KPMG

La Cyber-assurance

Institut des Actuaires

La préparation de ce support a bénéficié de l'aide d'Alain Depiquigny, courtier spécialisé en Cyber assurance et Cyber risque

Vendredi 12 mai 2017 Montpellier

Sommaire

KPMG

Introduction : le cyber risque

Introduction : définition du risque cyber

*Une **atteinte** aux **données numériques** détenues et/ou gérées par une organisation (entreprise, association, collectivité locale, administration) que celles-ci lui appartiennent ou qu'elles lui soient confiés par des tiers, ainsi que les conséquences d'une atteinte au **système d'information***

Introduction : l'assurance Risque Cyber

- L'assurance Risque Cyber couvre les conséquences des atteintes au système d 'information :
  - Reconstitution des données
  - Perte d'exploitation
  - Responsabilité civile
  - **Assistance** en cas de sinistre :
    - Forensic
    - Juridique
    - Communication…

- Les causes des atteintes peuvent être :
  - Accidentelles ou résulter d'actions non intentionnelles (erreur humaine)
  - Résulter d'actes de malveillance

- Elle se distingue de l'assurance fraude et d'une assurance « multirisques » de par le type de conséquence pris en charge

- Le marché de la cyber sécurité représente 77 milliards $ en 2015 et devrait monter à 170 milliards en 2020

Quelques chiffres

- 93% des entreprises françaises ont été victimes d'au moins une tentative de fraude au cours des 12 derniers mois
- 20% ont connu plus de 10 tentatives sur cette période et 30% n'ont pas réussi à déjouer toutes les tentatives
- Le taux de fraude en France a doublé en sept ans
- 3,5 Mds€ le coût de la cybercriminalité en France en 2015
- En 2016, doublement des fraudes (identifiées) au sein des entreprises de moins de 100 salariés

KPMG

Historique

Historique

- Origines de la cyber assurance dans les années 1980
- Premières offres de cyber assurance dans les années 1990 pour le secteur bancaire
- Le marché de la cyber assurance a connu une croissance relative importante mis sans commune mesure avec celle de l'informatique et du web
- Ces limites peuvent avoir plusieurs causes :
  - Les entreprises préfèrent s'auto-assurer,
  - Elles éprouvent des difficultés à comparer les offres d'assurance
  - Celles-ci ne couvrent pas l'ensemble des risques
  - L'inter-corrélation des risques ainsi que le manque de recul historique incite les assureurs à la prudence
- On observe néanmoins depuis quelques années une accélération du marché :
  - Des acteurs, assureurs et réassureurs, importants s'y intéressent
  - Des évolutions techniques et règlementaires font encore croître le besoin d'assurance des acteurs économiques

Historique

- Aujourd'hui la majorité des compagnies proposent une offre de cyber assurance, ce phénomène pouvant être daté à environ cinq ans

- Il est plus ancien aux USA où il date d'au moins 20 ans

- La tendance actuelle sur le marché de la cyber assurance se décline ainsi :
  - Capacité – appétits ↗
  - Prix ↘
  - Franchises ↘
  - Garanties ↗

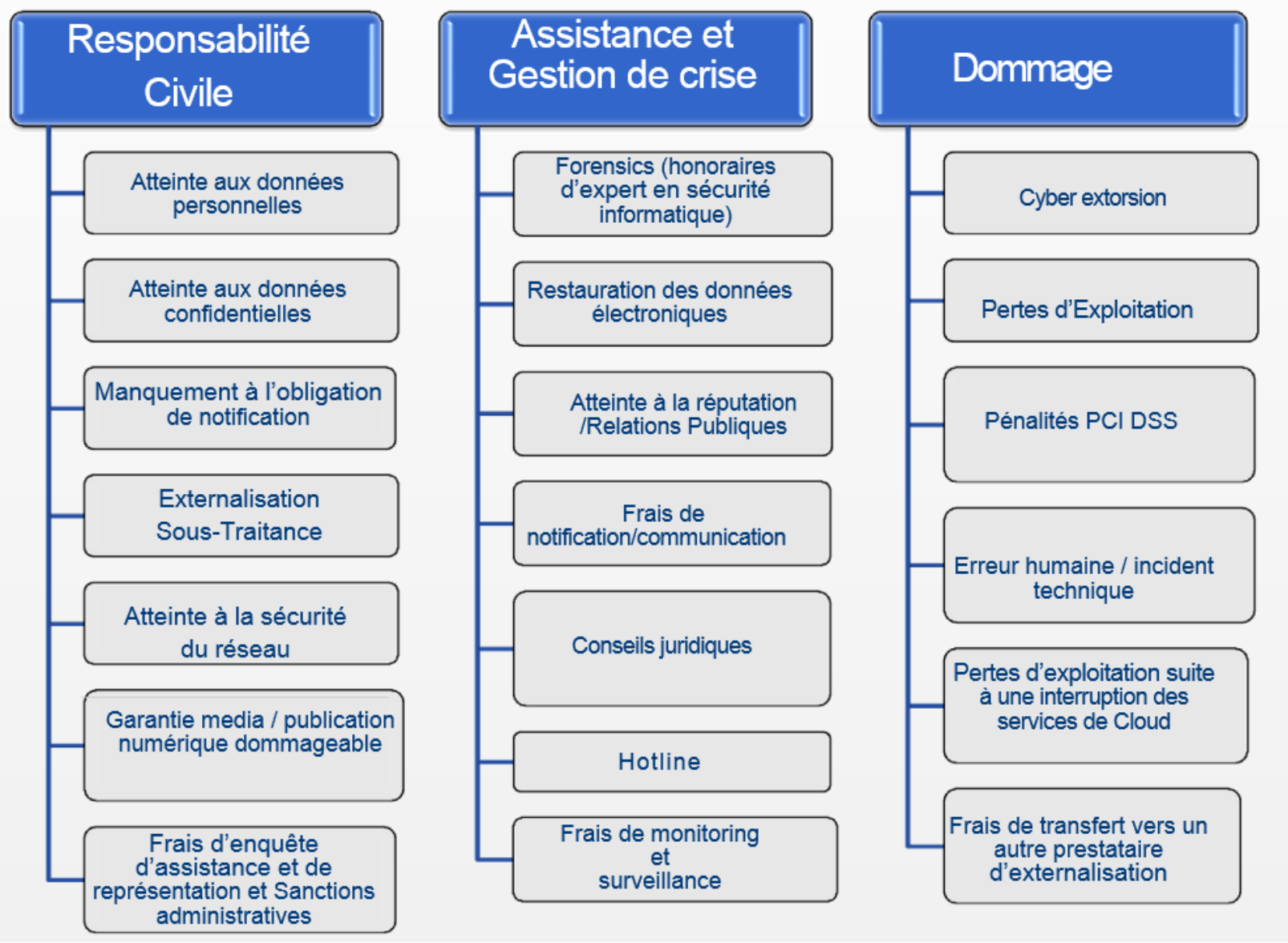
KPMG

Le marché :
-Les acteurs
-L'offre

Panorama du marché

- Une quinzaine d'acteurs présents sur le marché
- La capacité du marché français est de l'ordre de 600 M€, soit une croissance exponentielle depuis plusieurs années (x5 en 3 ans)
- Les acteurs majeurs sont anglo-saxons : AIG, CHUBB, LOYD'S, CNA, HISCOX
- Autres grands acteurs : ALLIANZ, AXA, ZURICH, XL
- Certains réassureurs interviennent en direct : SWISS Ré, MUNICH Ré

Les garanties d'un plan d'assurance cyber



Eléments de garanties et de franchise

- Eléments pour des offres standards :
  - Limite globale de 10M€ à 15M€ environ
  - Franchise de 10K€ à 15K€ (offre PME / ETI)

- Concernant les grands risques, les franchises dépassent 50K€, les limites globales sont spécifiques et se mesurent en dizaines de M€

KPMG

Quelques exemples

Exemples d'actualité

- Octobre 2015 : demande de rançon (« ransomware ») contre l'hydrolienne de Sabella en Bretagne. Interruption de production pendant quinze jours

- Importante coupure du réseau électrique ukrainien le 2 décembre 2015 due à l'implantation d'un virus à la suite d'une campagne de «phishing »

Ransomware

En 2015, peu avant Noël, une entreprise de broderie en ligne basée au Royaume-Uni a subi une attaque par ransomware. L'auteur de cette attaque a créé deux comptes utilisateurs et a tenté de crypter et de supprimer les données clients de l'entreprise, ainsi que d'autres informations concernant ses commandes, ses stocks et ses comptes. Il a ensuite envoyé une demande de rançon dans laquelle il donnait pour instruction à l'assuré d'envoyer un message à l'adresse e-mail communiquée.

L'auteur de l'attaque n'est pas parvenu à crypter les données, mais il a réussi à supprimer de nombreux fichiers et à déplacer certaines données. Ne pouvant plus se fier aux données déplacées, l'assuré se trouvait dans l'incapacité d'exercer son activité via le système. La dernière sauvegarde de données datait de quatre jours avant l'incident, de sorte que l'ensemble des données de la semaine précédente étaient également perdues.

Suite à cette attaque, l'assuré a reçu les conseils d'experts juridiques et informatiques. Les données de tiers ne semblaient pas avoir été compromises. Il fut donc conseillé à l'assuré de ne pas déclarer l'incident aux autorités en charge de la protection des données.

Les consultants informatiques de l'assuré lui ont proposé des solutions pour atténuer les conséquences de l'incident et l'ont conseillé sur les précautions à prendre pour éviter qu'il se reproduise. Ils lui ont notamment conseillé de sauvegarder les données contenues dans le serveur touché afin de déterminer l'origine de l'incident et de revoir son plan de reprise d'activité après sinistre.

Cryptage de fichier d'un intermédiaire d'assurance

L'un des ordinateurs de l'assuré a été contaminé par le malware CryptoWall, qui a crypté certains fichiers qui y étaient stockés ainsi que le serveur interne. Les fichiers ont été renommés « help_your_files.png » et une rançon a été demandée en échange de l'accès aux données.

L'assuré, basé au Royaume-Uni, pensait que les fichiers cryptés contenaient certaines données clients, comme des noms et des adresses, mais pas d'autres données à caractère personnel ni d'informations financières. Aucune preuve ne laissait suggérer que les données contenues dans les fichiers cryptés avaient été consultées ou exportées, ou que des données avaient pu être perdues, en raison des sauvegardes régulières prévues par le système informatique de l'assuré.

L'assuré a reçu les conseils d'un expert juridique concernant l'étendue de ses obligations déclaratives au Lloyd's et à la FCA. Des consultants externes en informatique ont également proposé certaines mesures d'urgence destinées à contenir l'incident (restriction du partage de fichiers entre utilisateurs, notamment) et ont proposé des mesures préventives destinées à éviter qu'un tel incident se reproduise.

KPMG

Réglementation -Obligations et responsabilité -GDPR

Obligations et responsabilités

USA

De nombreux états ont des lois encadrant l'utilisation de données personnelles qui complètent la règlementation fédérale. Celle-ci a été écrite selon des lois séparées pour les différents secteurs.
Les données de santé sont fortement règlementées. Les données liées aux activités financières sont soummises à des contraintes spécifiques en termes de protection et de notification. L'état fédéral étudie une loi pour rendre homogène les obligations de notification sur tout le territoire

1

Europe : l'état actuel (2017)

La directive 95/46/EC du 24 octobre 1995 définit les obligations d'information du consommateur sur la récupération de ses données personnelles. Les données ne peuvent sortir d'un territoire de l'union que vers un pays offrant une règlementation au moins aussi stricte. Un accord avec les USA en date du 1er décembre 2016 vient de permettre de tels échanges de données, ce qui n'était pas le cas jusqu'alors.
Les obligations de notification ne sont pas encore harmonisés mais vont l'être avec la directive GDPR.

2

Europe : les changements en cours

Au départ essentiellement de nature technique le cyber-risque présente une dimension juridique et de conformité de plus en plus importante et qui va aller croissante, notamment avec l'entrée en vigueur de la directive GDPR

3

L'évolution de la législation applicable en France

- Loi n° 78-17 du 6 janvier 1978 dite « Loi informatique et liberté »
- Directive européenne 95/46/CE de 1995
- Adoption de GDPR par le parlement européen le 12 avril 2016
- Application effective du GDPR le 24 mai 2018

KPMG

Modélisation actuarielle

Modélisation actuarielle

Les problèmes auxquels sont confrontés les actuaires

-Estimation de la fréquence

-Estimation de la sévérité (en coût en volume de données)

-Mise en évidence d'une corrélation coût-fréquence

-Estimation de la dérive temporelle du risque

→ Le manque de recul historique rend probablement illusoire à ce stade une estimation satisfaisante du coût de revient du risque, mais le marché évolue vite et davantage de données sont disponibles chaque année

→ L'hétérogénéité des tarifs est la conséquence naturelle de ce manque de recul statistique : l'assurance cyber n'est pas l'alternative à la prévention et aux politiques de protection du SI, mais son complément

→ Un champ de travail pour les actuaires !!

KPMG

Conclusion

Conclusion

Les questions structurantes autour de la cyber assurance

-Penser le programme d'assurance cyber conjointement avec l'assurance fraude : éviter les doublons mais surtout vérifier qu'il n'y a pas de « trou dans la raquette »

-L'assurance cyber doit comporter un volet assistance tant IT que juridique

-L'assurance cyber ne remplace pas la protection et la prévention contre le risque cyber, elle en est le complément

→ Le risque cyber sera-t-il obligatoire (après) demain compte tenu de l'importance des risques que les organisations font peser sur des tiers ?

→ Ou bien au contraire, compte tenu de sn caractère systémique verra-t-on un jour l'émergence de système de mutualisation publique ?

→ …Quelle place pour ce risque dans la régulation prudentielle du futur, une fonction clé attachée au risque cyber dans Solvabilité 3 et Bale 4 ?

KPMG

Merci

François BONNIN - Alain DEPIQUIGNY