de silence de la CNIL pendant 2 mois : le fournisseur doit considérer que les mesures prises ne sont pas appropriées et il doit informer les personnes concernées par la violation. | | | · Obligations en vertu de lois fédérales :<br>→ Loi HITECH (données personnelles sur la santé) :<br><br>- Protection des données : déployer des efforts raisonnables pour divulguer la seule information minimum nécessaire.<br>- Protection des données de santé : protéger les données de santé d'une utilisation ou divulgation inappropriée et maintenir des garanties raisonnables et appropriées du point de vue administratif, technique et physique pour empêcher l'utilisation ou la divulgation en violation des règles de confidentialité de données de santé protégées. | «La sécurité des réseaux et des systèmes d'information» signifie la capacité des réseaux et des systèmes d'information à résister , à un niveau de confiance donné, à toute action qui compromettent la :<br>- disponibilité<br>- l'authenticité<br>- l'intégrité<br>- la confidentialité<br>des données stockées ou transmises ou transformés ou des services connexes offerts par ou accessibles via ce que les systèmes d' information et des réseaux |

| | | | | | |
|---|---|---|---|---|---|
| | □ | | | **- Information des individus :** en cas de d'atteintes à leurs données personnelles de santé.<br>**- Alerte du « Department of Health Services »** (HHS) et des médias : dans les cas où une atteinte affecte plus de 500 personnes. Les violations de sécurité qui touchent moins de 500 personnes seront communiquées au HHS sur une base annuelle.<br>**- Alerte du gouvernement fédéral** : les fournisseurs de Dossier de Santé Personnel (« PHR »), les prestataires de services de ces fournisseurs et les réparateurs de PHR sont tenus d'aviser le gouvernement fédéral.<br><br>**→ FACTA :**<br>- Information des consommateurs : les organisations doivent prendre des mesures raisonnables pour protéger l'information des consommateurs tout au long du cycle de vie de ces données. Les consommateurs peuvent contester toute information inexacte.<br>- Alerte du consommateur : une notification de type «premier avertissement » (alertes à la fraude et alertes de service actif) doit alerter le consommateur de tout dysfonctionnement constaté sur un compte. | Les États membres veillent à ce que les fournisseurs de services digitaux identifient et prennent les mesures techniques et organisationnelles appropriées et proportionnées pour gérer les risques liés à la sécurité des réseaux et des systèmes d'information. Ces mesures doivent prendre en compte les éléments suivants:<br>- La sécurité des systèmes et des installations,<br>- La conformité avec les normes internationales.<br>- Surveillance, de vérification et d'essais,<br>- Gestion de la continuité des affaires,<br>- La gestion des incidents<br>En particulier, des mesures doivent être prises pour prévenir et minimiser l'impact des incidents affectant la sécurité des réseaux du fournisseur de services numériques et des systèmes d'information sur les services visés à l'annexe III (Fournisseurs de services digitaux) qui sont offerts au sein de l'Union, cherchant ainsi à assurer la continuité de ces services. |

| | | | | | |
|---|---|---|---|---|---|
| | **• Obligation des fournisseurs télécom à l'égard de leurs sous-traitants** :<br>La CNIL impose aux entreprises donneuses d'ordre de réaliser un audit auprès de leurs sous-traitants sur l'application des mesures de sécurité et de confidentialité des données. Sinon, elles sont responsables du fait de leurs sous-traitants. | **• Obligation des fournisseurs d'un service public télécom** :<br>Notification à l'ICO : il n'existe pas d'obligation prévue par le DPA. Cependant, la directive « Privacy and Electronic Communications Regulations 2003 » exige des fournisseurs qu'ils notifient toute violation des données personnelles à l'ICO. | **• Obligations (supplémentaires) pesant sur les fournisseurs de services de communication électronique (§ 109a TKG):**<br>Obligation de notifier, sans délai (24h), toutes violations de données à caractère personnel à la Bundesnetzagentur et au BfDI.<br>En cas de violation grave : obligation de notifier aux personnes concernées. | | Les États membres veillent à ce que <u>les fournisseurs de services digitaux notifient tout incident ayant un impact substantiel</u> sur la fourniture d'un service qu'ils offrent sein de l'Union à l'autorité compétente ou au CSIRT.<br>Les notifications doivent comporter des informations pour permettre à l'autorité compétente ou CSIRT pour déterminer l'importance de toute incidence transfrontalière. La notification ne doit pas exposer la partie notifiante à la responsabilité<br>Pour déterminer l' impact d'un incident , les paramètres suivants doivent être pris en compte , en particulier:<br>( a) le nombre d'utilisateurs touchés par l'incident , notamment les utilisateurs comptent sur le service pour la fourniture de leurs propres services ;<br>( b) la durée de l'incident;<br>( d) la mesure de la perturbation du fonctionnement du service<br>( c) la répartition géographique à l'égard de la zone touchée par l'incident ;<br>( e ) la mesure de l'impact sur les activités économiques et sociétaux<br>L'obligation de notifier un incident ne vaut que si le fournisseur de service numérique a accès à l'information nécessaire pour apprécier si les critères sont remplis.<br><u>Tout impact significatif sur la continuité des services essentiels d'un OIV en raison d'un incident affectant un fournisseur de service digitaux sera notifiée par l'OIV.</u> |

| | | | | | |
|---|---|---|---|---|---|
| | **• Sanction des entreprises et des responsables de traitements :**<br><br>→ Sanctions pénales :<br>- en cas de non-respect de l'obligation de sécurité (art. 226-17 C. pénal : 5 ans + 300.000€ d'amende).<br>- en cas de communication d'information à des personnes non autorisées (art. 226-22 C. pénal : 5 ans + 300.000€ d'amende, sauf imprudence ou négligence : 3 ans + 100.000€ d'amende).<br>- en cas de détention des données pour une durée supérieure à celle déclarée (art. 226-20 C. pénal : 5 ans + 300.000€ d'amende).<br>- en cas de refus ou d'entrave à l'information des personnes (art. 131-13 C. pénal : 1500€ d'amende par infraction et 3000€ en cas de récidive).<br>- en cas de non-accomplissement des formalités auprès de la CNIL (art. 226-16 C. pénal : 5 ans + 300.000€ d'amende).<br>- en cas de détournement de finalité des données (art. 226-21 C. pénal : 5 ans + 300.000€ d'amende).<br><br>→ Sanctions administratives :<br>La CNIL peut sanctionner tout manquement à la Loi « Informatique et Libertés » après enquête. Les sanctions prononcées doivent être proportionnelles à la gravité des manquements et des avantages tirés de ces manquements. Les pouvoirs de la CNIL :<br>- avertissement,<br>- astreinte,<br>- amende (150.000€ maximum pour une première sanction, 300.000€ en cas de récidive) | **• Sanctions de toute personne traitant des données personnelles :**<br><br>→ Sanctions des « civil offences » par le juge :<br>- en cas de non-respect de la confidentialité des données : cela vise notamment le fait d'avoir obtenu des données personnelles de manière illégale (vise les hackers et les imposteurs) ;<br>- en cas de diffamation ;<br>- en cas de « negligence » : la sanction du manquement à l'obligation générale de diligence (« duty of care ») est prévue par le DPA dans tous les cas où une donnée personnelle est conservée ou traitée ;<br>- le fait de procéder au traitement de données personnelles sans s'être enregistré préalablement sur le registre de l'ICO (« Register of Data Controllers ») ;<br>- le fait de ne pas respecter les notifications de l'ICO (amende de 5.000 livres).<br><br>Les sanctions sont prononcées par le juge. Il peut accorder des dommages et intérêts aux victimes et/ou ordonner la suppression des données personnelles pour prévenir d'autres dommages. | **• Sanctions de toute personne traitant des données personnelles :**<br><br>→ Sanctions pénales :<br><br>En cas du dessein d'enrichissement ou d'intention de causer un dommage : 2 ans de prison ou une peine pécuniaire appropriée.<br><br>→ Sanctions administratives :<br><br>En cas de non-respect des obligations légales /manquements : amende de 300.000€ (maximum), pouvant être augmentée en cas d´avantage économique plus important du coupable. | **• Les sanctions de droit varient suivant les Etats.**<br>- Certains Etats prévoient une sanction pécuniaire. Ex : Michigan : 750.000 $ maximum par atteinte de sécurité.<br>- Certains États prévoient que des pénalités et des dommages-intérêts appropriés puissent être évalués.<br><br>Les sanctions de droit visent les entités et leurs associés d'affaires. Ils peuvent être tenus civilement ou pénalement responsables des atteintes constatées.<br><br>**• Loi HITECH :**<br>Les sanctions varient de 100 $ à 1.500.000 $ au maximum.<br>La loi ne permet pas à un individu d'intenter une action contre un fournisseur. Cependant, elle permet au Procureur général de l'Etat d'intenter une action au nom de ses résidents.<br>Enfin, le HHS est maintenant nécessaire pour effectuer des audits périodiques des entités et de leurs associés d'affaires visés. | Sanctions : les États membres fixent les règles relatives aux sanctions applicables aux violations des dispositions nationales prises en application de la présente directive et prennent toutes les mesures nécessaires pour veiller à ce qu'elles soient mises en œuvre . Les sanctions prévues doivent être efficaces, proportionnées et dissuasives.<br>Les États membres informent la Commission de ces règles et de ces mesures et lui notifient , sans délai , toute modification ultérieure les concernant. |

| | | | | | |
|---|---|---|---|---|---|
| | | **→ Sanctions par l'ICO :**<br>L'ICO peut sanctionner tout manquement au Data Protection Act 1998 et au Privacy and Electronic Communications Regulations Act 2003. L'ICO, comme la CNIL, possède un pouvoir de contrôle et peut recevoir et instruire des plaintes.<br>Les pouvoirs de l'ICO :<br>- injonction : de prendre des mesures spécifiques pour se conformer avec le DPA,<br>- audit : l'ICO a l'autorité pour auditer les services départementaux sans autorisation.<br>- pénalité monétaire : amende jusqu'à 500,000 livres en cas de manquement sérieux au DPA,<br>- poursuites : incluant une possible peine de prison en cas de manquement délibéré au DPA,<br>- sanction des « criminal offences » : en cas de manquement portant sur des données sensibles traitées par les administrations publiques (ex : informations portant sur des condamnations pénales). L'ICO prononce des amendes (maximum 3.000€ en cas de poursuite sommaire ; maximum 100.000€ en cas de mise en accusation). | | **• FACTA :**<br><br>- Poursuites par le FTC : le FTC peut intenter une action pouvant entrainer jusqu'à 2500 $ de pénalités par effraction constatée à une règle du drapeau rouge.<br><br>- Poursuites par le bureau du Procureur général d'État : il peut réclamer jusqu'à 1000 $ pour chaque atteinte, ainsi que la prise en charge des frais d'avocat.<br><br>- Poursuites civiles par les consommateurs : les consommateurs peuvent avoir droit à réparation des dommages réels subis du fait du non-respect d'une des dispositions de FACTA, plus d'additionnels dommages et intérêts déterminés par voie de justice ainsi que la prise en charge des frais d'avocat. | |
| | **• Sanction des fournisseurs télécom :**<br><br>→ Sanction pénale : 5 ans d'emprisonnement + 300.000€ d'amende (226-17-1 C. Pénal).<br><br>→ Sanction administrative par la CNIL pour manquement à la Loi Informatique et Libertés.<br><br>• Cumul possible des sanctions pénales et administratives. | **• Sanction des fournisseurs d'un service public télécom** : En cas de défaut de notification à l'ICO : amende de 1.000 livres ainsi qu'une mauvaise publicité par l'ICO. | **• Sanctions (supplémentaires) des fournisseurs télécom :**<br><br>→ Sanctions administratives :<br><br>En cas de non-respect des obligations légales /manquements (§ 109 a TKG) : amende de 100.000€ (maximum), pouvant être augmentée en cas d'avantage économique plus important du coupable. | | |

| | FRANCE | GRANDE BRETAGNE | ALLEMAGNE | U.S. | E.U. |
|---|---|---|---|---|---|
| **Opérateurs d'importance vitale (OIV)** | **ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)**<br><br>***Arrêté du 3 juillet 2008***<br>***Loi de Programmation Militaire (LPM) du 18 décembre 2013*** | **CPNI (Center for the Protection of National Infrastructure)**<br><br>***Security Service Act 1989*** | **BSI (Bundesamt für Sicherheit in der Informationstechnik)**<br><br>***BSI Gesetz,***<br>***IT Sicherheitsgesetz*** | **Projet de Loi fédérale à l'étude** | ***Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union 2015 december 18th*** |
| | • **Définition des OIV** : tous les opérateurs ayant une activité d'importance vitale.<br><br>Liste des secteurs d'importance vitale : activités civiles de l'Etat ; activités militaires de l'Etat ; activités judiciaires ; espace et recherche ; santé ; gestion de l'eau et de l'alimentation ; énergie ; communication ; électronique ; audiovisuel et information ; transports ; finances et industrie. | • **Définition des OIV** : toute entité qui est possède ou exploite des services vitaux ou propriétés vitales pour le commerce, la santé publique ou la sécurité (institutions publiques ou privées, entreprises, organisations).<br><br>Liste des secteurs d'importance vitale : équipements médicaux et services d'urgence ; gestion de l'eau et de l'alimentation ; énergie ; réseaux de télécommunications ; institutions financières. | • **Définition des OIV** : tous les opérateurs des constructions, installations ou des parties de ceux-ci, ayant une activité d'importance vitale dans les secteurs suivants :<br><br>Liste des secteurs d'importance vitale : énergie ; technologies de l'information et de la télécommunication ; transport et circulation ; santé ; gestion de l'eau et de l'alimentation ; finance et l´assurance.<br>Les détails seront déterminés par décret. | • **Loi sur la sécurité des données de 2015 (H.R. 2205) :** Vise les particuliers, sociétés ou autres entités non gouvernementales qui accèdent, conservent, communiquent, ou manipulent des informations financières sensibles ou des informations personnelles privées.<br><br>• **Loi sur la sécurité des données et la notification des atteintes (HR 1170) :** Vise certaines entités commerciales et organisations à but non lucratif qui utilisent, accèdent, transmettent, stockent, disposent ou collectent des informations personnelles confidentielles non cryptées.<br><br>• **Loi sur la protection des consommateurs (S. 1,158) :** Vise certaines entités | • **Définition des OIV :** opérateurs de l'énergie, du transport, de la banque et de la finance, de la santé, de l'eau, des infrastructures du digital (les détails sont en annexe II du projet de directive) |

| | | | | | |
|---|---|---|---|---|---|
| | | | | commerciales qui recueillent, utilisent, accèdent, transmettent, stockent, disposent d'informations personnelles sensibles sous forme électronique ou numérique. | |
| | **• Obligations des OIV :**<br><br>- mettre en œuvre, à leurs frais, les règles de sécurité nécessaires à la protection de leurs systèmes d'information (L. 1332-6-1 Code de la défense).<br>- Informer sans délai le Premier ministre des incidents (L. 1332-6-2 Code de la défense).<br>- Soumettre leurs systèmes d'information à des contrôles pour vérifier le niveau de sécurité, à leurs frais (L. 1332-6-3 Code de la défense). → Audits effectués par l'ANSSI (avec éventuellement des experts externes à sa demande).<br>- en cas de crise majeure, le Premier ministre peut décider des mesures à mettre en œuvre par les OIV (L. 1332-6-4 Code de la défense).<br><br>**• Obligations des OIV à l'égard de leurs sous-traitants :**<br><br>Les sous-traitants qui participent aux systèmes d'information des OIV doivent respecter les mêmes niveaux et règles de sécurité. Les OIV doivent répondre de la défaillance de leurs sous-traitants intervenant sur leurs systèmes d'information. | **• Conseil du CPNI à l'égard des OIV :**<br><br>Le CPNI est issu de la fusion du NISCC (National Infrastructure Security Co-ordination Centre) et du NSAC (National Security Advice Centre) en 2007.<br><br>Initialement, le NISCC donnait des conseils sur la défense des réseaux informatiques. Le CPNI donne aujourd'hui des conseils sur la sécurité intégrée (en combinant des informations personnelles et physiques) aux entreprises et organisations qui sont en charge des infrastructures nationales.<br><br>C'est à travers ces conseils que le CPNI protège la sécurité nationale aux Royaume-Uni, en aidant ainsi à réduire la vulnérabilité des infrastructures nationales face au terrorisme et aux autres menaces.<br><br>**• Contrôle des OIV :**<br><br>Le Security Service Act permet au Ministre de prendre des mandats judiciaires afin de mener certaines actions. L'exécution du mandat judiciaire est encadrée par un « Commissioner » et est réalisé dans le cadre d'une procédure d'investigation devant le tribunal. | **• Obligations des OIV :**<br><br>- sécuriser leur système informatique selon l'état actuel de la technique.<br>- faire contrôler les mesures de sécurité au moins tous les 2 ans.<br>- notifier sans délai tous les incidents de sécurité importants au BSI (le BSI va partager les résultats et expériences avec tous les OIV).<br><br>• Obligations particulières des opérateurs des sites web :<br><br>Exigences accrues quant aux mesures techniques et organisationnelles visant à protéger les données des clients.<br><br>**• Obligations particulières des opérateurs des réseaux de télécommunications:**<br>Avertir le client lorsque la ligne d'accès du client est utilisée dans une attaque (si, par exemple elle fait partie d'un botnet). | **• Loi sur la sécurité des données de 2015 (H.R. 2205):**<br><br>- Exige des individus, sociétés ou autres entités non gouvernementales la mise en œuvre d'un programme de sécurité de l'information et d'information des consommateurs ;<br>- Exige, par application de la loi fédérale, la mise en place d'agences administratives appropriées.<br>- Exige, par application de la loi fédérale, la mise en place de réseaux de cartes de paiement appropriés.<br>- Exige, par application de la loi fédérale, la mise en place d'agences d'information aux consommateurs de certains manquements de données d'informations sensibles et non encodées susceptibles de provoquer des usurpations identité ou des transactions frauduleuses sur des comptes financiers de consommateurs.<br><br>**• Loi sur la sécurité des données et la notification des atteintes (HR 1170) :**<br><br>Exige de certaines entités commerciales et des organisations à but non lucratif de restaurer l'intégrité, la sécurité et la confidentialité de leurs systèmes de | **• Obligation des OIV**<br><br><u>Les États membres veillent à ce que les OIV notifient sans délai à l'autorité compétente ou au CSIRT tout incident ayant un impact significatif sur la continuité des services qu'ils fournissent .</u><br>Les notifications doivent inclure des informations pertinentes permettant de permettre à l'autorité compétente ou le CSIRT pour déterminer toute incidence de l' effet transfrontalier de l'incident .<br><br>Pour déterminer l'importance de l' impact d'un incident , les paramètres suivants seront notamment pris en compte:<br>( a) le nombre d'utilisateurs touchés par l'interruption d'un service essentiel ;<br>( b) la durée de l'incident;<br>( c) la répartition géographique à l'égard de la zone touchée par l'incident .<br><br>Après consultation de l'OIV concerné , l'autorité compétente ou le CSIRT peuvent informer le public ou exiger des OIV de le faire, des incidents individuels , lorsque la sensibilisation du public est nécessaire pour prévenir ou traiter un incident.<br><br>Les autorités compétentes , agissant de concert au |

| | | | | | |
|---|---|---|---|---|---|
| | | | | données suite à la découverte d'une faille de sécurité.<br><br>Nécessite la notification:<br>(1) aux résidents US concernés quand il y a un risque raisonnable qu'un tel manquement entraîne l'usurpation d'identité, un préjudice économique, ou une fraude financière ;<br>(2) à la FTC et aux services secrets américains ou au FBI, si une personne non autorisée accède ou acquiert des informations personnelles de plus de 10.000 personnes;<br>(3) aux agences d'information et aux consommateurs si l'avis doit être fourni à plus de 10.000 personnes. | sein du groupe de coopération développent et adopte des guidelines concernant les circonstances dans lesquelles les OIV sont tenus de notifier les incidents , y compris sur les paramètres seravnt à déterminer l'importance de l' impact d'un incident. |
| | □ | □ | □ | **• Loi sur la protection des consommateurs (S. 1,158) :**<br><br>- Exige de certaines entités commerciales qui recueillent, utilisent, accèdent, transmettent, stockent, ou disposent d'informations personnelles sensibles sous forme électronique ou numérique de 10.000 ou plusieurs personnes américaines au cours d'une période de 12 mois de mettre en œuvre un programme de respect de la vie privée des consommateurs et de sécurité des données qui respecte les règles de protection identifiées par la FTC.<br><br>- Exige que les entités, suite à la découverte d'une atteinte de la sécurité, avisent les résidents pour lesquels on suspecte | Tout impact significatif sur la continuité des services essentiels d'un OIV en raison d'un incident affectant un fournisseur de service digitaux sera notifiée par l'OIV. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | que des renseignements personnels non encodés ont été consultés ou exfiltrés.<br>La loi définit des procédures de notification spéciales pour : (1) des entités tierces qui conservent ou traitent des données sous forme électronique au nom d'une autre entité ; et (2) certains fournisseurs de transmission électronique de données , de routage, de stockage, ou de services de connexion réseau. | |
| | | | | - Exige des entités de notifier à une entité fédérale désignée par le Department of Homeland Security (DHS) si une atteinte à la sécurité concerne : (1) des informations personnelles concernant plus de 5.000 personnes, (2) des bases de données contenant des informations personnelles concernant plus de 500.000 personnes à l'échelle nationale, (3) des bases de données fédérales, ou (4) des employés et entrepreneurs impliqués dans la sécurité nationale ou l'exécution de la loi fédérale.<br>- Exige de l'entité désignée qu'elle fournisse l'information reçue aux : (1) services secrets américains ou FBI à des fins d'application de la loi ; et (2) autres organismes fédéraux pour l'application de | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | la loi, de la sécurité nationale, ou à des fins de sécurité des données. Elle établit un processus pour le ministère de la justice (DOJ) permettant l'ajustement des seuils de déclenchement applicables pour le renforcement des dispositions légales et les notifications de sécurité nationale.<br><br>- Exige que l'avis concernant certains manquements soit fourni aux agences d'information des consommateurs et à la FTC. | |
| | **• Sanction des dirigeants des OIV :**<br><br>L. 1332-7, Code de la défense :<br>- Pour les dirigeants personnes physiques : amende de 150.000€. Sanction prononcée après mise en demeure, sauf concernant l'information sans délai du Premier ministre.<br>- Pour les dirigeants personnes morales : amende max de 150.000€ x 5 (art. 131-38 du Code pénal). | → Le CPNI n'a pas de pouvoir de sanction.<br><br>→ Le Ministre peut prendre des mandats judiciaires (procédure judiciaire). | • **Sanction des OIV :**<br><br>→ Sanctions administratives : en cas de non-respect des obligations légales /manquements amende de 100.000€ (maximum). | **• Loi sur la protection des consommateurs (S. 1,158) :**<br><br>→ Sanction pénale : la loi crée une infraction pénale pour dissimulation d'une atteinte de la sécurité des données informatiques contenant des informations personnelles identifiables et sensibles qui entraîne un préjudice économique de 1000 $ ou plus à toute personne.<br><br>→ Sanction civile : la loi autorise le ministère de la Justice (DOJ) à intenter une action civile pour interdire à des personnes non autorisées ou à des entités d'accéder ou de transmettre des commandes informatiques (les « botnet »), qui :<br>- entraveraient l'intégrité ou la disponibilité de plus de 100 ordinateurs utilisés par les institutions financières ou le gouvernement fédéral ;<br>- affecteraient le commerce ou la | **• Sanctions des OIV** :<br>Les États membres fixent les règles relatives aux sanctions applicables aux violations des dispositions nationales prises en application de la présente directive et prennent toutes les mesures nécessaires pour veiller à ce qu'elles soient mises en œuvre . Les sanctions prévues doivent être efficaces, proportionnées et dissuasives.<br>Les États membres informent la Commission de ces règles et de ces mesures et lui notifient , sans délai , toute modification ultérieure les concernant. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | communication interétatique ou étrangère pendant une durée de un an ; y compris en refusant l'accès aux ordinateurs, l'installation de logiciels indésirables ;<br>- obtiendraient des informations sans autorisation.<br><br>La loi autorise la DOJ :<br>- à exiger l'aliénation ou la mise à disposition d'un bien obtenu à la suite d'une telle atteinte ;<br>- à adresser des injonctions interdisant la disposition d'un bien obtenu à la suite d'une telle atteinte. | |

## 5.4. ANNEXE 4 – SCENARIOS SINISTRES

### 5.4.1 Scenario Cloud

***Exfiltration de données***

Données confidentielles de clients d'un grand nombre d'entreprises rendues publiques de façon systémique

Scénario Stress Test Accumulation: Leakomania

Trois brèches dans la sécurité d'un logiciel permettent à un gang criminel d'organiser l'exfiltration de données provenant de milliers d'entreprises.

Des milliards d'enregistrements de données confidentielles sont divulguées en quelques mois, plus que le nombre total d'enregistrements de données confidentielles divulgués au cours des dix dernières années.

***Attaque par deni de service (DoS ou DDoS)***

Une attaque par déni de service (DoS) est une attaque informatique ayant pour but de rendre indisponible un service.

Attaques en masses pour perturber l'activité commerciale en ligne d'un grand nombre d'entreprises en désactivant leur site internet

Scénario Stress Test Accumulation: Mass DDoS

Des hacker activistes planifient la plus grande attaque par déni de service encore jamais vue et ciblent les sites internet d'entreprises commerciales pour perturber leur commerce en ligne.

Ils génèrent un trafic DDoS sans précédent, qui se concentre sur les entreprises assurées.

***Défaillance d'un fournisseur de Cloud***

Un grand nombre d'entreprises ont leur activité commerciale perturbée par la perte des fonctionnalités du Cloud quand un grand fournisseur de Cloud subit une défaillance

Scénario Stress Test Accumulation: Compromission de Cloud

Une erreur technique conduit à une panne d'un fournisseur de Cloud, ce qui provoque la perte de service de ses clients pendant plusieurs heures jusqu'à ce qu'ils soient progressivement reconnectés. La panne est à une échelle jamais vue par une politique de sécurité des contenus (CSP Content Security Policy), en termes de proportion de clients touchés et de temps de reconnexion.

***Cyber Compromission de Transaction financière***

Vol de grosses sommes d'argent par cyber-attaques sur plusieurs entreprises qui réalisent des transactions financières

Scénario Stress Test Accumulation: Intrusion sur transactions financières

Une opération coordonnée de vol sur de nombreuses sociétés de services financiers permettant de voler des fonds provenant de transactions, d'argent des distributeurs automatiques, et d'effectuer les délits d'initiés en utilisant des informations sensibles. Elle est réalisée à une échelle jamais observée à ce jour.

***Cyber Extorsion de fonds***

De nombreuses entreprises sont prises en otage par des hackers qui désactivent des fonctionnalités informatiques pour obtenir une rançon

Scénario Stress Test Accumulation: Frénésie d'extorsion

Les hackers, à l'aide d'un logiciel malveillant arrivent à créer un système sophistiqué de cryptage des serveurs de PME. Ils attaquent un grand nombre d'entreprises, et exigent des paiements de rançon élevées, à une échelle jamais observée à ce jour.

*Source: Managing Cyber insurance accumulation risk, cambridge Center for risk Studies Risk Management Solutions (libre traduction*

### 5.4.2. Tableau de classification par secteur d'activité pour la gestion des risques de cumul cyber

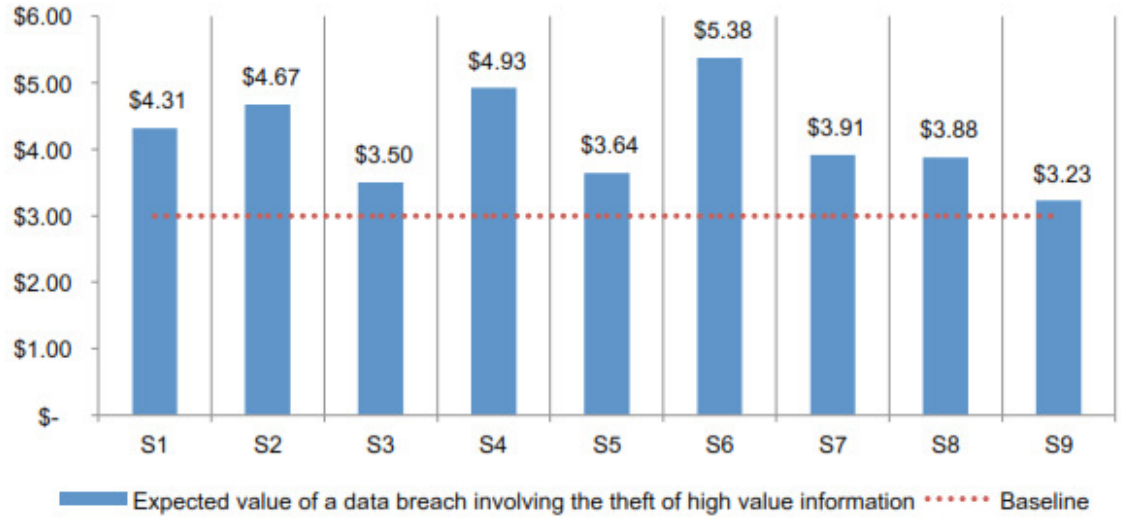
| V1.0 Code | Secteur d'activité | Description |
|---|---|---|
| 1 | **Informatique- IT** | |
| 1.1 | **IT - logiciels** | Les sociétés de logiciels impliquées dans la conception, le développement, la documentation et la publication de logiciels informatiques |
| 1.2 | **IT – materiel informatique** | Les entreprises impliquées dans la fabrication et / ou l'assemblage d'ordinateurs (ordinateurs centraux, les ordinateurs personnels, postes de travail, ordinateurs portables et serveurs informatiques) et d'équipements périphériques (par exemple les périphériques de stockage, imprimantes, écrans, etc.) |
| 1.3 | **IT - Services** | Les sociétés fournissant des services d'hébergement ou de traitement de données (dont Cloud et les services de diffusion en continu « streaming »); publication sur Internet et le contenu de la diffusion (dont médias sociaux); portails de recherche sur Internet; services liés à la conception de systèmes informatiques, la gestion des installations informatiques, services de programmation informatique, et de matériel informatique ou de conseil en logiciels. |
| 2 | **Commerce de détail** | Les détaillants pour le grand public, les vendeurs de biens et services à la fois dans les magasins de vente au détail et en ligne, des grossistes et des distributeurs |
| 3 | **Services financiers** | |
| 3.1 | **Finance - Banques** | Les entreprises exerçant une activité de banque commerciale, les institutions d'épargne, coopératives de crédit, banques émettrices de carte de crédit, financement des ventes, sociétés et courtiers de prêts hypothécaires, traitement des transactions financières, les activités de réserve et compensation, et les banques centrales. |
| 3.2 | **Finance - Assurance** | Les compagnies d'assurance directe, compagnies de réassurance, et les organismes d'assurance et de courtage. |
| 3.3 | **Finance – Gestion de portefeuilles** | Les banques d'investissement, les sociétés de négoce de valeurs mobilières et de courtage, le négoce et le courtage de contrats de marchandises, bourse de valeurs mobilières et de marchandises, les clubs d'investissement et de capital-risque, gestion de portefeuille, conseils en placement et des fonds d'entités légales et fiducies |
| 4 | **Santé** | Les entreprises fournissant des biens et services pour traiter les patients par des soins curatifs, préventifs, de réadaptation ou palliatifs. |
| 5 | **Services Professionnels** | Professions fournissant des conseils et des services spécialisés. Certains services professionnels qui nécessitent de détenir une licence professionnelle comme les architectes, les auditeurs, les ingénieurs, les médecins et les avocats. |
| 6 | **Energie** | Les entreprises d'exploration, extraction et le développement des réserves de pétrole et de gaz, forage de gaz et pétrole, entreprises de fourniture d'électricité |
| 7 | **Télécommunications** | Les entreprises qui facilitent l'échange d'informations sur de grandes distances par des moyens électroniques. |
| 8 | **Services publics** | Le secteur des services publics comprend des entreprises d' électricité, de gaz et les entreprises d'eau et fournisseurs intégrés |
| 9 | **Tourisme & Hôtellerie** | Les entreprises qui fournissent des services pour le tourisme, voyage, hébergement, restauration et l'hôtellerie |
| 10 | **Industrie manufacturière** | Sociétés de fabrication ou traitement de marchandises, en particulier en grandes quantités et au moyen de machines |
| 11 | **Pharmacie** | L'industrie pharmaceutique développe, produit et commercialise des médicaments ou des produits pharmaceutiques pour être utilisés comme médicaments. Les compagnies pharmaceutiques peuvent opérer dans les médicaments génériques ou de marque et des dispositifs médicaux |
| 12 | **Défense / Fourniture militaire** | l'industrie de la Défense comprend l'industrie gouvernementale et commerciale impliquée dans la recherche, le développement, la production, et le service de matériel militaire, des équipements et des installations |
| 13 | **Spectacle & Media** | Les entreprises qui fournissent des nouvelles, de l'information et du divertissement: radio, télévision, cinéma, théâtre |
| 14 | **Transport/Aviation/Spatial** | Les entreprises de transport de marchandises ou de clients. Le secteur des transports est constitué de compagnies aériennes, de chemins de fer et les entreprises de transport routier |
| 15 | **Autorité Publique; ONG; Organisations à but non lucratif** | Les agences gouvernementales nationales ou locales, les organisations non gouvernementales et à but non-lucratif |
| 16 | **Immobilier, Propriétés & Construction** | Les sociétés de gestion, de développement, et de transactions de biens comme des terrains, des bâtiments, ainsi que ses ressources naturelles telles que les cultures, les minéraux, ou de l'eau |
| 17 | **Education** | Les collèges et les universités, les écoles de quartier publiques et privées, les sociétés de prêts étudiants et de frais de scolarité |
| 18 | **Mines & Industries primaires** | Les entreprises présentes dans l'exploitation minière, l'extraction et le traitement des minerais d'extraction, le charbon, les minerais, les principales matières premières et des ressources naturelles. |
| 19 | **Alimentation & Agriculture** | Les sociétés de l'industrie agroalimentaire, y compris la production, la transformation, la distribution et la vente en gros |
| 20 | **Divers** | |

*Extrait du rapport : « Managing Cyber Insurance Accumulation Risk » du Centre d'études des risques de l'université de Cambridge, février 2016 (libre traduction)*

### 5.4.3. Estimation de couts pour une entreprise

**Figure 9. Expected value of data breach costs involving the loss or theft of 100,000 or more customer records for nine scenarios.** ($000,000 omitted)


**Figure 10. Expected value of data breach costs involving the theft of high value information for nine scenarios.** ($000,000 omitted)

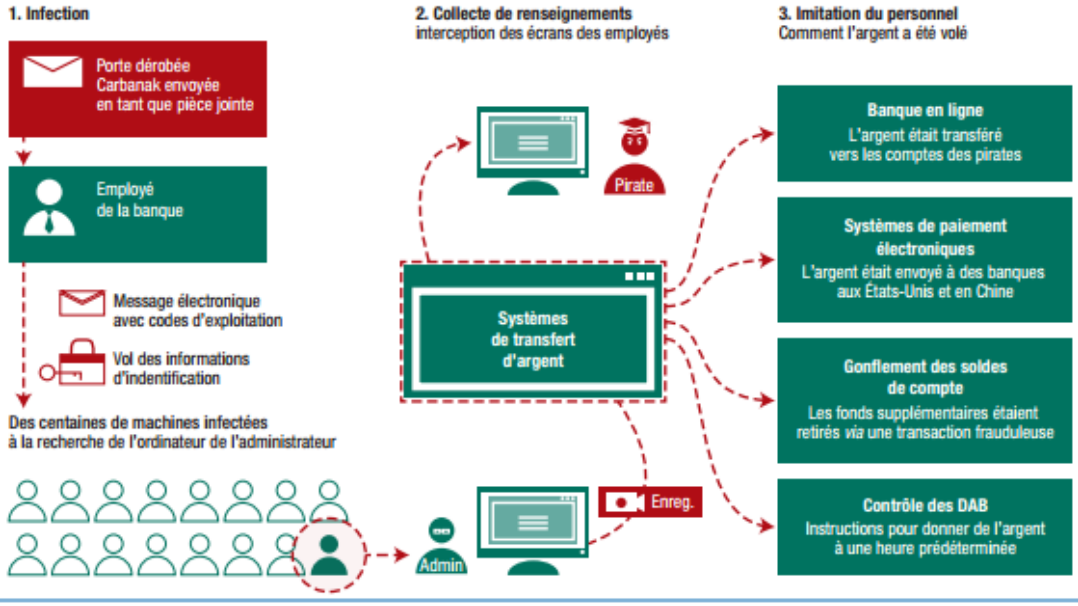



*Source: Data Breach: The Cloud Multiplier Effect, Ponemon Institute sponsored by Netskope, June 2014*

5.4.4. Exemple de sinistre APT (Advanced Persistent Threat) - Carnabak

Schéma 4

Le fonctionnement de l'attaque de Carbanak




*Source : Kaspersky Lab.*