LES DOSSIERS TECHNIQUES

Assurance des risques cyber

Guide Pratique

Janvier 2018

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

Synthèse managériale

Ce guide souhaite apporter un éclairage sur la couverture assurantielle des risques cyber.

Face aux nouvelles menaces dont la presse se fait régulièrement l'écho, les entreprises doivent se protéger. Mais doivent-elles forcément souscrire une police d'assurance spécifique ?

En cas de sinistre majeur comment interviendront les polices d'assurances traditionnelles déjà souscrites par les entreprises ?

Quelles sont leurs limites ? Quelle place doit-on accorder à la « cyber-assurance » ?

Il est impossible de répondre de façon générale à ces questions : toutes les entreprises n'ont pas les mêmes besoins, les contrats proposés par les assureurs ne couvrent pas tous le même périmètre, certaines exclusions peuvent limiter considérablement l'intérêt de ces nouvelles polices, etc.

Ce guide a été réalisé par des experts de la sécurité informatique, des courtiers, des assureurs et des consultants afin de vous aider à discerner ce dont vous avez réellement besoin pour votre entreprise.

Il vous permettra de poser les bonnes questions aux interlocuteurs qui ne manqueront pas de vous solliciter pour souscrire une nouvelle assurance.

Nous donnerons quelques clefs pour identifier les risques, décrirons les manques des contrats d'assurances traditionnels et indiquerons les limites des polices « cyber ». Nous expliquerons enfin le processus de souscription et la façon dont les sinistres seront pris en charge par l'assureur.

À travers trois exemples d'entreprises de tailles différentes, nous animerons le fil rouge de cet ouvrage afin de rendre la plus concrète possible chacune des parties.

L'article L. 122-5 de la propriété intellectuelle n'autorisant pas les représentations ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de l'ayant droit ou ayant cause, sauf exception stricte (« copies ou reproductions réalisées à partir d'une source licite et strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective », analyses et les courtes citations dans un but d'exemple et d'illustration, etc.), toute représentation ou reproduction, par quelque procédé que ce soit du présent document sans autorisation préalable du CLUSIF constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Table des matières

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

L'animateur et le co-animateur du groupe de travail :

Xavier	**LEPROUX**	*CHUBB*	Animateur
Dominique	**GUENAUX**	*SERMA*	Co-animateur

Les rédacteurs du document :

Etienne	**BUSNEL**	*BESSE*
Martin	**DESCAZEAUX**	*WAVESTONE*
Dominique	**GUENAUX**	*SERMA*
Jean-Paul	**JOANANY**	*GENERALI*
Jacques	**IZART**	*ASSURWEST*
Xavier	**LEPROUX**	*CHUBB*

Les participants aux groupes de travail :

Daniel	**BRESSAN**	*APPRENTIS AUTEUIL*
Laurent	**CHARREYRON**	*CXP*
Florence	**HANCZAKOWSKI**	*CLUSIF*

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture.

I. Introduction

I.1. Philosophie de la démarche CLUSIF

Depuis quelques années et grâce à des pionniers, le monde de l'assurance a su prendre la mesure du marché de la cyber-assurance, proposant une gamme de produits permettant d'assurer les biens immatériels des entreprises comme leur patrimoine informationnel, essence même de leurs activités métiers.

Si certains assureurs proposent aujourd'hui des contrats aux entreprises pour les garantir dans une certaine mesure contre les cyber-attaques, il n'en reste pas moins que la qualification d'un dossier de cyber-assurance reste complexe.

Dans ces conditions, quels sont les contextes bénéfiques à la souscription de ces contrats ? Comment procéder pour évaluer le risque ? Comment mesurer et analyser les clauses permettant d'obtenir un contrat adapté tout en gardant à l'esprit les couvertures d'assurance déjà en place.

Pour réussir à définir correctement ces besoins, il est nécessaire de prendre en compte les aspects techniques, humains, juridiques et financiers qui permettront de garantir efficacement son entreprise face aux cyber-attaques.

Ce guide pratique a été élaboré à partir du retour d'expérience d'experts, pour les experts, les RSSI, les risks manager, les DSI, les directeurs financiers, les juristes, les chefs d'entreprise, quelle que soit la taille de leur entreprise.

Ce document n'est pas un catalogue de solutions et d'offres d'assureurs, mais bien un guide pratique qui permet de mieux appréhender l'assurance cyber.

I.2. Fil conducteur : 3 exemples

Un fil conducteur pour 3 profils d'entreprise permet de se projeter : une TPE, une PME, un grand groupe. Au cours du document, des encarts décrivant ces profils viendront étayer et illustrer les propos. Pour en faciliter la lecture, un code couleur a été adopté pour chaque profil.

Fil Rouge

Les trois exemples suivants sont développés et analysés au chapitre VI.

Société SINIALE

La société SINIALE est une TPE de 10 employés, spécialisée dans la fabrication de panneaux signalétiques et qui réalise 1,1 millions d'euros de chiffre d'affaires. Elle dispose d'un atelier équipé de diverses machines-outils à commande numérique dont une est dédiée à la découpe au laser de pièces métalliques.

Mr DAFIX, comptable de la société fait également office de responsable informatique et s'assure que tous les ordinateurs fonctionnent en réseau. Il fait parfois appel à la société locale CALLME dédiée à la maintenance du parc informatique avec laquelle un accord cadre a été mis en place.

La société a été victime d'un virus de type Cryptolocker dont la particularité est de chiffrer une partie du disque dur d'un PC utilisé en production.

Société BRIDAL

Le groupe agro-alimentaire BRIDAL compte 1200 collaborateurs pour un chiffre d'affaires d'1 milliard d'euros. Spécialisé dans les légumes frais en sachet et les plats cuisinés, le groupe vend ses produits à tous les acteurs de la grande distribution. La promotion des produits et le service consommateurs sont fait majoritairement par l'intermédiaire de sites et d'outils Web très répandus. L'exploitation informatique du groupe est internalisée et centralisée sur le site du Mans et est répliquée en temps réel avec le site secondaire de Chartres.

A la suite de l'imprudence d'un employé, un virus de type Cheval de Troie est installé sur un poste de travail et a pour conséquence d'affecter le fonctionnement de la plateforme logistique pendant plusieurs jours.

Société BATUR

La société BATUR est spécialisée dans le distribution en quincaillerie industrielle. Elle réalise 100 millions d'euros de chiffre d'affaires et emploie 150 collaborateurs, répartis aux deux tiers à la gestion du magasin destiné aux professionnels et à la vente en ligne pour les particuliers, et pour le dernier tiers à la gestion de la chaîne logistique pour assurer notamment les expéditions et la réception de marchandises.

Le site Web de vente en ligne a été piraté, des données personnelles des clients ont fuité et des malversations à la carte bancaire ont été commises.

I.3. Enjeux du cyber-risque

Bien que largement répandu aujourd'hui en France et dans le monde, le terme de cyber-risque n'a pas été défini officiellement. On trouve un certain nombre de définitions mais elles divergent sur de nombreux points et sont parfois contradictoires. Cependant, un plus petit dénominateur commun semble partagé : le cyber-risque correspond, *a minima*, à **l'ensemble des risques liés à la malveillance externe ou interne pouvant porter atteinte à un système d'information (SI)**. Dans son acception la plus large, le cyber-risque inclut également l'erreur humaine, les pannes ou encore le détournement de fonds via le SI.

Le cyber-risque est aujourd'hui sur le devant de la scène pour une raison simple : la menace explose. Une étude récente relate que le nombre de cyber-attaques recensées a progressé de 51% en France en 2015 et de 38 % dans le monde[1]. Cette augmentation a été constatée sur le terrain par les sociétés spécialisées en sécurité informatique. Cette recrudescence peut notamment s'expliquer par des gains de plus en plus importants pour les attaquants, des cibles nombreuses et souvent insuffisamment protégées, une expertise accessible et une probabilité faible d'être identifiée. Du côté des entreprises, les impacts sont majeurs, et pas uniquement sur le système d'information : une cyber-attaque peut avoir de réels impacts opérationnels, comme en attestent les attaques évoquées quotidiennement dans la presse.

Face à ces menaces, les pouvoirs publics se sont emparés du sujet : la Loi de Programmation Militaire a été votée, la responsabilité du chef d'entreprise a été alourdie, le règlement européen pour la protection des données personnelles (RGPD[2]) entrera en vigueur en 2018...

[1] *The Global State of Information Security Survey 2016 – Price Waterhouse Cooper*
[2] https://www.cnil.fr/fr/reglement-europeen-protection-donnees

I.4. Comment traiter le cyber-risque ?

Traiter le cyber-risque commence par l'identifier et l'analyser. Comme évoqué dans le chapitre III, une analyse préalable du cyber-risque, qualitative et quantitative, est indispensable au bon traitement du risque. Une fois cette étape réalisée, plusieurs actions peuvent s'envisager : déployer de nouvelles mesures de protection, s'organiser pour gérer une crise cyber et éventuellement transférer le risque résiduel à l'assurance.

I.5. La cyber-assurance dans le monde

Lorsque l'on compare les Etats-Unis et l'Europe, les polices cyber ont suivi ces dernières années des trajectoires assez différentes. Chez nous, les garanties prenant en charge les sinistres informatiques d'origine immatérielle sont apparues au début des années 90, en ne proposant que des garanties de type 'dommages' (i.e. pertes d'exploitation à la suite d'attaque virale) ; ce n'est que depuis quelques années qu'une police cyber à part entière (dommages + responsabilité civile) est apparue en France et dans les autres pays limitrophes.

Aux Etats-Unis, le développement des polices cyber avait pris son essor dès 2003, avec l'introduction de la '*California Security Breach Information Act*' qui rendait obligatoire pour les sociétés de notifier leurs clients en cas de fuite de données personnelles. La grande majorité des autres Etats d'Amérique imposent aujourd'hui cette obligation, qui ne s'appliquera aux sociétés européennes qu'en mai 2018. Pour mémoire, le secteur Télécom est concerné par cette obligation depuis 2011.

Il reste que l'on a aujourd'hui encore deux approches différentes en matière d'assurance : l'approche anglo-saxonne (« *privacy* »), qui va focaliser sur des garanties de type responsabilité civile/frais et dépenses à la suite d'atteinte à la confidentialité des données, et l'approche européenne, qui offre en général des garanties beaucoup plus larges en intégrant, en plus de la responsabilité civile, des couvertures dommages.

I.6. L'assurance cyber concerne-t-elle tous les secteurs d'activité ?

Pour une entreprise, s'interroger sur la nécessité ou non de souscrire une assurance cyber revient à s'interroger sur son niveau de dépendance vis-à-vis de l'outil informatique et des conséquences qu'aurait une atteinte (disponibilité, confidentialité, intégrité) de celui-ci sur son activité.

Cette question, bon nombre de sociétés se la sont déjà posée, en particulier lorsqu'elles sont contraintes par leurs obligations réglementaires entre autres à disposer d'un plan de continuité d'activité (PCA) ou de mettre en œuvre des dispositifs permettant de garantir l'intégrité et la confidentialité de leurs actifs. C'est notamment le cas pour les grandes entreprises du secteur financier (Banques,

Assurances, etc.) ou pour celles dont l'arrêt ou la dégradation des activités pourrait entraîner des atteintes à l'ordre public voire à la sûreté de l'État (Défense, Energie, Transports, Alimentation, etc.).

Néanmoins, même sans contraintes légales, il est de la responsabilité des dirigeants de s'assurer que leurs entreprises soient en capacité de se « remettre » d'un sinistre grave. L'assistance dont ils pourraient bénéficier au titre des garanties d'un contrat d'assurance fait partie des solutions qui sont à leur disposition. En cas de sinistres « classiques » (inondations, incendies, vols, dégradations, etc.), l'évidence d'une assurance pour couvrir ces risques ne fait pas débat, alors pourquoi en serait-il autrement pour les cyber-risques ?

A l'ère numérique, peu d'entreprises (ou activités) peuvent encore se passer de l'informatique, les quelques questions suivantes pourraient convaincre ceux qui en doutent encore :

- Votre entreprise a-t-elle besoin de systèmes informatiques (ordinateurs, réseaux de communications, applications, données, sites web) pour ses activités ?
- Pouvez-vous envisager de perdre votre base clients ?
- Pourriez-vous envisager de ne plus accéder à votre messagerie électronique ?
- Un recensement de tous les moyens informatiques utilisés a-t-il déjà été réalisé ?
- Un recensement des évènements qui pourraient causer une indisponibilité des moyens informatiques a-t-il été mené ?
- Avez-vous toujours pu expliquer la raison d'une indisponibilité de vos systèmes d'information ?
- Pendant combien de temps votre entreprise pourrait-elle se passer des moyens informatiques ?
- Quelles seraient les conséquences financières de cette indisponibilité ?
- Quelles mesures sont déjà en place pour éviter cette indisponibilité ?
- Un plan pour la remise en service des moyens informatiques a-t-il été défini ?
- Un test de ce plan de remise en service a-t-il été réalisé ?
- Une estimation des coûts pour la remise en état des moyens informatiques a-t-elle été effectuée ?
- Quelles conséquences en termes de confiance et d'image vis-à-vis de vos clients ou actionnaires en cas de cyber sinistre matérialisé par une fuite d'information confidentielle : secret professionnel vis-à-vis des clients, R&D, projet d'opération sur le capital de la société (M&A)
- Etc.

II. Couverture de l'assurance cyber

II.1. Rappel sur les polices d'assurance existantes

Pour comprendre ce que couvre une police cyber, il faut repartir des polices existantes afin d'examiner leurs limites et voir ce que peut apporter une police cyber. Le tableau ci-dessous en donne une vision synthétique :

<table>
<tr><th></th><th>Conditions de déclenchement</th><th>Indemnisations possibles</th><th>Couverture en cas de sinistre sur le SI</th><th>Limites pour le système d'information</th></tr>
<tr><td rowspan="3">Police Dommage aux Biens</td><td rowspan="3">Pas d'indemnisation sans dommage matériel (bris, destruction,…)</td><td>Indemnisation des dommages matériels</td><td rowspan="3">Frais de reconstitution de données/systèmes</td><td>Pas d'indemnisation en l'absence de dommage matériel</td></tr>
<tr><td>Pertes d'exploitation et frais supplémentaires d'exploitation après un dommage matériel</td><td>Limites de garanties souvent très insuffisantes pour couvrir la reconstruction de données et/ou de systèmes</td></tr>
<tr><td>Frais et pertes consécutifs à un dommage matériel</td><td>Exclusion du virus informatique et de l'indisponibilité pour l'assuré d'accéder à ses données</td></tr>
<tr><td>Police Responsabilité Civile Générale (RC)</td><td rowspan="2">Garantie mise en œuvre sous réserve d'un réclamation d'un tiers, d'un préjudice subi par le tiers et d'une faute de l'Assuré</td><td>Dommages corporels

Dommages matériels

Dommages immatériels consécutifs à un dommage matériel ou corporel</td><td>Indemnisation du tiers si pas d'exclusion virus</td><td rowspan="2">Exclusion fréquente de tout dommage causé par un virus

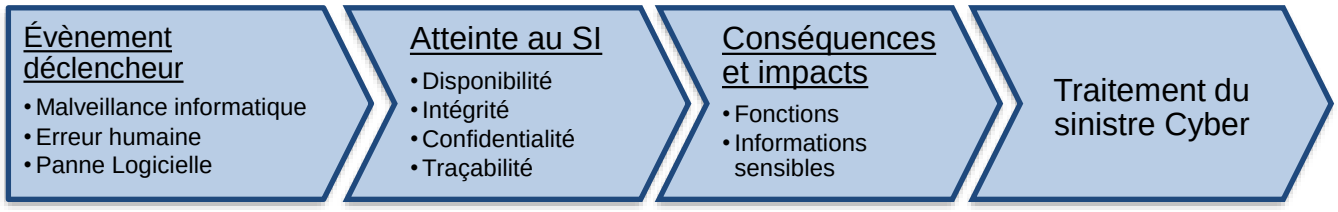
Dans le cas, d'une attaque informatique, il peut être compliqué de démontrer la faute de l'Assuré

Beaucoup d'assureurs considèrent que la police RC n'a pas vocation à couvrir les conséquences d'un risque Cyber mais les activités de l'entreprise</td></tr>
<tr><td>Police Responsabilité après livraison /après travaux</td><td>Extension aux frais de retrait et frais de dépose /repose pour les produits vendus ou les prestations de services réalisées</td><td>Extension aux frais de retrait et frais de dépose /repose pour les produits vendus</td></tr>
</table>

	Conditions de déclenchement	Indemnisations possibles	Couverture en cas de sinistre sur le SI	Limites pour le système d'information
Police Fraude	Détournement d'actifs (valeurs ou biens)	Perte financière consécutive		
Police Kidnapping et Rançon	Demande de rançon avec possibilités de pertes financières	Montant de la rançon Frais de négociation	Possibilité de prendre en charge le montant de la rançon pour menace contre le SI de l'assuré	

II.2. La couverture d'une police cyber

D'une façon générale, un sinistre cyber peut être représenté comme la combinaison d'un évènement déclencheur, d'une atteinte à un système d'information (Disponibilité, Intégrité, Confidentialité, Traçabilité/imputabilité) et des conséquences sur l'assuré du fait de la sensibilité des fonctions remplies et des données traitées par le système d'information touché.



L'objectif d'une assurance cyber consiste à couvrir les conséquences financières du sinistre, qui seraient liées à :

- des dommages subis par l'assuré (y compris des pertes et frais financiers induits par le sinistre) ;
- des réclamations à la suite de dommages subis par un(des) tiers consécutif(s) au sinistre.

En matière d'indemnisation, l'assurance cyber suit le même principe indemnitaire que pour les autres assurances : l'assuré doit démontrer à l'assureur qu'il a subi un préjudice réel et surtout chiffrable. Ainsi, le temps passé par les équipes internes à

gérer un sinistre sera difficilement indemnisable, de même qu'un vol de données de R&D.

En complément, l'assurance cyber peut également aider à :

- mettre à disposition de l'assuré des compétences en gestion de crise, en communication, conseils juridiques, ainsi qu'une expertise technique en investigation et reconstruction de tout ou partie de son SI ;
- faire de la prévention en proposant des revues régulières de la sécurité, des améliorations, des plans d'actions.

D'une façon générale, une des difficultés de la souscription d'une police cyber consiste à évaluer la cohérence avec le reste des couvertures assurantielles. Il s'agit de ne pas laisser de trous de couverture mais également de ne pas couvrir plusieurs fois le même risque. Ces articulations entre la police cyber et les autres polices « classiques » (dommage aux biens, responsabilité civile, fraude, rançon, …) sont un des points d'attention majeurs à prendre en compte lors de la souscription.

II.2.1. Cause (Événement déclencheur)

L'objectif de base d'une couverture cyber consiste à garantir les conséquences d'une attaque malveillante sur les systèmes d'information. On entend par « attaque malveillante » le fait qu'elle soit menée par un acteur impactant (directement ou indirectement) l'entreprise à travers l'utilisation qu'elle a de son système d'information. Cette police doit donc couvrir notamment :

- les attaques en disponibilité (DoS, DDoS, malware, …) ;
- l'atteinte à la confidentialité de données personnelles, médicales, confidentielles, etc., gérées ou détenues par l'assuré ;
- la modification non sollicitée d'un site web (défiguration ou défacement) ;

La garantie devra également s'appliquer dans les cas suivants :

- les intrusions directement subies par l'assuré ou subis par les tiers du fait de la compromission des SI de l'assuré ;
- l'utilisation illégitime du SI de l'assuré.

Certaines polices distinguent une attaque ciblée sur l'assuré d'une attaque plus globale qui le toucherait « par hasard ».

Lors d'un sinistre, cette distinction n'est pas simple à faire sur la base des « preuves » techniques et le risque est grand d'entrer dans des discussions sans fins entre l'assuré, les experts, l'assureur…

Par extension, il est envisageable de faire couvrir par une police cyber des évènements déclencheurs qui ont potentiellement les mêmes conséquences sur les systèmes d'information : l'erreur humaine, la panne logicielle et la malveillance interne.

II.2.2. Périmètre ou cible

Le périmètre sur lequel se produit l'évènement déclencheur doit pouvoir intégrer l'ensemble des briques du système d'information. Naturellement, cela inclut les matériels, logiciels et données qui se trouvent sur les sites physiques de l'assuré mais cela doit aller bien au-delà. Il faut effectivement intégrer l'évolution des SI et les nouveaux services offerts : les fonctions et données hébergées dans le Cloud ou sur des environnements externalisés, quel que soit leur niveau d'intégration (Software [SaaS], Plateforme [PaaS], Infrastructure [IaaS]). Y intégrer également les matériels, logiciels, fonctions et données hébergés ou confiés à un tiers. Les composants mobiles (qu'ils soient propriété de l'entreprise ou de ses salariés – BYOD) sont également un périmètre à couvrir tant ils contiennent potentiellement des données sensibles et concourent de plus en plus à l'efficacité de l'entreprise.

On peut de ce fait étendre ce périmètre bien au-delà de l'implantation physique de l'entreprise : la communication à travers les réseaux sociaux fait également appel à des briques de systèmes d'information qu'il convient la plupart du temps d'intégrer dans le périmètre garanti.

Il apparaît clairement que la notion de système d'information doit être prise dans son sens le plus large.

Le périmètre peut également être étendu à des fournisseurs (dans son ensemble, pas uniquement des fournisseurs du SI), des clients, des partenaires, etc. qui subiraient des sinistres couverts dans la police et qui entraîneraient des conséquences financières pour l'entreprise assurée. On parle alors de « carence fournisseur ».

II.2.3. Conséquences et impacts

Les conséquences d'un sinistre cyber peuvent être de différentes natures, comme évoqué précédemment. L'assurance prend généralement en compte :

- les frais de gestion de crise (communication, avocats, etc.) ;
- les frais d'investigation (consultants, experts techniques, etc.) ;
- les frais de remédiation/reconstruction et les frais supplémentaires qui ont dû être engagés par l'assuré suite au sinistre (ajout d'un call-center, de matériels, de services externalisés pour compenser voire limiter les effets du sinistre) ;
- les frais de reconstitution de données perdues ;
- les frais de notification (si obligatoire) ;
- le montant d'une rançon ;

- dans une certaine mesure, les pénalités contractuelles avec des clients/partenaires ;
- la facturation indue ;
- les pertes d'exploitation consécutives à un sinistre cyber.
  Celles-ci sont constituées par la perte de marge brute, déterminée en appliquant le taux de marge brute à la différence entre le chiffre d'affaires qui aurait été réalisé pendant la période d'indemnisation en l'absence de sinistre, et le chiffre d'affaires effectivement réalisé pendant cette même période ;
- les préjudices subis par des tiers lorsque ceux-ci portent réclamation.

Un point d'attention concerne les frais d'amélioration que les assureurs ont plus de mal à accepter. Cependant, dans un certain nombre de cas, remettre en fonction un système à l'identique de ce qu'il était peut-être impossible, ou plus compliqué et donc plus onéreux que de remettre un système à neuf. Ce point doit faire l'objet d'un échange avec l'assureur pour vérifier la bonne compréhension réciproque.

En synthèse, le tableau ci-après représente les différents éléments décrits précédemment en indiquant (à titre indicatif à la date de publication de ce document), ceux que l'on trouve de façon standard, ceux qu'il est possible de trouver (éventuellement sous forme d'option) et ceux qui sont rares voire inexistants dans les contrats d'assurance cyber « classiques » :

<table>
<tr><th></th><th colspan="2">Standard</th><th colspan="2">Possible mais souvent optionnel</th><th>Rare</th></tr>
<tr><td rowspan="4">Evénement déclecheur</td><td colspan="2" rowspan="4">Attaque externe</td><td colspan="2">Erreur humaine</td><td>Dommage matériel (incendie, bris, vol, …)</td></tr>
<tr><td colspan="2">Panne Logicielle</td><td>Menace d'attaque</td></tr>
<tr><td colspan="2">Cyber-terrorisme</td><td rowspan="2">Erreur de programmation</td></tr>
<tr><td colspan="2">Acte de malveillance interne</td></tr>
<tr><td>Périmètre</td><td>SI Propriété de l'assuré</td><td>SI utilisé par l'assuré, opéré par un fournisseur (Cloud, SaaS, …)</td><td colspan="2">SI de fournisseurs / clients / …</td><td>SI Tiers (réseaux sociaux, Sites Web)</td></tr>
<tr><td rowspan="5">Garanties</td><td>Frais de remédiation / reconstruction et les frais supplémentaires qui ont dû être engagés suite au sinistre</td><td>Perte d'exploitation et frais supplémentaires</td><td>Pénalités contractuelles</td><td>Frais d'amélioration</td><td>Facturations indues</td></tr>
<tr><td>Frais d'investigation (consultants, experts techniques, …)</td><td>Indemnisation en responsabilité civile :

- Atteinte à la vie privée
- Atteinte à la sécurisation des réseaux
- Atteinte médiatique</td><td>Rançon</td><td>Sanctions réglementaires / administratives</td><td>Produits non conformes</td></tr>
<tr><td>Frais de notification</td><td>Frais de gestion de crise (communication, avocats, …)</td><td>Fraude par surfacturation de services informatiques</td><td>Pénalités PCI-DSS</td><td>Impacts spécifiques</td></tr>
<tr><td rowspan="2">Service d'aide technique à la gestion des incidents</td><td rowspan="2"></td><td colspan="2" rowspan="2">Carence Fournisseurs / Clients / …</td><td>Indemnisation en responsabilité civile sur dommages corporels</td></tr>
<tr><td>Indemnisation en responsabilité civile professionnelle</td></tr>
</table>

On trouvera ci-après une illustration des frais engagés à la suite d'un sinistre cyber par chacune des trois entreprises de notre fil rouge.

Fil Rouge

Société SINIALE

Mr Dafix, Directeur fiancier, ne se doutait pas en ouvrant une piece jointe infectée dans son mail qu'il aurait à supporter:

- Des frais de reconstitution des données pour son poste et celui du disque réseau.
- Des coûts liés à la sous traitance d'une partie de la production suite à l'indisponibilité de la machine à découpe laser.

Société BATUR

Lorsque le site de vente en ligne a dû être arrêté après les fuites de données clients, la société a fait face aux dépenses suivantes :

- Frais d'investigation pour comprendre ce qui s'est réellement passé
- Frais de notification aux clients (mailing courrier)
- Frais de réparation et de mise à jour des logiciels
- Frais associés au rétablissement de son image de marque.

Société BRIDAL

L'indisponibilité des logiciels de la plateforme logistique a été provoquée à distance par un pirate. En conséquences les expéditions et la réception des marchandises sont quasiment arrêtées pendant 5 jours.

Les dépenses liées à cet incident s'élèvent à prés de 2,5 millions d'euros, et concernent notamment les frais suivants :

- Frais d'investigation par une équipe d'experts
- Frais de remédiation des environnements de production informatique
- Frais de logistique exceptionnels pour éviter de perdre les produits périssables
- Pénalités financières imposées par les clients (grande distribution)

II.2.4. Limites de garanties

Plusieurs caractéristiques vont s'appliquer à tout ou partie des garanties.

II.2.4.a. Limite contractuelle d'indemnisation

La première limite concerne le montant maximal que l'assureur s'engage à verser à l'assuré au titre des indemnisations : on parle ici de Limite Contractuelle d'Indemnisation (LCI). Ce montant peut être global pour l'ensemble des garanties ou spécifique à chaque garantie.

Cette limite peut être accompagnée de sous-limite(s) sur certaines garanties permettant à l'assureur de mieux maîtriser son risque de cumul.

Historiquement les polices cyber n'accordaient pas le plein de la garantie de couverture sur le « virus informatique » ou l'erreur humaine par exemple. Aujourd'hui, il reste un certain nombre de sous-limites, principalement : les frais d'urgence, les sanctions administratives, les pénalités PCI-DSS, et comme vu précédemment, la carence fournisseur dans certains cas.

Concernant l'indemnisation, il convient également de préciser si la limite ou les sous-limites sont valables pour un sinistre (la limite est reconstituée à chaque nouveau sinistre) ou en cumul sur une période (i.e. par an).

II.2.4.b. Franchise

La franchise est également une caractéristique liée à l'indemnisation. Elle peut être définie par garantie ou au global pour chaque sinistre. Il s'agit du montant qui reste à la charge de l'assuré après indemnisation par l'assureur. L'objectif est notamment d'éviter de multiplier les sinistres pour concentrer cette indemnisation sur les sinistres plus importants. Cela permet également de continuer à responsabiliser l'assuré dans la prise en compte de sa sécurité et des investissements nécessaires sans se reposer de façon déraisonnable sur la police d'assurance.

De même, le calcul peut être par sinistre ou par période (i.e. par an).

Cette franchise peut prendre différentes formes : montant fixe, durée en heure, pourcentage de l'indemnisation, définition d'un minimum et d'un maximum.

II.2.4.c. Exclusions

Comme toute police d'assurance, les textes de garantie cyber imposent à l'assuré des exclusions 'générales' comme par exemples : les conséquences d'un acte de terrorisme commis en dehors du territoire français, d'une guerre civile ou étrangère,

d'une grève ou émeute populaire, de tout ce qui touche de près ou de loin au nucléaire, la saisie ou confiscation des données par un état, les amendes administratives, pénales, etc.

Examinons maintenant ce qui est propre à la police cyber :

- Pour la partie « dommages » : l'exclusion « terrorisme » est partiellement rachetée puisque le cyber terrorisme est habituellement couvert. En revanche, restent notamment exclus : les dommages matériels, les dommages corporels, l'utilisation volontaire de programmes illégaux ou sans droit d'utilisation, et parfois l'attaque informatique non ciblée.

  Trois cas particuliers sont à considérer :
  - *Carence fournisseur* : si les assureurs étendent en général la garantie cyber aux évènements pouvant se produire chez les prestataires informatiques de l'assuré, la carence de fournisseur (c'est-à-dire essentiellement les conséquences d'une interruption de la fourniture de courant électrique ou ressources Telecom) n'est pas accordée automatiquement et va plutôt faire l'objet d'une sous-limite dans la police ; Cette carence peut, le cas échéant, être étendue aux fournisseurs critiques de biens et de services de l'assuré.
  - *Erreur de programmation* : cette exclusion « historique » est maintenant partiellement rachetée chez certains assureurs ; pour autant que le programme a fait l'objet d'une recette et fonctionné sans erreur pendant une certaine période. À distinguer de l'erreur humaine dont les conséquences sont garanties historiquement par la police cyber.
  - *Fraude* : attention, le détournement de fonds ou de valeurs n'est pas garanti en standard par la police cyber, mais peut l'être en option.

- Pour la partie responsabilité civile : les principales exclusions concernent les réclamations relatives à un dommage matériel ou corporel, l'exécution ou la fourniture de produits ou services (couverts par la responsabilité civile professionnelle), ou encore la contrefaçon ou exploitation abusive de brevets.

II.2.5. Clause de non-renonciation à recours

Il s'agit d'un point contractuel important pour l'assureur qui souhaite, une fois l'indemnité versée, être toujours en mesure de récupérer tout ou partie de cette indemnité à travers le mécanisme de « recours subrogatoire ».

Comment se traduit sur un plan contractuel cette problématique ?

- Garantie « dommages » : à l'origine, la police « tous risques informatiques » stipulait que l'assuré s'engageait à ne renoncer à aucune des garanties accordées par le fabricant du matériel, du prestataire informatique, de l'éditeur de logiciels, etc., ni à abandonner l'exercice d'aucun recours contre tous

responsables ou garants. Vu la multiplicité des intervenants aujourd'hui dans le domaine informatique et le développement de l'externalisation (services « cloud » par exemple), le maintien d'une telle clause viendrait à vider le contrat d'une grande partie de sa substance. De ce fait, beaucoup de compagnies acceptent désormais la formulation suivante : « *l'assureur accepte les renonciations à recours consenties par l'assuré lorsque ces renonciations sont réciproques, ou qu'elles sont usuelles dans la profession* ».

- Garantie « Responsabilité Civile » : la police cyber suit la même logique en excluant seulement de la garantie « *les conséquences pécuniaires d'engagements contractuels ayant pour objet d'aggraver la responsabilité de l'assuré au-delà du Droit commun et des usages de la profession* ».

Étant donné les enjeux financiers potentiels, l'assureur peut être amené à réclamer les contrats de prestation informatiques, afin de connaître en particulier le montant de la responsabilité contractuelle imposée (la plupart du temps) par le prestataire. Cette somme représentera en effet le montant maximum que l'assureur pourra récupérer en étant subrogé dans les droits de l'assuré, après versement de l'indemnité à ce dernier.

II.2.6. Garanties déjà accordées par les polices Responsabilité civile ou Dommages classiques ?

Une fois l'analyse de risque effectuée au sein de sa société, qui a pu faire ressortir un certain nombre de vulnérabilités associées à un coût financier potentiel, il importe d'examiner ses polices « Responsabilité Civile » et « Dommages » ; l'objectif est ici de voir dans quelles mesures les évènements de type cyber sont garantis ou non. On regardera en particulier les points suivants :

- Police « Dommages » : pour que puisse jouer la garantie, il faut bien entendu qu'il y ait un « dommage matériel » direct impactant les équipements (bris de machines, incendie, etc.) de l'assuré ou ceux de ses prestataires si la garantie « carence de fournisseurs » a été souscrite. La police « dommages » impose parfois une exclusion « virus » ou « acte de malveillance informatique ». Dans le meilleur des cas, l'assureur accepte de racheter partiellement cette exclusion, en ne remboursant toutefois que les coûts de reconstitution de données, mais en aucun cas les frais supplémentaires ou autres pertes d'exploitation. Ceci tendrait à expliquer la raison pour laquelle un nombre croissant de sociétés industrielles mettent en place une police cyber.
- Police « Responsabilité Civile » : dans de nombreux cas, cette police n'exclut pas les deux principaux évènements cyber qui sont : d'une part, la « transmission de virus à un tiers », et, d'autre part, les « conséquences d'une atteinte à la confidentialité des données confidentielles » (en particulier les données confiées à l'assuré par un tiers). Ces garanties sont dites

« silencieuses », dans la mesure où, bien que non exclues, elles ne constituent pas le cœur des couvertures « Responsabilité Civile ». En revanche, ces garanties sont souvent fortement sous-limitées dans le cadre des « dommages immatériels non consécutifs » (à un dommage matériel ou corporel).

Quoi qu'il en soit, on estime que dans les années qui viennent, les assureurs de responsabilité civile vont regarder de plus près leurs expositions cyber et, le cas échéant, sous-limiter, voire exclure, les évènements décrits précédemment.

II.2.7. Assurabilité de la cyber-extorsion et des sanctions administratives

Les polices cyber peuvent proposer ou non la garantie concernant ces deux postes :

- Cyber-extorsion : certains assureurs ne garantissent que les frais exposés pour mettre fin à la tentative de cyber-extorsion (intervention d'un consultant spécialisé), s'interdisant de rembourser en cas de paiement la rançon en elle-même ; ils justifient leur position sur la base notamment de l'article 6 du code Civil qui stipule « *qu'on ne peut déroger, par convention particulière, aux lois qui intéressent l'ordre public et les bonnes mœurs* ». Un contre-pied à cet argument peut être fait lorsque l'on constate qu'une grande partie de ces attaques par logiciel rançon sont faites depuis l'étranger.

- Sanctions administratives prononcées par les Autorités : il s'agit d'un point très important à examiner dans la mesure où le nouveau règlement européen pour la protection des données personnelles (RGPD) va imposer, dès mai 2018 et en cas de non-respect de la règlementation, des sanctions administratives pouvant aller jusqu'à 4% du chiffre d'affaires monde des entreprises. Là encore, la position des assureurs n'est pas homogène, ceux qui ont choisi de ne pas prendre en compte cette situation mettent en avant l'article 1113-1 du Code des Assurances (l'assurance d'un risque suppose que sa survenance respecte un caractère aléatoire) ; on considère ici qu'il n'y a plus de caractère aléatoire puisque l'amende ou sanction administrative en question est consécutive à une faute ou à une négligence du management de l'entreprise

Dans les deux cas et afin de pallier d'éventuelles difficultés d'interprétation, les polices cyber indiquent souvent que ces faits sont indemnisables pour autant qu'ils soient bien « assurables » au sens de la règlementation en vigueur. En attendant une position claire, il est plus raisonnable de considérer que le montant d'une telle amende ne sera pas couvert par une police cyber.

III. Analyse préalable du risque

L'assurance cyber, comme toute assurance, est un outil de transfert de risque. La réflexion sur la pertinence de s'assurer doit donc s'inscrire dans une **approche globale d'analyse du risque cyber**.

Cette analyse, qui peut suivre les grands standards du marché tels qu'EBIOS[3] ou MEHARI[4], permettra dans un premier temps de mettre en exergue :

- les processus et biens essentiels de l'entreprise ;
- les menaces auxquelles l'entreprise est exposée ;
- ses vulnérabilités ;
- ses actifs impactés ;
- la liste des risques cyber auxquels elle est confrontée.

Le point de départ de ce travail devra naturellement porter sur la criticité des systèmes d'information de l'entreprise, que ces derniers soient externalisés ou non auprès d'un prestataire de services informatiques. Pour mesurer cette criticité, il peut être intéressant en première approche de se focaliser sur la disponibilité.

Pour ce faire il est possible d'utiliser comme indicateur, le DMIA (durée maximum d'interruption admissible). Pour un site de vente en ligne tourné vers le grand public, cette durée maximum est évidemment très courte, et une interruption d'une ou deux heures pourrait induire des pertes sérieuses (cas d'activités internet à très forte saisonnalité type ventes de fleurs en ligne). Il y a lieu de noter que cette analyse doit être menée métier par métier au sein de l'entreprise. Ainsi, si les activités d'approvisionnement, de stockage, ou de production ne tolèrent guère un arrêt prolongé des systèmes d'information, les métiers de la gestion, comptabilité ne seront la plupart du temps pas impactés de la même façon. Le bon sens tend à déterminer où se trouve le maillon le plus faible, ou goulot d'étranglement de l'entreprise.

Le second volet de cette analyse a trait aux données elles-mêmes. De la même façon, il existe un indicateur utile, le PDMA (perte de données maximale admissible) qui devrait déterminer le cycle de sauvegardes de l'entreprise. Ce PDMA peut être de quelques minutes dans certains secteurs très sensibles (transactions bancaires par exemple) ou, à l'opposé, de plusieurs jours, voire davantage dans une PME faiblement informatisée. Bien entendu, cet indicateur concerne les données plutôt d'exploitation, celles qui sont nécessaires au quotidien. Il peut s'agir également de données sensibles, type données personnelles, données financières, cartes

[3] **E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité

[4] **MÉ**thode **HA**rmonisée d'analyse des **Ri**sques, initialement développée par le CLUSIF

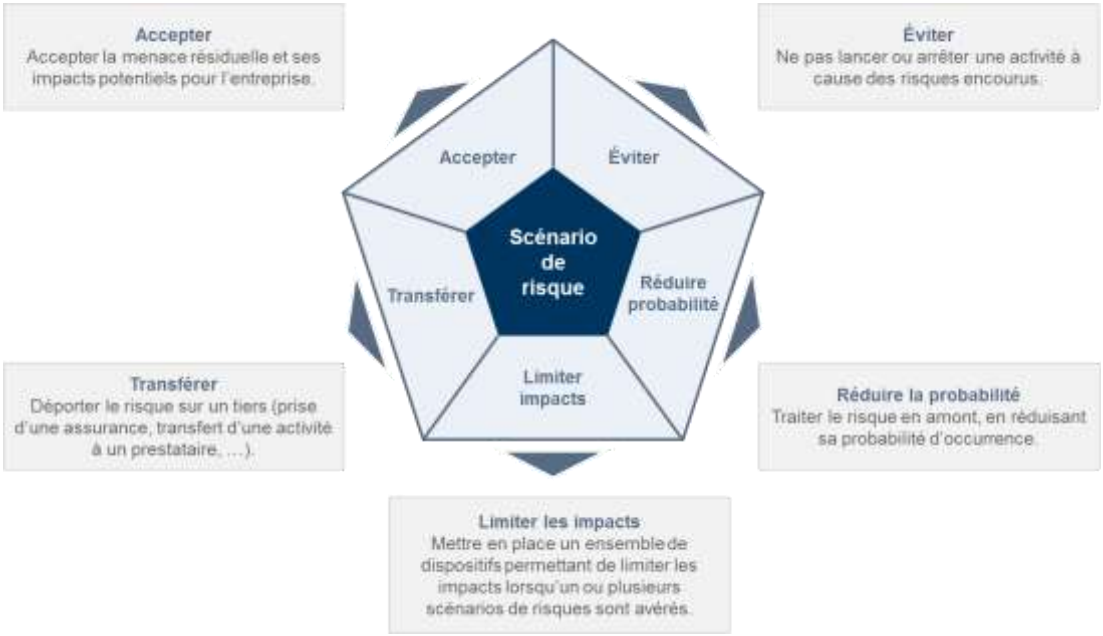
bancaires, etc. Le vol, la perte ou la fuite de données sensibles doit aujourd'hui être pris en compte de façon très sérieuse, d'autant plus désormais que le respect du RGPD s'impose à toutes les entreprises. L'analyse devra à ce sujet porter sur la façon dont sont gérées ces données (sont-elles stockées sur des serveurs dédiés, un chiffrement est-il mis en place ? Ces données sont-elles confiées à un ou plusieurs prestataires ? etc.)

Ensuite, afin de déterminer la criticité de ces risques, une analyse de leur probabilité d'occurrence et de leurs impacts (tous deux liés notamment aux mesures de protection mise en place) est réalisée.

Les impacts peuvent être quantifiés selon plusieurs critères (image, règlementaire, financier, etc.). Dans une approche assurantielle, l'analyse des impacts financiers, bien que souvent complexe à réaliser, est fortement recommandée afin d'avoir une première vision du montant de garantie pouvant être souscrit. Il peut être choisi de ne pas procéder à une analyse fine afin de souscrire rapidement, mais une analyse plus poussée, a minima du ou des scénarios de risques majeurs est recommandée par la suite. Pour ce faire, la démarche conseillée consiste à identifier l'ensemble des frais, directs et indirects, associés aux différents risques, et de les quantifier, sur la base :

- de frais connus par l'entreprise (perte d'exploitation, etc.) ;
- d'études (Ponemon, Gartner, etc.) donnant des abaques sur le sujet ;
- d'hypothèses prises par l'entreprise (intervention pendant X jours d'un expert à taux journalier de Y €, etc.) ;
- d'outils du marché proposé par certains courtiers / assureurs / prestataires de service ;
- d'accompagnement de la part de sociétés spécialisées.

Une fois ces risques quantifiés, leur traitement suit une démarche classique de gestion des risques : des contre-mesures sont identifiées, un plan d'action est réalisé, et la question du transfert du risque se pose.



Dans le cadre de la réflexion sur le transfert de ses risques, et donc de la pertinence de souscrire une assurance cyber, l'entreprise devra alors répondre aux questions suivantes :

- Suis-je en capacité d'assumer les impacts financiers de mes risques ?
- Si non, quelle proportion pourrais-je prendre à ma charge et, en conséquence, quelle proportion transférer ?
- Ai-je déjà une ou plusieurs assurances couvrant une partie de mes impacts financiers ? Si oui, à quelle hauteur ?
- Suis-je à même de traiter le risque en cas d'occurrence ? Ai-je les équipes et expertises adéquates ?
- Suis-je amené par mes clients à devoir produire une attestation d'assurance cyber ?
- En conclusion, est-ce que le fait de ne pas être assuré peut mettre en péril mon business ?

Il est à noter que dans le cas de petite structure, cette analyse peut être allégée. Pour autant, une réflexion sur son risque et son exposition doit être impérativement menée avant toute souscription.

En illustration de notre fil rouge, l'analyse préalable des risques serait la suivante.

Fil Rouge

Société SINIALE

Exemples de risque :

- Arrêt de la production suite à un rançongiciel
- Vol de données clients
- Modification des commandes clients entraînant des erreurs ou retards de livraison

Société BATUR

Exemples de risque :

- Indisponibilité du site de vente en ligne
- Vol de données cartes bancaires
- Vol de données clients
- Modification malveillante des prix entraînant une perte de marge commerciale

Société BRIDAL

Exemples de risque :

- Incapacité à acheminer les produits chez les clients
- Vol de données clients
- Interruption de la chaîne de production
- Infraction règlementaire grave suite à la perte de traçabilité des produits

IV. Souscription

IV.1. Préambule

Plusieurs raisons peuvent conduire une entreprise à initier un processus de souscription d'une assurance cyber :

- une analyse de risques menée en interne a recommandé que le risque résiduel soit transféré à un assureur (cf. Chapitre précédent) ;
- l'entreprise est soumise à des contraintes réglementaires, sectorielles ou à des demandes de ses clients lui demandant de souscrire une assurance de ce type ;
- sensibilisée aux cyber-risques par son assureur, ou par l'actualité, elle a adopté une démarche proactive et entamé une démarche intégrant le recours à un assureur pour s'en préserver ;
- etc.

Quelles que peuvent être ces raisons, elle va devoir, si elle n'a pas mené une analyse de risques, fournir à l'assureur, ou à l'intermédiaire d'assurances (courtier, agent général) les informations nécessaires à la détermination des couvertures du risque cyber correspondant le mieux à ses besoins.

IV.2. Les éléments à prendre en considération

L'assureur cherche à avoir une vue d'ensemble des pratiques de sécurité informatique de l'entreprise. Il évaluera son niveau de maturité, et appréciera si ses pratiques paraissent en adéquation avec ses enjeux financiers. À titre d'exemple, si une indisponibilité des systèmes conduit immédiatement à une perte de chiffre d'affaires, il sera capital pour l'assureur de vérifier l'existence ou non d'un plan de secours informatique.

Le plus souvent, ces informations sont communiquées à travers un questionnaire plus ou moins élaboré selon la taille de l'entreprise ou son secteur d'activité. Il reprend habituellement les points suivants :

- informations générales sur l'entreprise ;
- organisation et gouvernance de la sécurité informatique
- périmètre de l'étude ;
- criticité des systèmes d'information ;
- politique de sécurité informatique ;
- mesures de protection de l'information / contrôle d'accès ;
- gestion des sauvegardes ;

- protection des équipements informatiques ;
- exploitation réseaux / protection contre le risque d'intrusion

  Les réseaux de communications sont aujourd'hui indispensables à la conduite des activités d'une entreprise, mais en contrepartie ils peuvent être également le vecteur de nombreuses menaces. Ainsi pour une société de e-commerce, la disponibilité de son accès au réseau Internet est vitale, mais elle est de ce fait à la merci des attaques de type déni de service distribué (DDOS) qui ces dernières années ont réussi à provoquer le dysfonctionnement des plus grands acteurs du Net.
- plan de reprise d'activité / plan de secours informatique ;
- nature et volumétrie des données ;
- parmi les données qu'il est important d'identifier il faut retenir :
    - les données clients ;
    - les données relatives aux cartes de paiement ;
    - les données des collaborateurs ;
    - les données de santé ;
    - les données financières ;
    - les données stratégiques ;
    - les informations relatives à la propriété industrielle/intellectuelle ;
- mode de collecte de ces données ;
- politique de protection des données personnelles ;
- la gestion des sous-traitants et des services Cloud ;
- historique des incidents (indisponibilité des SI, atteinte à la confidentialité des données).

Un échange avec l'assureur pourra à réception du questionnaire avoir lieu si nécessité pour lui d'avoir confirmation de certains éléments, typiquement, que :

- la politique de sécurité informatique de la maison-mère s'applique à l'ensemble des filiales françaises ou à l'international ;
- les paiements par cartes bancaires sont bien externalisés chez un prestataire spécialisé ;
- il n'y a pas d'abandon de recours en cas de sinistre vis-à-vis du prestataire (hébergement serveurs, cloud, etc.) ;
- etc.

Pour confirmer la prise de garantie, certaines compagnies pourront demander une attestation de non-connaissance de litiges.

Suivant la taille du proposant et le montant de garantie envisagé, les assureurs n'exigent bien entendu pas le même niveau d'information.

On trouvera dans les exemples ci-dessous l'application de ces différentes modalités.

Fil Rouge

Société SINIALE

Vu l'activité à priori peu exposée aux risques cyber, le chiffre d'affaires modeste et la limite de garantie achetée (100k€), l'assureur a accepté de mettre en place la garantie sans poser de question relative à la sécurité informatique.

Société BATUR

Le proposant a rempli le questionnaire et l'assureur s'est particulièrement intéressé aux réponses portant sur la question et la sécurité concernant les activités de vente en ligne (10% aujourd'hui du CA de l'entreprise, activité en progression).

Société BRIDAL

Le courtier a proposé à l'assureur une visite d'évaluation en compagnie d'un ingénieur en sécurité informatique; durant cette visite, un focus a été fait sur les enjeux liés à une indisponibilité de l'ERP, et l'assureur a posé des questions concernant le plan de continuité d'activité mis en place par l'entreprise.

IV.3. Problématique de confidentialité

Les informations communiquées par la société en phase d'étude pour l'assurance cyber peuvent revêtir un caractère confidentiel. Il est donc pertinent de se poser la question de ce que deviennent ces informations et de quelle façon elles sont conservées par l'assureur.

Dans la pratique, plusieurs cas de figure peuvent se présenter, fonction la plupart du temps de la taille de l'entreprise :

- Sur le segment des TPE/PME-PMI réalisant jusqu'à quelques dizaines de millions d'euros de chiffre d'affaires, les assureurs peuvent dans certains cas se contenter de réponses à un nombre limité de questions « basiques » touchant la sécurité informatique (présence de logiciels anti-virus, mots de passes, sauvegardes au moins hebdomadaires, etc.) ;

  Il s'agit donc de règles de base en sécurité informatique qu'observent aujourd'hui une très grande majorité des entreprises. La confidentialité de ces informations n'est donc pas un enjeu.

- Pour les sociétés de taille plus importante, le questionnaire remis aux assureurs doit en effet faire l'objet d'un traitement assurant la confidentialité des informations y figurant ;
- Enfin, s'agissant de sociétés ou de groupes d'une taille importante, l'usage va vers l'organisation de réunions de souscription auxquelles sont conviés les assureurs du marché, moyennant la signature d'accords de confidentialité qui engagent donc clients et assureurs, en cas notamment de fuite ou d'atteinte à la confidentialité de ces mêmes données.

IV.4. Périmètre

Les sociétés ayant des filiales sont confrontées à un choix en matière de police cyber : centraliser le dispositif d'assurance ou laisser les filiales assurer leurs risques informatiques de façon autonome.

La politique de gestion des risques et d'achat, la taille et la culture du groupe, la situation géographique des filiales sont autant de paramètres qui vont conduire à centraliser la démarche assurance ou à déléguer aux filiales le soin de s'assurer.

Une bonne gestion des risques au niveau d'un groupe nécessite une vision globale et un reporting consolidé.

Cela peut s'obtenir de deux façons :

1) Une seule police pour tout le groupe

Quand la réglementation le permet c'est sans doute le plus efficace et le plus simple à mettre en place. Il sera judicieux de définir un cahier des charges précis pour couvrir l'ensemble des entités à partir d'une même police. C'est particulièrement opportun lorsque l'approche SI est harmonisée.
La cohérence du dispositif de prévention/protection/assurance serait renforcée si l'intervention des prestataires en cas de sinistre cyber était coordonnée et rémunérée par le même assureur sous la supervision d'un Risk Manager groupe. Cette solution garantit au dirigeant du groupe une parfaite maîtrise de l'efficacité de son programme d'assurance. Elle suppose que l'assureur choisi ait la capacité d'intervenir sur l'ensemble des pays concernés. On trouve ce type de solution pour les groupes

opérant uniquement au sein de l'Union européenne (dispositif LPS[5]). Le seul bémol est que dans ce type de programme les filiales n'ont pas d'interlocuteur local.

2) Une police maître et des polices locales

Dans certains pays il sera nécessaire de prévoir une police locale pour assurer le risque cyber.

Dans ce cas une lecture attentive des garanties souscrites est recommandée. Dans certains programmes une police « maître » peut être souscrite en France et se décliner dans les différents pays concernés à travers des polices locales. Dans ce cas la police « maître » suppléera le cas échéant en différence de conditions de garanties et différence de limites de couverture (DIC/DIL[6]) les polices locales qui seraient insuffisantes du fait d'une réglementation locale moins contraignante par exemple.

Il paraît dangereux en matière de cyber-assurance de laisser chaque filiale souscrire la police de son choix sans garantir l'ensemble au niveau d'une police « maître ». Une garantie non souscrite par une filiale ou une intervention non coordonnée d'un prestataire informatique au moment du sinistre pourrait être lourde de conséquence pour le groupe. C'est d'autant plus vrai lorsque les Systèmes d'Information sont connectés entre eux. Une chaîne n'est forte que par son maillon le plus faible.

Quel que soit le dispositif retenu (une seule police ou une police « maître » et des polices locales), il est important que le dirigeant puisse avoir une vision globale de la gestion de son risque.

IV.5. Contre quelles menaces veut-on se protéger ?

IV.5.1. Risques à couvrir

Les analyses de risques existantes identifient les actifs (dont les informations et données) les plus critiques pour l'entreprise et les risques les plus importants parmi lesquels les risques cyber. Pour la plupart, ces analyses ne permettent pas de qualifier ni de quantifier le risque cyber dans une logique assurantielle (financière).

Les entreprises doivent donc réfléchir en termes de transfert du risque cyber vers l'assurance.

Un scénario catastrophe cyber pourrait mettre en danger la pérennité de leur business, leur existence et entraîner leur faillite. Elles doivent également prendre en

[5] Libre Prestation de Services
[6] Difference In Condition / Difference In Limit

compte les responsabilités civiles professionnelles mais également la responsabilité de leurs mandataires sociaux[7].

IV.5.2. Les scénarios du pire

Le contrat cyber repose sur un 1er risque, c'est-à-dire contractuellement le montant maximum par sinistre et par an que l'assureur indemnisera. L'analyse de scénarios catastrophiques, peut permettre à une entreprise de chiffrer leurs conséquences financières. Ce montant doit correspondre au sinistre maximum possible que l'entreprise peut avoir à supporter par exemple en cas :

- d'interruption partielle ou totale de ses systèmes d'information ou de son ou ses prestataires en cas d'externalisation de tout ou partie de ses moyens informatiques ;
- d'atteinte à la confidentialité des données, et notamment en cas de fuite massive de données personnelles.

Il conviendra notamment d'essayer de chiffrer :

- le chiffre d'affaires perdu durant l'incident (marge brute quotidienne, ...) ;
- la perte de chiffre d'affaires dans les semaines ou mois à venir due à la perte de confiance de la clientèle ;
- la perte de productivité des employés impactés (coûts salariaux) ;
- les frais supplémentaires (appel à la sous-traitance) ;
- les frais de restauration des systèmes (réalisée en interne ou par un prestataire extérieur) ;
- les frais de gestion de crise ;
- etc.

Différents instituts de recherche, parfois en partenariat avec certains assureurs cyber qui fournissent des chiffres issus de dossiers réellement indemnisés, donnent aujourd'hui des estimations de coût par donnée personnelle impactée suivant les différents secteurs d'activité.

Sur ces bases, l'entreprise peut se livrer à un exercice somme toute assez simple : identifier le nombre de données personnelles stockées sur un même serveur / groupe de serveurs au sein d'un même espace physique, et en déduire un coût approximatif en cas de compromission de l'ensemble de ces mêmes données.

[7] Source : http://www.irt-systemx.fr/v2/wp-content/uploads/2016/11/ISX-IC-EIC-transfert-risque-LIV-0401-v10_2016-10-25.pdf

Dans certains cas, plusieurs évènements (et donc leurs impacts financiers), pourront se cumuler (scénario d'une fuite de données personnelles massive poussant la société à couper ses services en ligne par mesure de précaution, ce qui génèrera autant de pertes d'exploitation).

IV.5.3. Les couvertures recherchées

L'analyse de risque et l'étude de scénarios catastrophes doivent avoir permis de déterminer quelles garanties sont essentielles pour limiter les conséquences financières d'un sinistre cyber. Les contrats existant proposent notamment les garanties suivantes :

- frais d'expertise informatique :
  En cas d'atteinte aux données et/ou d'une atteinte à la sécurité du système informatique, réelle(s) ou alléguée(s), les frais d'assistance et d'expertise en sécurité informatique peuvent être pris en charge pour :
  - vérifier l'existence et déterminer la cause et l'étendue de l'atteinte ;
  - limiter les effets de l'atteinte aux données et/ou de l'atteinte à la sécurité du système informatique ;
  - formuler des préconisations en matière de reconstitution de données et/ou de protection du système informatique ;

  Ces prestations peuvent être réalisées par un prestataire.
- frais de reconstitution de données ;
- frais de notification :

  Les frais engagés pour assurer la notification à l'autorité administrative compétente et/ou aux personnes ayant subi une atteinte à leurs données à caractère personnel. Ces frais peuvent être engagés en l'absence d'obligation légale ou réglementaire.

  Sont compris les frais engagés pour identifier les personnes ayant subi une atteinte à leurs données à caractère personnel, pour collecter les informations nécessaires et préparer la notification ainsi que pour notifier l'atteinte, à savoir les frais de rédaction, d'impression, d'envoi et de publication.

- frais de monitoring :

  Cela concerne les frais engagés pour détecter et contrôler toute utilisation non autorisée de données à caractère personnel découverte pendant la période d'assurance et suite à une atteinte aux données à caractère personnel.

- pertes d'exploitation et/ou frais supplémentaires après dommages matériels ;
- pertes d'exploitation et/ou frais supplémentaires après sabotages immatériels ;
- frais en cas d'atteinte à la réputation ;

  Peuvent être pris en charge les frais de conseil en relations publiques pour élaborer et mettre en œuvre une stratégie de communication pour limiter les effets de l'atteinte, ou encore les frais préconisés par ce conseil tels que le nettoyage, le noyage et/ou le re-référencement.

- frais en cas de tentatives de cyber-extorsion ;
- fraude informatique ;
- Etc.

IV.6. Audit des assurances existantes

Un audit des contrats d'assurances de l'entreprise va permettre de mesurer la façon dont le risque résiduel devra ou non être transféré à l'assureur et de déterminer les zones non couvertes ou les doubles garanties superflues. Cet audit devra s'intéresser aux contrats « cyber » destinés à couvrir spécifiquement les risques informatiques et la protection des données, mais devra également couvrir les autres assurances de l'entreprise :

- assurance responsabilité civile/professionnelle de l'entreprise ;
- assurance responsabilité civile du dirigeant ;
- assurance multirisque entreprise ou dommages aux biens ;
- assurance « tout risque informatique » ;
- assurance protection juridique ;
- assurance fraude ;
- Etc.

Il s'agit de mesurer comment les dommages liés aux risques cyber pourront être pris en compte ainsi que la gestion de crise. Il s'assurera que les services proposés par le contrat cyber en cas de sinistre s'harmonisent avec les éventuels dispositifs existant en matière de gestion de crise.

Il faudra étudier avec attention les exclusions que comportent ces contrats. Face aux scénarios de crise qui auront été imaginés (Cf. § « Les scénarios du pire »), un travail de traduction des garanties proposées est nécessaire pour s'assurer que le périmètre couvert correspond aux besoins définis.

Dans cette optique, la réécriture d'un contrat existant (suppression d'une exclusion par exemple ou ajout d'une garantie) ou la souscription d'un contrat spécifique pourrait se révéler utile.

Il sera intéressant de bâtir ou d'adapter le programme d'assurances en faisant jouer la concurrence entre les différents contrats proposés par les assureurs.

L'assurance des risques cyber en France reste un domaine encore souvent vierge. Peu de clients sont équipés et tous les assureurs ne disposent pas encore d'une offre mature. Il existe des différences de couvertures entre les contrats. Les intermédiaires tels que les courtiers joueront alors pleinement leurs rôles en guidant l'entreprise dans ce monde technique en pleine évolution.

IV.7. Rôles et Acteurs

Dans l'entreprise, le profil du souscripteur et de l'évaluateur des risques dépend généralement de sa taille. Plus une entreprise est importante en nombre de salariés, plus elle aura de ressources qualifiées en interne pour assurer le rôle de souscripteur et de gestionnaire de risques.

Pour une entreprise de type TPE ou PME, il est vraisemblable que ce soit le dirigeant de l'entreprise qui assure à la fois l'évaluation des risques et le rôle de souscripteur.

Pour une entreprise de taille intermédiaire ou grosse PME, la décision de souscrire le risque sera plutôt dévolue au Directeur Administratif et Financier (DAF) qui lui-même s'appuiera sur le Directeur des Systèmes d'informations et/ou du RSSI s'il est présent.

Enfin, pour une grande entreprise, le gestionnaire des risques (Risk Manager) s'appuiera sur ses compétences et celles des RSSI et DAF pour assurer l'évaluation des risques et la souscription.

Le tableau ci-dessous récapitule les rôles que peuvent jouer différents acteurs face ou aux côtés de l'assureur lors de la souscription.

Acteurs	**Contribution**
Dirigeant RSSI – *Responsable de la Sécurité des Systèmes d'information*. DSI : *Directeur des Systèmes d'Information* DAF – *Directeur Administratif et Financier* DPD – *Délégué à la protection des données* RPCA : *Responsable du Plan de Continuité d'Activité* Secrétaire Général Risk Manager, Responsable des assurances Contrôle Interne Inspection Générale, Audit Interne	En fonction de la taille de l'entreprise, plusieurs de ces acteurs pourront être sollicités pour • Définir le périmètre de l'étude et de la valeur des éléments à protéger (i.e. stock des matériels informatiques et valorisation des données à protéger). Si la couverture du parc informatique ne pose pas de problème particulier, la valorisation des Data (stock et flux) est un sujet plus sensible. En fonction de l'activité exercée par l'entreprise la protection des données peut être un enjeu stratégique. Certaines approches permettent de préciser la structuration des données et de cerner leur valeur potentielle. • Réaliser un diagnostic du ou des Systèmes d'Information, du dispositif de protection et de prévention qui est un préalable nécessaire avant toute souscription. Ce diagnostic peut être réalisé en interne, par un courtier, un prestataire externe ou encore par les compagnies d'assurances. Selon les intervenants et la taille de l'entreprise, cette prestation pourra ou non être facturée.

Acteurs	Contribution
Courtier	Le courtier d'assurances entre dans la catégorie juridique des Intermédiaires en Assurances (IAS). Souvent spécialisé sur le marché de l'entreprise, il définit avec ses clients un cahier des charges qu'il soumet aux compagnies d'assurances. Le courtier challengera les responsables internes des risques cyber pour optimiser les outils permettant de s'en préserver. Il conseillera le dirigeant d'entreprise afin de protéger son propre patrimoine en cas de mise en cause personnelle à la suite d'un sinistre cyber. Le courtier est un intervenant externe qui peut aider les TPE ne disposant pas des compétences en interne à appréhender les risques cybers et aidera les plus grosses entités à faire travailler ensemble les services internes de l'entreprise qui ont parfois du mal à communiquer (DSI/Risk Management).
Prestataires	Des prestataires peuvent être sollicités par l'entreprise ou par les assureurs pour : • Accompagner l'entreprise (assistance à la maîtrise d'ouvrage), • Réaliser une analyse de risques amont et aider au démarrage de la souscription, • Réaliser des audits, • Rédiger le cahier des charges de l'entreprise à destination de l'assureur, • Réaliser une analyse technique de la police envisagée (intégrée ensuite dans la réflexion entre le Client et son courtier. Les prestataires n'ont pas le droit d'aider à choisir un assureur en se basant sur les critères financiers qui restent le choix du Client ou du courtier qui aura reçu un mandat du client.

IV.8. Proposition de l'assureur

IV.8.1. L'offre technique

Celle-ci va consister en :

- une description des garanties (éléments déclencheurs, types de frais pris en compte, etc.) ;
- une limite contractuelle d'indemnisation et une franchise (soit au niveau global, soit pour chaque garantie) ;
- une description des exclusions et des obligations éventuelles du client (tenir son système à jour, mettre en œuvre un anti-virus, etc.) ;

- une description des services complémentaires éventuellement proposés (gestion de crise, expertise technique, etc.).

IV.8.2. Le budget

Il est difficile de dire ce que peut représenter le coût d'une assurance cyber car le budget dépend de nombreux paramètres (limite de garantie, secteur d'activité, périmètre assuré, sinistralité, etc…).

En effet le contrat peut englober des garanties complémentaires comme la couverture du matériel informatique ou encore de la 'fraude toutes causes'…

En général, le contrat vient s'ajouter aux contrats existants en offrant un certain nombre de garanties complémentaires.

Ce qu'il faut retenir c'est que pour les TPE ce type de contrat peut démarrer en deçà de 1000€ de prime annuelle.

Pour les grands comptes une approche sur-mesure s'impose et il est difficile d'indiquer des montants de primes, même indicatifs.

V. La vie du contrat

V.1. Impact de la mise en œuvre du contrat

La principale conséquence de la mise en place d'un contrat cyber est l'importance de revisiter les différents plans de reprise/continuité d'activité, de gestion de crise, etc. afin d'y intégrer l'assureur et/ou le courtier comme un acteur à part entière dans le processus et de bien formaliser son rôle, son mode de sollicitation, …

Il est également préconisé de tester régulièrement ces plans en y intégrant le contact de l'assureur et la validation que les actions attendues de sa part par l'assuré sont effectivement celles prévues par l'assureur.

V.2. Nécessité de suivi du contrat

Une fois le contrat souscrit, un suivi régulier doit être prévu entre l'intermédiaire d'assurance et son client. Il faut absolument qu'un professionnel de l'assurance mesure régulièrement (et à chaque changement important pour l'entreprise) la bonne adéquation entre la cartographie des risques de l'entreprise et les garanties des contrats d'assurance qu'elle a souscrites.

Il est fréquent que les évolutions naturelles de la vie de l'entreprise (développement, croissance externe, restructuration, etc.) rendent le programme d'assurance inefficace ou moins efficace. C'est le cas par exemple lorsque l'entreprise décide de créer une activité nouvelle et qu'elle oublie de le mentionner dans son contrat RC. C'est également le cas lorsque l'entreprise dans le cadre de son activité « traditionnelle » développe de nouveaux marchés dans des secteurs ou des pays entrant dans le champ des exclusions du contrat qu'elle a initialement souscrit.

Ces remarques générales valent pour tous les contrats d'assurances de l'entreprise et les polices cyber ne font pas exception.

Il est important de mesurer les évolutions en termes d'activité de l'entreprise, de valeur à assurer, de chiffre d'affaires, de nature et volume des données traitées etc. et de le déclarer à l'assureur en cas de modification ou changements significatifs.

Chacun de ces items peut avoir des conséquences sur le programme d'assurance qui a été mis en place.

V.3. Devoirs de l'assuré

Dans certains cas, le contrat peut prévoir l'obligation pour l'assuré de déclarer à l'assureur certaines évolutions pouvant avoir un impact sur le contrat, faute de quoi

un sinistre se produisant dans ce contexte inconnu de l'assureur peut être moins bien couvert voire carrément exclu.

On peut notamment trouver dans ces évolutions :

- l'externalisation du développement, de l'administration ou de l'exploitation du système d'information ;
- le rachat de société(s);
- la création de services « digitaux ». Exemple : une plateforme web pour développer, diversifier, accélérer son activité peut faire évoluer notablement le niveau de risque cyber ;
- un partenariat stratégique nouveau qui génère des flux d'informations qu'il faudra protéger et assurer ;
- l'achat d'un fichier de prospection qui peut nécessiter un renfort de garanties sur le volet « données personnelles ».

Par ailleurs, certains contrats prévoient également que l'assuré s'engage à observer un niveau minimum de sécurité informatique qui passe par :

- la mise à jour des systèmes et logiciels (notamment antivirus) ;
- l'existence de sauvegardes régulières, externalisées, testées ;
- la présence d'un PRA formalisé, et testé régulièrement ;
- la conformité à certains standards (ex. PCI-DSS).

De même que précédemment concernant les déclarations lors d'un sinistre, si des investigations montrent que les obligations de l'assuré ne sont pas remplies, la couverture peut être minorée, voire le sinistre carrément exclu.

V.4. Evolution de la prime

Certaines évolutions auront un impact sur la prime, d'autres non.

Concernant les contrats d'assurance cyber, il est fréquent que le niveau de protection au moment de la souscription évolue positivement, parfois à la demande de l'assureur. Un suivi régulier peut aider le client et son intermédiaire à renégocier la prime afin de tenir compte des efforts réalisés en termes de prévention ou de protection.

La couverture du périmètre à protéger peut également évoluer dans le temps à la hausse (développement du parc d'ordinateurs) ou à la baisse (externalisation du parc).

Il est difficile d'établir un lien « mathématique » entre les moyens de lutte contre les cyber risques et le niveau de prime du contrat cyber. Les assureurs manquent de statistiques pour corréler de façon fine protection/prévention et sinistralité.

Dans la pratique, l'assureur peut accepter de fixer un montant de primes qui tient compte des moyens que le client accepte de mobiliser pour diminuer sa vulnérabilité aux risques informatiques.

Cette négociation sera surtout pertinente pour l'assurance des grands comptes.

Concernant les TPE, les contrats sont souvent standards et les primes faibles. Le suivi permet d'éviter les écarts entre ce que l'on a déclaré au moment de la souscription et les évolutions observées au fil des années. La prime étant cependant très faible (moins de 1000 € pour certaines TPE) les marges de négociation seront quasi inexistantes.

V.5. Gestion des sinistres

Comme pour l'assurance automobile, ce n'est pas l'assureur qui va effectuer l'expertise ni réaliser les réparations.

Les compétences informatique, juridique et de communication peuvent être présentes dans les grands groupes, mais pas nécessairement dans des organisations plus petites. Le service apparaît alors comme un apport essentiel de la police cyber.

Un sinistre cyber provoque une crise à laquelle les entreprises doivent se préparer pour trois raisons :

- quel que soit le niveau de protection et de prévention mis en place toutes les entreprises font ou feront l'objet d'une attaque de type cyber dans les mois ou les années qui viennent. Il est possible et même nécessaire de tout faire pour limiter le succès de ces attaques. Il est impossible de disposer d'une protection garantissant l'échec de toutes les attaques. Les cybercriminels parviennent à percer les coffres forts les mieux gardés ; une bonne politique de sécurité informatique doit donc intégrer un volet gestion de crise en cas d'atteinte aux données ou aux systèmes.
- il est essentiel sur ce type de sinistre d'intervenir rapidement pour en limiter les impacts tout en maîtrisant la confidentialité des interventions ;
- la gestion de crise peut elle-même engendrer de nouveaux risques si elle est mal organisée. Le travail en mode dégradé en est un exemple. La gestion de crise exige anticipation, souplesse et implique parfois de prendre des décisions avec des conséquences négatives mais salvatrices dans leur globalité.

Tous les deux ans, le CLUSIF réalise en France une enquête auprès des entreprises de plus de 100 salariés, des particuliers et en alternance auprès, soit des collectivités territoriales, soit des hôpitaux et des établissements de santé de plus de 100 lits, concernant leurs pratiques et les incidents de sécurité sur leurs SI.

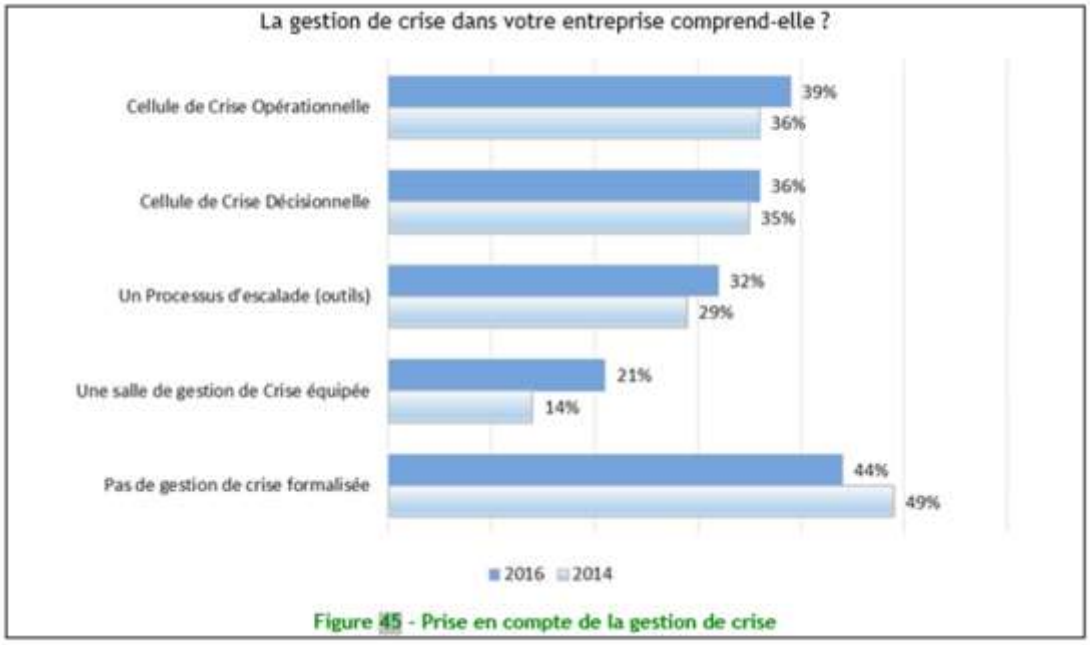


Figure 45 - Prise en compte de la gestion de crise

Menaces informatiques et pratiques de sécurité en France, Edition 2016

Il en ressort en 2016 que :

- 44% des entreprises disposent d'une gestion de crise formalisée ;
- 36% possèdent une cellule de crise, opérationnelle et/ou décisionnelle ;
- 21% disposent d'une salle équipée ;
- 32% ont mis en œuvre un processus d'escalade.

Ces chiffres reflètent le manque de maturité en gestion de crise sécurité des systèmes d'information (SSI) en France, malgré une légère amélioration au fil des années.

Un guide de préparation aux situations d'urgence est disponible sur le portail interministériel de prévention des risques majeurs[8]. Le SGDSN[9] a publié un guide sur la continuité d'activité au sens général du terme.

Plusieurs lois et règlements incitent à préparer la gestion de crise. Chacun devra, en fonction de sa branche d'activité, vérifier s'il existe des documents concernant la gestion de crise (environnement, sites SEVESO, réglementation bancaire, etc.).

Les dirigeants d'entreprise sont entourés de conseils et prestataires de services quelle que soit leur taille (expert-comptable, avocat, etc.). Pour la structuration et la gestion de leur SI les PME ont recours à une société spécialisée qui les aide à acheter le matériel, le mettre en main auprès des collaborateurs, assurer la maintenance. Ce prestataire informatique est en charge de la sécurité du SI. Dans ce

[8] http://www.gouvernement.fr/risques
[9] http://www.sgdsn.gouv.fr/

domaine, il se limite souvent à installer les antivirus et pares-feux et conseille parfois de façon sommaire son client sur la sauvegarde des données.

Si le client ne pose pas plus de questions, les sauvegardes ne seront d'ailleurs parfois jamais testées.

Autant dire que si notre PME subit le choc d'une attaque organisée sur son système d'information aucun de ses interlocuteurs habituels n'aura l'expérience ou l'expertise nécessaire pour l'aider à faire face, à prendre les bonnes décisions dans le domaine du droit ou de la sécurité informatique.

S'il n'a pas anticipé, notre dirigeant devra trouver les bons interlocuteurs en quelques heures au plus fort de la crise. Le temps perdu dans ces recherches et négociations risque fort d'augmenter l'impact de son sinistre.

V.5.1. Prestations associées en cas de sinistre

C'est pour éviter ce scénario catastrophe que les principaux contrats d'assurances Cyber permettent de bénéficier d'un service de gestion de crise en cas de sinistre. Au-delà du volet indemnitaire, ces contrats prévoient l'intervention de professionnels spécialisés qui interviennent sur site ou à distance pour aider les clients à faire face, stopper l'hémorragie et organiser la riposte.

- Les consultants techniques (Forensic) vont intervenir sur site ou à distance pour comprendre l'origine du sinistre et prendre les premières mesures permettant de stopper la fuite ou la corruption des données, la destruction des matériels, la propagation des virus, etc. Ils permettront à l'entreprise de prendre ses dispositions pour éviter la survenance d'un nouveau sinistre du même type. Cela peut aller jusqu'à la collecte de preuves permettant d'envisager par la suite un dépôt de plainte et une investigation judiciaire. Dans ce cas, il convient de faire appel à des intervenants spécifiques, habilités à collecter des preuves. Il est à noter que ces experts techniques peuvent également intervenir en amont (à la demande de l'assuré) afin d'auditer le système d'information et d'accompagner sa mise en sécurité ;
- Les juristes spécialisés aideront l'entreprise à prendre les bonnes décisions dans le respect des réglementations qui s'imposent à tous les secteurs d'activité (ex : respect de la loi Informatique et Libertés) ou au secteur spécifique dans lequel évolue le client (i.e. société de télécommunication). La protection des données personnelles par exemple est un sujet sur lequel la réglementation évolue régulièrement sous l'impulsion du législateur national ou de l'Union européenne. L'intervention des juristes aidera le chef d'entreprise à faire face à d'éventuelles mises en cause de la responsabilité de son entreprise voire de sa responsabilité civile. Ils aideront le chef d'entreprise à préparer des réponses à apporter aux autorités et/ou aux parties prenantes voire à préparer la défense de l'assuré en cas de mise en cause ou de procès. N'oublions pas qu'en cas d'atteinte aux données

personnelles les sanctions peuvent désormais être très lourdes pour l'entreprise défaillante.

- Des centres d'appel peuvent être mobilisés pour aider l'entreprise à faire face aux questions des clients impactés par le sinistre cyber ; ils assureront le cas échéant la notification auprès des clients concernés par l'atteinte aux données personnelles. Cette notification sera rendue obligatoire à compter de mai 2018.
- La communication de crise a pour objectifs d'informer, de rassurer, de protéger l'image de l'entreprise. Elle doit apporter des réponses précises et rapides à toutes les parties prenantes : médias, autorités, clients, salariés, etc. Même lorsque le chef d'entreprise souhaite gérer directement toutes les prises de parole, l'aide d'une agence spécialisée pourra lui être proposée pour l'aider à bâtir dans l'urgence sa communication de crise. Les médias numériques et sociaux permettant une propagation large et rapide des informations, chaque entreprise doit se préparer à faire face à la rumeur avec précision et rapidité. Il peut être à cet égard très utile de se faire assister d'un spécialiste en collecte et analyse en temps réel des informations diffusées par les différents médias, ce prestataire pourra dans certains cas et via différentes techniques amoindrir ou « enfouir » les messages pouvant porter atteinte à l'image de son client.

Le contrat d'assurance cyber va aider l'entreprise à réagir rapidement en :

- finançant la mise en place d'une cellule de gestion de crise,
- bénéficiant immédiatement du réseau de prestataires de services spécialisés (juristes, forensic, agence de communication, consultant gestion de crise...),
- finançant les prestations apportées par ces prestataires externes qui aideront le dirigeant d'entreprise et ses équipes à garder le contrôle opérationnel de la situation.

Ainsi, dès notification de l'incident, l'assureur (ou directement l'assuré selon les cas), peut mobiliser ces experts. Leur coordination globale est gérée, selon les cas, par l'assureur, par l'assuré lui-même, voire par un des experts, identifié comme tel. Il est à noter que ces frais d'expertise sont intégrés aux garanties et sont donc à la charge de l'assureur.

Cette expertise doit être dissociée de l'**expert d'assurance**, dont le rôle est de constater le sinistre de l'assuré et de le quantifier financièrement en vue d'une indemnisation rapide.

V.5.2. Délai pour prévenir l'assureur

L'article L113-2 du code des assurances stipule que l'assuré doit « donner avis à l'assureur, dès qu'il en a eu connaissance et au plus tard dans le délai fixé par le

contrat, de tout sinistre de nature à entraîner la garantie de l'assureur. Ce délai ne peut être inférieur à cinq jours ouvrés. »

En tout état de cause, il est indispensable pour l'assuré de **notifier au plus tôt** son assureur d'un sinistre, sous peine de se voir refuser ses garanties. Par ailleurs, notifier son assureur au plus tôt permettra de mobiliser rapidement le panel d'experts nécessaire à la résolution de l'incident (si prévu au contrat, voir paragraphe précédent), et limitera ainsi les impacts du sinistre. Cela permet également d'engager rapidement des frais d'urgence en étant confiant sur leur prise en charge par l'assureur.

Il est à noter que le délai de notification commence au moment où l'assuré **« a eu connaissance » de l'incident**, et non – et cela a toute son importance dans le contexte cyber – à la date de l'intrusion / du démarrage de l'attaque. À noter que le RGPD impose la notification dans les 72 heures qui suivent la découverte de l'incident.

V.5.3. Chiffrage de sinistre

Le chiffrage du sinistre se déroule en général après la période de crise et se base sur la quantification du préjudice subi par l'assuré.

Un certain nombre de postes sont relativement simples à quantifier (intervention d'experts, déplacement dans le cloud de machines voire de postes de travail, notification, etc.) mais d'autres sont nettement plus complexes.

Ainsi, les pertes d'exploitation font l'objet d'un calcul visant à démontrer le lien entre le sinistre et la baisse du chiffre d'affaires et l'évaluation de cette baisse, tout en intégrant les frais éventuels que l'entreprise n'aura pas eu à débourser compte tenu du sinistre (arrêt d'achat de matières premières si la chaîne de production est arrêtée, etc.).
De même, la perte d'image de marque et les autres conséquences financières sont des préjudices complexes à chiffrer objectivement.
Autre point compliqué, l'intervention des équipes informatiques de l'assuré dans la gestion de crise est difficile à valoriser, sachant que les salaires sont payés de toute manière par l'assuré et que cela n'occasionne pas a priori un préjudice financier.

Dans tous les cas, c'est le travail d'un expert d'assurance que d'identifier et valoriser les différents préjudices financiers, de s'assurer qu'ils font bien partie des garanties souscrites et de vérifier les conditions d'indemnisation (plafond, franchise, cumul, exclusions, etc.).

V.5.4. Lien entre cause et conséquence (éléments de preuve à fournir)

À la demande de l'assureur, l'assuré va devoir fournir des éléments de preuves démontrant, dans la mesure du possible, les causes et les conséquences du sinistre.

Voici des exemples d'éléments de preuve démontrant la cause du sinistre (intrusion, installation d'un logiciel malveillant, injection de code, etc.) :

- fichiers de journalisation (journaux système, journaux de sécurité, etc.) issus du serveur attaqué ;
- rapport d'activité issu d'un outil de sécurité (antivirus, firewall, sonde de détection, etc.) installé sur le serveur ou le réseau ;
- rapport d'activité issu d'un consultant technique en charge d'une analyse forensic ;
- éventuellement des copies d'écran.

Pour les éléments de preuve démontrant les conséquences du sinistre (par exemple vol de données, défacement de site web, attaque DDOS, chiffrement de fichiers ou de disques durs), il faudra s'appuyer sur des éléments spécifiques en lien avec la nature du sinistre :

- fichiers de journalisation (journaux système, journaux de sécurité, etc.) issus de serveur démontrant le vol de données (par exemple : une connexion ftp) ;
- copies d'écran pour le défacement de site web ;
- rapport d'analyse de réseau pour une attaque DDOS ;
- copies d'écran affichant un message lié au chiffrement d'un fichier, répertoire ou disque.

Il faut rappeler cependant que compte tenu du délai moyen constaté avant la découverte d'une attaque (plusieurs mois) ou la sophistication/dissimulation de certaines attaques, la récupération des éléments de preuves peut être une phase très fastidieuse voire impossible à mener dans certains cas.

VI. Cas pratiques

Pour illustrer ce guide, il a été décidé de fournir des cas réels ou vraisemblables qui éclaireront le lecteur. Trois cas sont présentés. Chacun d'eux représente une typologie d'entreprise différente pour coller le plus possible à la réalité des entreprises en France.

- Cas n°1 : une TPE, très petite entreprise dans l'industrie
- Cas n°2 : une ETI, entreprise de taille intermédiaire dans la distribution.
- Cas n°3 : un groupe dans le secteur agro-alimentaire.

Les noms des entreprises ou des personnes citées sont fictifs mais les situations sont tirées d'expériences réelles qui se sont produites en France ou à l'étranger.

VI.1. Cas n°1 : Une TPE dans l'industrie

Société SINIALE

La société SINIALE est une TPE de 10 employés, spécialisée dans la fabrication de panneaux en signalétique, qui réalise 1,1 million de chiffre d'affaires. Elle dispose d'un atelier équipé de diverses machines-outils à commande numérique dont une est dédiée à la découpe au laser de pièces métalliques. Mr DAFIX, comptable de la société, fait également office de responsable Informatique et s'assure que tous les ordinateurs fonctionnent en réseau.

Il fait parfois appel à la société locale CALLME dédiée à la maintenance du parc Informatique avec laquelle il a contracté un accord cadre.

Le 18 juin dernier, Mr DAFIX reçoit un email avec pour attachement une facture qu'il croit provenir de la société MSC (biling@msc.com). A l'ouverture de la facture, Mr DAFIX s'aperçoit que la facture est une erreur et ne prête pas attention au message d'alerte provenant de son logiciel antivirus.

Très tôt le lendemain, Mr COUPOT en charge de l'utilisation de la machine à découpe laser avertit le chef d'atelier que l'ordinateur relié à la machine ne fonctionne pas. L'ordinateur est un vieux PC qui a été installé en 2008 en version Windows XP et qui n'était pas équipé d'un logiciel antivirus puisqu'il n'était pas relié à l'Internet – l'informaticien de l'époque avait désactivé le navigateur.

Lorsque Mr DAFIX arrive au bureau, il est loin de se douter que son ordinateur de bureau très récent (Windows 10) ne démarre pas lui non plus.

Il fait donc appel à la société CALLME qui, à distance, identifie un virus de type rançongiciel et décide de se déplacer sur le site de son client. Très vite, la société CALLME fait le lien entre le problème et l'ouverture, la veille, de la pièce jointe sur le poste de Mr DAFIX.

L'analyse est sans appel, le virus a non seulement chiffré l'ensemble du disque dur du poste de Mr DAFIX mais a également chiffré un espace disque relié en réseau (disque NAS) sur lequel le PC de Mr COUPOT vient chercher les fichiers de configuration de la machine à découpe au laser.

Les conséquences pour la société SINIALE sont immédiates : la production de pièces pour les commandes clients est gelée et la gestion de la comptabilité, de la trésorerie et des bulletins de paie est interrompue tant que le poste de Mr DAFIX n'est pas réhabilité.

Finalement, pendant le temps d'acquisition et de réinstallation d'un nouveau PC pour la commande numérique de la machine à découper au laser (2 semaines), la société SINIALE a décidé de sous-traiter la fonction à une société locale occasionnant plus de 17 000 euros de dépenses et de nombreuses heures stressantes passées à réorganiser la production et à prévenir les clients du retard de livraison.

Pour le poste de Mr DAFIX, les sauvegardes vieilles de quelques jours ont permis de retrouver un environnement sain au bout de 5 jours de travail avec un fort appui de la société CALLME qui a facturé sa prestation 4 000 euros. Il a été décidé de généraliser les antivirus sur l'ensemble des postes de l'entreprises (1 200 euros).

Finalement, c'est 22 200 euros que la société a dû débourser pour retourner à un environnement normal et légèrement plus sécurisé qu'avant l'incident.

La société n'ayant pas souscrit d'assurance spécifique aux risques cyber, elle a dû supporter l'intégralité des dépenses.

À titre d'exemple, il existe en 2018 des contrats d'assurance qui couvrent les risques de la société SINIALE pour une prime proche de 1 000 euros par an, une franchise de l'ordre de 800 euros et un montant maximum de couverture de 30 000 euros.

Dans ce cas, 4 000 euros auraient été indemnisés au titre des frais d'expertise et 17 000 euros au titre des frais supplémentaires d'exploitation. Les 1 200 euros de la généralisation d'anti-virus n'auraient pas été pris en charge. Il faut déduire de ce montant la franchise.

VI.2. Cas n°2 : une ETI dans la distribution

Société BATUR

La société BATUR est spécialisée dans la distribution en quincaillerie industrielle. Elle réalise 100 millions d'euros de chiffre d'affaires et emploie 150 collaborateurs répartis aux deux tiers à la gestion du magasin destiné aux professionnels et à la vente en ligne pour les particuliers, et pour le dernier tiers à la gestion de la chaîne logistique pour assurer notamment les expéditions et la réception de marchandises.

L'agence Web WEBRIX a développé le site Web de vente à distance en s'appuyant sur le logiciel Mazento installé en octobre 2012. Mr BOYER en charge de l'informatique de la société BATUR assure le suivi de l'hébergement (TheDatacenter) et la sauvegarde régulière du site Web. Il apporte également un soutien à l'équipe commerciale lorsqu'il faut mettre à jour le catalogue des produits. Le contrat de maintenance liant la société WEBRIX avec la société BATUR a été rompu en décembre 2013 à la suite de la mise en liquidation de l'agence Web. L'utilisation de l'outil Mazento étant bien maîtrisée par Mr BOYER, aucun nouveau contrat de maintenance n'a été signé depuis.

Fin 2015, la vente en ligne pour les particuliers et professionnels représente 10% du chiffre d'affaires (10 millions d'euros).

En juin 2016, la gendarmerie nationale appelle la société BATUR suite au dépôt de plainte de deux clients ayant acheté en 2015 un produit sur le site Web de la société et prétendant que leurs données de carte bancaire ont été volées. Intriguée, la société BATUR diligente un audit de sécurité qui démontre qu'une cyber attaque a été réalisée au deuxième trimestre 2015.

L'audit, qui a été facturé 10 000 euros, indique également que le logiciel Mazento n'a pas été mis à jour depuis octobre 2013 et que de nombreuses failles de sécurité sont recensées dans les versions produites avant 2016. Un pirate a donc utilisé une faille de sécurité dans l'environnement Mazento pour voler la base de données Clients et se servir des données de cartes bancaires pour effectuer des achats frauduleux à l'étranger.

Dès le 1er juillet 2016, la société BATUR décide d'informer, par courrier, l'ensemble de ses 8 000 clients particuliers et professionnels qu'elle a été victime d'un piratage de son site Web.

L'absence de Plan de Reprise d'Activité (PRA) a fait perdre un temps précieux à l'entreprise qui a mal géré la remédiation du service de vente en ligne. Il a fallu 2 semaines pour remettre le service en production. Outre le manque à gagner en termes de vente (environ 300 000 euros de perte de marge brute) et les coûts de renforcement de la sécurité du site Web (12 000 euros), le principal moteur de

recherche a décidé de déréférencer le site Web batur-pro.com pour 4 semaines, aggravant le manque à gagner et occasionnant un réel déficit d'image pour les clients et les prospects.

Finalement, le préjudice total pour la société BATUR a été évalué à 120 000 euros.

Heureusement, la société BATUR avait contracté en février 2015 un contrat d'assurance cyber qui la couvrait contre la perte de données et les frais de notification à concurrence de 200 000 euros, moyennant une prime annuelle de 20 000 euros et une franchise de 10 000 euros. Exceptés les coûts de renforcement de la sécurité du site Web (12 000 euros), la société a été remboursée de 98 000 euros (120 000 – 12 000 / frais d'amélioration – 10 000 / franchise).

VI.3. Cas n°3 : un groupe dans le secteur agro-alimentaire.

Société BRIDAL

Le groupe agro-alimentaire BRIDAL compte 1 200 collaborateurs pour un chiffre d'affaires de 1 milliard d'euros. Spécialisé dans les légumes frais en sachet et les plats cuisinés, le groupe vend ses produits à tous les acteurs de la grande distribution. La promotion des produits et le service Consommateurs sont faits majoritairement par l'intermédiaire de sites Web et des outils Web très répandus.

L'exploitation Informatique du groupe est internalisée et centralisée sur le site du Mans et est répliquée en quasi temps réel avec le site secondaire de Chartres.

Rompu aux risques de cybersécurité, le groupe BRIDAL a mis en place un Plan de continuité d'activité (PCA) et utilise de nombreuses solutions pour contrer des attaques cyber (pare-feu nouvelle génération avec analyse en continu des flux Internet, redondance des systèmes d'information, sauvegardes des systèmes en temps réel, anti-virus, etc.).

Le matin du 16 mars 2016, un employé trouve une clé USB sur le parking de l'entreprise. Arrivé au bureau et à l'encontre des règles édictées par la PSSI, il ne résiste pas à l'idée de voir le contenu de cette clé pour identifier son propriétaire. Une fois insérée dans l'ordinateur (poste fixe), la clé semble vide puisqu'aucun fichier n'apparaît dans l'explorateur Windows. La politique de sécurité des systèmes d'information (PSSI) en place n'a pas été respectée par l'employé.

Trois mois plus tard, le 15 juin 2016, le progiciel d'entreprise pour la gestion de la logistique ne répond plus. Alors que l'équipe Informatique (20 personnes) s'affaire à redémarrer le service, les 125 employés en charge des commandes clients, des livraisons, de la gestion des entrepôts, de la gestion des achats, sont en attente du retour au bon fonctionnement du progiciel.

En début d'après-midi, l'équipe informatique essaie de basculer sur l'environnement de production de secours basé à Chartres, mais le système de basculement n'est pas pleinement opérationnel. Constat de l'équipe informatique : le système de gestion de base de données de l'éditeur BaseData est inopérant et montre que les bases de données contiennent des données incohérentes, apparemment chiffrées. Le support de BaseData est appelé en urgence pour assurer un diagnostic.

En fin de soirée, alors qu'aucun camion n'a pu sortir des entrepôts du groupe, les experts de BaseData donnent leur conclusion : les sites ont été victimes d'une attaque informatique qui a détruit sur les deux sites les données systèmes de l'ERP et chiffré les bases de données utilisateurs et produits.

Le directeur informatique en lien avec le directeur général prend alors trois décisions majeures :

- déclencher la cellule de crise pour assurer une communication cohérente et mettre en œuvre le PRA (Plan de Reprise d'Activité) ;
- faire venir en urgence une équipe d'experts de BaseData pour remettre en fonctionnement le progiciel ;
- diligenter une équipe d'experts en sécurité informatique pour analyser la cause du problème.

Le lendemain, les experts de BaseData sur le site du Mans, décident de réinstaller intégralement le système de gestion de base de données et de s'appuyer sur un jeu de sauvegarde du 10 juin 2016 pour reconstituer les bases de données.

Le même jour, les experts en sécurité informatique découvrent qu'un virus (un Cheval de Troie) installé sur un poste interne est à l'origine de l'attaque informatique. En revanche, ils ne parviennent pas à tracer l'arrivée du virus depuis le réseau externe (Mail ou Internet). Ils en déduisent que le virus est arrivé par un support média externe (clé USB, disque dur ou carte mémoire).

Un message envoyé par le directeur informatique, à tout le personnel, permettra d'identifier l'employé ayant inséré une clé USB non identifiée. L'analyse de cette clé démontrera la présence du virus fautif bien qu'invisible pour un néophyte.

Finalement, le progiciel reviendra à un niveau opérationnel au bout du quatrième jour, et c'est seulement au cinquième jour que l'entreprise a repris un fonctionnement normal.

Pendant ces cinq jours, le groupe aura fait face à de nombreux désagréments opérationnels, financiers, techniques, humains et d'image. Sur tous ces plans, le groupe :

- n'a pas pu livrer ses produits à ses clients, occasionnant des pertes d'exploitation, des mises au rebut de produits frais et des pénalités contractuelles avec les magasins de la grande distribution. Certains produits n'ont pas été remis en rayon pendant plusieurs jours ;

- n’a pas pu réceptionner les produits frais des producteurs, occasionnant des mécontentements et des pénalités financières ;
- a dû recourir à un chômage technique auprès de certains de ses salariés, occasionnant des coûts financiers et des mécontentements ;
- a dû supporter des coûts exceptionnels liés à la gestion technique des entrepôts (location espace entrepôts réfrigérés supplémentaires) ;
- doit encore (janvier 2017) supporter un déficit d’image lié à ce dysfonctionnement.

Finalement, le préjudice financier pour le groupe s’élève à 2,5 millions d’euros.

Le groupe BRIDAL avait contracté en 2015 une assurance cyber couvrant les frais suivants à la suite d’une cyber-attaque :

- les frais de reconstitution de données à la suite d’une perte ou un vol, les frais de notification, les frais de gestion de crise, etc.
- cyber-extorsion, frais d’atteintes à la réputation, etc.

Cependant l’entreprise n’avait pas contracté une assurance contre les malveillances internes, qu’elles soient issues d’un employé ou d’un contractant. L’assureur a donc refusé de prendre en charge la totalité des frais occasionnés par ce litige.

Une analyse interne a démontré quelques mois plus tard que les impacts associés à cet incident auraient pu grandement être diminués si :

- des basculements vers l’environnement de secours avaient été testés régulièrement ;
- un programme de sensibilisation à la cybercriminalité et aux bonnes pratiques de sécurité avait été mis en place pour l’ensemble du personnel.

VII. Prospectif

VII.1. Prospectif (IoT, nouveaux usages)

Les progrès technologiques de ces dernières années, notamment dans les domaines de l'intelligence artificielle, des communications sans fil et du big data, ont fait émerger deux nouvelles familles de produits : l'internet des objets et les véhicules autonomes.

Concernant l'Internet des objets, certains spécialistes estiment qu'en 2020, près de 1000 milliards de dispositifs seront connectés à Internet. Incrustés dans nos vêtements, installés par dizaines dans nos maisons, dispositifs de surveillance à hôpital et dans les usines, de vérification dans les entrepôts : les objets connectés créent des usages variés et multiples qui visent à rendre notre vie plus confortable, mieux contrôlée et plus efficace.

Les véhicules autonomes, automobiles, drones et d'une certaine manière les robots, constituent eux aussi de formidables opportunités visant à améliorer et sécuriser notre vie quotidienne.

Malheureusement, l'adoption massive de ces nouveaux usages apporte son lot de nouveaux risques ayant des effets et impacts négatifs très importants. À titre d'exemple, prenons le botnet Mirai qui, en septembre 2016, a pris le contrôle de centaines de milliers de caméras de surveillance pour considérablement réduire l'accès internet de nombreux sites majeurs de la côte Est américaine. Autre exemple, un groupe de Chinois a démontré qu'il pouvait prendre le contrôle à distance des voitures de marque *Tesla* même pendant qu'elles roulaient.

Il est encore très difficile pour les assureurs de proposer des offres pour ces nouvelles technologies et les usages associés, mais gageons que dans quelques années des offres de cyber-assurances vont apparaître pour adresser ces nouveaux risques.

VIII. Définitions / Glossaire

Cyber-attaque	Une cyber-attaque est une **atteinte à des systèmes informatiques réalisée dans un but malveillant.** Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les smartphones ou les tablettes.
Cyber-risque	Il existe 4 types de cyber-risques aux conséquences diverses, affectant directement ou indirectement les particuliers, les administrations et les entreprises : **la cybercriminalité, l'atteinte à l'image, l'espionnage, le sabotage.**
DMIA	La **durée maximale d'interruption admissible** est l'expression de besoin de disponibilité des différents métiers ou services, dans une organisation.
DDOS	Une attaque par **déni de service** (abr. DoS attack pour Denial of Service attack en anglais) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. À l'heure actuelle la grande majorité de ces attaques se font à partir de plusieurs sources, on parle alors d'attaque par déni de service distribuée (abr. **DDoS** attack pour Distributed Denial of Service attack).
DOS	Voir DDOS
Dommage	Le dommage est l'atteinte subie par une personne. En assurance, le dommage correspond à un préjudice, c'est à dire une atteinte à des droits subjectifs, par un ou plusieurs tiers, qui justifie une réparation pour l'assuré, ou une indemnisation dans la majorité des cas.
Erreur humaine	Une erreur de manipulation y compris dans le choix du programme utilisé, une erreur de paramétrage ainsi que toute intervention ponctuelle inappropriée d'un préposé de l'Assuré ou d'un Prestataire de services.
Exclusion	Cela concerne tout ce qui n'est pas garanti par le contrat d'assurance. Tous les contrats d'assurance intègrent des exclusions de garanties.
Frais d'amélioration	Les frais d'amélioration constituent les **frais supplémentaires** à engager lorsqu'il n'est pas possible ou trop coûteux de remettre le système d'information à l'identique avant le sinistre.
Franchise	Une franchise prévue dans un contrat d'assurance est la **somme restant à la charge** de l'assuré (donc non indemnisée par l'assureur) dans le cas où survient un sinistre.
Garantie	**Obligation** de l'assureur de dédommager l'assuré en cas de réalisation d'un risque déterminé dans les termes du contrat d'assurance.
IaaS	L'infrastructure en tant que service ou, en anglais, infrastructure as a service (**IaaS**) est un modèle de cloud computing qui permet aux entreprises de disposer d'une infrastructure informatique (serveurs, stockage, sauvegarde, réseau) se trouvant physiquement chez le fournisseur.
IoT	L'Internet des objets (en anglais « Internet of Things » ou IoT) représente l'extension d'Internet à des choses et à des lieux du monde physique.
Limite contractuelle	Plafond maximum d'indemnisation par sinistre auquel l'assuré peut prétendre au titre des garanties.

d'indemnisation	
Limite de garantie	La limitation de garantie détermine i) les conditions dans lesquelles l'assureur accepte de prendre en charge un sinistre, ii) les conditions dans lesquelles l'assurance peut jouer ou non, le champ d'application, iii) le niveau des remboursements et iv) les franchises.
Malveillance	Le risque de malveillance se réfère aux menaces et aux dangers liés à l'homme sur les biens, les personnes, les ouvrages et les installations alors que les autres facteurs de risque sont d'origine accidentelle ou liés à des événements naturels.
Malware	Un logiciel malveillant ou maliciel, aussi dénommé **malware** et parfois logiciel nuisible ou pourriciel, est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.
Noyage	Le noyage est une technique qui consiste à développer sa présence sur le web et donc sur les moteurs de recherche dans le but de faire recalculer les résultats gênants dans vos pages de résultats.
Non-renonciation à recours	Clause habituelle d'un contrat d'assurance qui interdit à un assuré de renoncer à sa faculté à recourir contre un ou plusieurs de ses prestataires en cas d'incident
PaaS	Plate-forme en tant que service, **PaaS**, de l'anglais platform as a service, est l'un des types de cloud computing, permettant de mettre à disposition des entreprises un environnement d'exécution rapidement disponible, en leur laissant la maîtrise des applications qu'elles peuvent installer, configurer et utiliser elles-mêmes.
PDMA	La perte de données maximale admissible (**PDMA**), en anglais recovery point objective (RPO) quantifie les données qu'un système d'information peut être amené à perdre par suite d'un incident. Usuellement, elle exprime une durée entre l'incident provoquant la perte de données et la date la plus récente des données qui seront utilisées en remplacement des données perdues. Cette durée est exprimée généralement en heures ou minutes.
PSSI	La Politique de Sécurité des Systèmes d'Information (**PSSI**) définit les règles et les principes de sécurité qui s'appliquent sur les systèmes d'information d'une organisation
Perte de marge brute	La perte de la marge brute est le **produit** de la **baisse du chiffre d'affaires par le taux de marge brute**
Prime	La prime d'assurance est le **prix** que le preneur d'assurance doit payer pour pouvoir bénéficier de la couverture d'assurance en cas de sinistre.
RC	La responsabilité civile (RC) est l'obligation de réparer le dommage causé à autrui. Elle peut faire l'objet d'une assurance, parfois obligatoire et régie par différents textes de loi.
RGPD	Le Règlement Général pour la Protection des Données (RGPD) désigne la dernière initiative européenne concernant les données personnelles, publié en 2016 et devant entrer en application dans les États membres le 25 mai 2018. Il comprend notamment de nouvelles obligations relatives à la portabilité des données personnelles et à la responsabilisation des dépositaires de ces données qui impactent fortement les usages qui se rapportent à ce type de données.

Risque résiduel	Le risque résiduel est le « **risque subsistant après le traitement du risque** » ou le « risque subsistant après que des **mesures de prévention ont été prises**. »
SaaS	Le logiciel en tant que service ou software as a service (**SaaS**) est un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur. C'est donc la livraison conjointe de moyens, de services et d'expertise qui permet aux entreprises d'externaliser intégralement un aspect de leur système d'information (messagerie, sécurité…) et de l'assimiler à un coût de fonctionnement plutôt qu'à un investissement.
Sinistre	Le sinistre est constitué par la survenance du risque prévu par le contrat d'assurance ; il entraîne la mise en jeu de la garantie.
Sinistre majeur	Un sinistre majeur est un événement dû à **un phénomène naturel, une défaillance technologique ou un accident** découlant ou non de l'intervention humaine, qui cause de graves préjudices aux personnes ou d'importants dommages aux biens et exige de l'assuré des **mesures inhabituelles**.
Sous-limite	L'assureur peut en principe **limiter sa garantie** au moyen d'un plafond qui s'applique par année et/ou par sinistre. On parle alors de sous-limite.
Taux de marge brute	Le taux de marge brute correspond au rapport de la **différence entre le prix de vente et le coût d'achat** d'une marchandise sur le coût d'achat.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue de Mogador
75009 Paris
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

Téléchargez toutes les productions du CLUSIF sur
www.clusif.fr/publications