MAUBOURG ENTREPRISE

EXPERTISE FINANCIERE
CONSEIL EN STRATEGIE ET GESTION PATRIMONIALE
PLANIFICATION FISCALE ET SOCIALE

Siège Social : 1 rue Villaret de Joyeuse - 75017 Paris
SIRET N° 432 240 182 R.C.S PARIS
Capital Social : 10.000 € - Code NAF : 6622Z

Tél. 01 42 85 80 00 • Fax 01 42 85 80 44
www.maubourg-patrimoine.fr
info@maubourg-patrimoine.fr

# Deux ou trois choses à savoir avant de souscrire une cyber assurance

## Quelques exemples

### Vol des disques durs de l'entreprise :

Une entreprise qui travaille dans le domaine médical est victime du vol de plusieurs disques durs externes contenant les données médicales & bancaires de 300 000 clients. Des salariés, au cours d'un déplacement professionnel, ont perdu les disques durs dans les transports. Une enquête de la CNIL est ouverte et des plaintes sont engagées par plusieurs centaines de patients également.

***Intervention de l'assureur :*** *l'assureur en cyber risques prend en charge les frais d'avocat, les frais de relations publiques pour gérer l'enquête, les frais de notification (300.000 individus + administration, suivant réglementation en vigueur), les frais de crédit monitoring ou « surveillance de données bancaires »[1] et les coûts de communication via un centre d'appels.*

[1] Utilisé en cas de compromission de données, le service de monitoring de données vise à vérifier que ces dernières ne sont pas utilisées frauduleusement par des tiers (usurpations d'identité, transactions bancaires frauduleuses par ex.). Pour les données bancaires à surveiller, on parle de « credit monitoring ». Le prestataire met en place une

**Fraude d'un salarié dans une société d'expertise dommages – accident :**

L'employé d'une société d'expertise dommage-accident outrepasse ses autorités d'accès aux bases de données de l'entreprise pour aller chercher et copier les archives numériques concernant les victimes d'accidents de la circulation, pour les transmettre à un cabinet d'avocat à des fins de démarchage commercial. Une action est engagée par les personnes victimes de la fraude du fait de la violation des données personnelles et de la divulgation d'informations confidentielles. L'employé auteur de la fraude est poursuivi sur le plan pénal.

***Intervention de l'assureur :*** *l'assureur en cyber risques prend en charge les frais de notification (13.000 individus + les autorités de contrôle), les coûts générés par le « call center » et le service de crédit monitoring ainsi que les frais d'avocat (détermination des obligations de notification) et les frais d'expertise informatique relatifs à la revue de l'ensemble des dossiers clients).*

**Vol de 5 ordinateurs portables remplis de données :**

Une entreprise subit le vol de 5 ordinateurs portables lui appartenant suite à une effraction dans les bureaux. Les ordinateurs contenaient des informations confidentielles sur ses employés et ses clients. Malgré la plainte déposée par l'entreprise, aucune poursuite judiciaire n'a pu être intentée puisque l'auteur du vol n'a jamais été retrouvé. Les clients et employés concernés ont été prévenus, ainsi que le régulateur (CNIL).

***Intervention de l'assureur :*** *l'entreprise assurée a été très réactive dans le traitement de la perte de données. Par conséquent, il n'y a pas eu d'actions intentées contre elle du fait des opérations de monitoring mises en place. Aucun prestataire informatique n'a été mandaté dans ce cas puisque les ordinateurs volés n'ont bien sûr jamais été retrouvés, donc inaccessibles à toute analyse. L'assureur a cherché au côté de l'entreprise assurée un prestataire pour le monitoring de données. Le prestataire retenu ne faisait pas partie des partenaires habituels de la compagnie d'assurance. L'assureur en cyber risques a pris en charge les frais de notification (150 individus + administration), le monitoring de données pendant 6 mois, les frais d'avocat et d'experts pour déterminer l'étendue des obligations de notification, savoir combien de clients et employés étaient concernés, définir quel régulateur avertir et savoir quelles mesures correctives mettre en place.*

**Piratage des comptes utilisateurs d'un site internet :** le site internet d'une entreprise se fait pirater et voler 150 identifiants & mots de passe. Le vol est signalé à l'entreprise par un tiers spécialiste de la cyber-sécurité.

***Intervention de l'assureur :*** *aucune poursuite judiciaire n'est engagée puisque l'auteur du piratage et du vol n'a pas été retrouvé. Les clients et employés concernés ont été prévenus, ainsi que le régulateur. Aucune action en justice n'a été engagée contre l'entreprise assurée du fait des opérations de monitoring mises en place très rapidement. Un avocat pour déterminer les*

---

surveillance des données, (similaire aux alertes google mais en plus sophistiqué), essentiellement sur internet et auprès des banques / institutions financières, des administrations, du fisc, etc

*obligations de notification et une agence de communication de crise partenaire (pour gérer les relations publiques) de l'assureur en cyber risques sont mandatés. Aucun prestataire informatique n'a besoin d'intervenir autre que la société spécialisée qui a porté l'incident à la connaissance de l'assuré.*

## Archivage et stockage de données médicales :

Le serveur d'une entreprise est piraté suite à l'intervention d'un tiers sur son système informatique. Le prestataire mis en cause a involontairement créé une faille de sécurité, à savoir l'accès à distance possible au serveur sans aucun filtre pendant plusieurs heures. Le piratage des serveurs a généré des perturbations et interruptions des services fournis aux clients (stockage et archivage de données médicales pour les professionnels de santé). Le serveur a dû être arrêté et redémarré. L'entreprise est contrainte de changer l'intégralité des identifiants et mots de passe des utilisateurs de ses services.

***Intervention de l'assureur :*** *l'entreprise reçoit plusieurs réclamations de clients, principalement du fait de l'inaccessibilité des dossiers et historiques des patients lors des consultations (synthèse des analyses, évolution des prescriptions, etc.). L'entreprise victime du piratage a également consenti plusieurs gestes commerciaux et avoirs sur factures en accord avec l'assureur qui a donc pu les prendre en charge. L'intervention de l'assureur a concerné les frais d'expertise informatique (analyse du système d'information pour trouver et réparer la faille), les frais de communication auprès des clients, l'indemnisation des clients victimes d'un préjudice lié aux problèmes dans la fourniture de services de l'entreprise et les frais de mise en place d'une hotline avec un centre d'appels.*

## Piratage des comptes utilisateurs d'un site internet :

Le site internet d'une entreprise se fait pirater et voler 150 identifiants & mots de passe. Le vol est signalé à l'entreprise par un tiers spécialiste de la cyber-sécurité.

***Intervention de l'assureur :*** *aucune poursuite judiciaire n'est engagée puisque l'auteur du piratage et du vol n'a pas été retrouvé. Les clients et employés concernés ont été prévenus, ainsi que le régulateur. Aucune action en justice n'a été engagée contre l'entreprise assurée du fait des opérations de monitoring mises en place très rapidement. Un avocat pour déterminer les obligations de notification et une agence de communication de crise partenaire (pour gérer les relations publiques) de l'assureur en cyber risques sont mandatés. Aucun prestataire informatique n'a besoin d'intervenir autre que la société spécialisée qui a porté l'incident à la connaissance de l'assuré.*

## Piratage des lignes téléphoniques :

Un centre d'appel se fait pirater ses installations téléphoniques : 22 000 appels frauduleux sont passés à destination de téléphones mobiles situés à l'étranger sont émis en 3 jours. La société

possède plusieurs sites en Europe et en Afrique du Nord et propose notamment des prestations de hotlines, de démarchage téléphonique et de services clients. Le centre d'appels a détecté une consommation téléphonique anormale vers des destinations internationales inhabituelles (Europe de l'Est, Amérique du Sud). Ses installations téléphoniques étaient pourtant protégées par plusieurs solutions de sécurité qui n'ont cependant pas empêché le cyber-pirate de s'y introduire en utilisant des identifiants et mots de passe valides (usurpation d'identité). L'entreprise subit une surfacturation téléphonique et analyse tout son système d'information pour trouver et réparer la faille utilisée par le pirate.

**Intervention de l'assureur :** La cause du piratage n'était pas un problème d'installation ou de configuration du système téléphonique de l'assuré. Aucun recours n'a donc été possible contre le prestataire de télécommunication. L'assureur en cyber risques a pris les charges la surfacturation téléphonique subie par le centre d'appel et les frais d'expertise informatique (analyse du système d'information pour trouver et réparer la faille).

## Vol des codes sources d'un éditeur de logiciel :

Un petit éditeur de logiciels et solutions internet développe et commercialise un calculateur d'investissement et d'optimisation fiscale. L'entreprise se fait pirater par un de ses concurrents les codes sources de sa solution. Le concurrent commercialise ensuite une solution identique sur la base des codes piratés. Le concurrent s'est abonné pendant 1 an à la solution proposée par l'entreprise victime du piratage et a profité de cet accès temporaire pour créer son propre calculateur.

**Intervention de l'assureur :** il accompagne l'entreprise assurée dans son recours contre le concurrent via un avocat spécialisé et un prestataire informatique qui détermine le modus operandi du concurrent et établit une note technique pour fonder le recours et trouver une solution transactionnelle avec le concurrent, ce qui permet d'éviter une procédure judiciaire dont la durée indéterminée serait préjudiciable pour l'entreprise assurée.

## Piratage du site internet pour détourner la clientèle :

Une entreprise propose des services de sensibilisation à la sécurité routière via un site internet. Le site internet de l'entreprise est piraté par un concurrent qui cherche à détourner sa clientèle de l'entreprise. Le concurrent a modifié / fait modifier les coordonnées figurant sur le site internet de l'entreprise, en remplaçant celles de l'assuré par les siennes (adresse mail notamment). Le piratage entraîne une baisse importante du chiffre d'affaires pour l'entreprise victime du piratage.

***Intervention de l'assureur :*** *L'assureur en cyber risques prend en charge les frais d'avocat et d'expertise informatique contre le concurrent auteur du piratage. A cela vient s'ajouter l'indemnisation versée par le concurrent négociée par l'assureur.*

**Piratage d'un hébergeur conduisant à la panne de sites internet :**

Une société d'infogérance et d'hébergement voit 5 des sites internet clients hébergés sur ses serveurs se faire pirater pendant 1 mois. Les dommages causés par le piratage sont multiples : pertes de données, baisses du chiffre d'affaires et préjudice d'image (e-réputation). Les sites internet victimes du piratage sont des sites e-commerce et des sites internet permettant à des sociétés de vendre leurs prestations de service. Ces derniers voient leur messagerie bloquée puis effacée ainsi que le contenu de leur site internet respectif modifié. La société d'infogérance subit une dégradation sérieuse de son image auprès de ses clients. L'expert en informatique et l'agence de communication de crise qui interviennent suite au piratage faisaient partie du panel de partenaires de l'assureur en cyber risques

***Intervention de l'assureur :*** *sur les conseils de l'assureur, les réclamations amiables ont été adressées par les clients à l'assuré, qui souhaitait rester leur point d'entrée dans le sinistre. Elles ont été gérées en collaboration entre l'assureur et le client (détermination de la position puis validation d'un projet de réponse).*

## Les enseignements à tirer

**L'expérience du service sinistre de l'assureur et l'accompagnement par des prestataires spécialisés** sont les facteurs clés de succès pour gérer les conséquences d'une attaque informatique : avocats, experts en cyber sécurité, agences de communication, société de monitoring des données.

**L'accompagnement de l'assureur et de ses prestataires** est l'un des facteur-clé du choix d'un courtier pour assurer au mieux son client. En ce qui concerne les cyber risques, il ne faut pas négliger l'expérience de l'assureur en matière de gestion des sinistres. Il faut prendre en compte également la qualité des prestataires qui entourent l'assureur.

**La solution transactionnelle avec les autres parties est privilégiée par les assureurs spécialisés** : cela permet d'écourter la durée du litige, de préserver sa relation commerciale avec des clients et d'obtenir plus rapidement une réparation ou une indemnisation du préjudice. La transaction en matière de ransomware est toutefois de plus en plus fréquemment abandonnée par les assureurs qui pourraient ainsi encourager le piratage informatique.

**La garantie contre le piratage de ligne téléphonique** ne fait pas partie de tous les contrats Cyber du marché. Elle peut être une option qu'il faut ajouter au contrat. Par exemple, les garanties contre la cyber-fraude et le piratage téléphonique sont incluses dans la délégation proposée par Maubourg Entreprise.

## Quelques définitions

**Vol de données :**

Accès non autorisé à des données, dans la plupart des cas, extraction ou copie des données du réseau de la victime. Cela peut aussi être le vol de disques durs externes appartenant à l'entreprise par exemple.

**Cyber extorsion** : Des cyber criminels encryptent les données/systèmes de leur victime (via un ransomware ou rançongiciel en français), menaçant de publier les données volées, prenant en otage les données/systèmes, etc. jusqu'à ce que leurs victimes satisfassent leurs demandes de rançon.

**Fraude par détournement de réglement :**

Cyber-criminels détournant des paiements vers un compte bancaire frauduleux.

**Email professionnel compromis :** Accès et contrôle non autorisé d'un compte email professionnel pouvant servir à des vols de données ou du détournement de fonds.

**Pour plus d'informations :**

- Courriel : info@maubourg-entreprise.fr
- Téléphone F : 01.42.85.80.00