La dénonciation des abus de ceux qui sont investis d'un pouvoir économique et politique a connu des formulations différentes au fil des époques et des continents.

Nous avons connus dans les années 1980 le phénomène de la criminalité financière en « COL BLANC» décrit par les sociologues comme une délinquance économique. Nous voyons apparaitre depuis les années 2000 une nouvelle catégorie de délinquants (souvent des jeunes génies de l'informatique) qui s'attaquent aux systèmes de l'information et de la communication des entreprises « LES HACKERS EN BASQUET» .

Nous sommes de plus en plus concernés :

Il n'a pas fallu attendre les évènements récents qui ont démarrés avec TV5 Monde et les différentes infractions constatées dans les sociétés de média pour se rendre compte d'une montée inquiétante de la cybercriminalité.

Si on constatait il y a quelques années des attaques isolées, dont l'objectif était seulement de démontrer leur capacité à entrer dans les systèmes, on observe désormais un véritable terrorisme informatique, en recherche de médiatisation, avec des utilisations frauduleuses de données ou des demandes de rançon, ciblant à la fois les entreprises et les organisations étatiques.

Inquiétude des Entrepreneurs

Il ressort d'une enquête de la FEB que 66% des entreprises interrogées n'ont pas une vision complète de toutes les implications d'une approche sérieuse et efficace de la sécurité cybernétique. Plus de 75% ne s'y retrouvent pas dans la réglementation et les instances compétentes. (Source : Communiqué de presse du CERT, Cyber Security Coalition — 20/10/2014).

En Belgique, le coût de la cybercriminalité est estimé à 3,5 milliards d'euros, soit plus de 1% du produit intérieur brut. Entre janvier et juin 2014, CERT.be a reçu plus de 751.000 notifications d'ordinateurs infectés en Belgique. L'équipe a également reçu, au cours du même semestre, en moyenne 614 avis d'incidents cybernétiques par mois, soit 80% de plus qu'en 2013.

Enfin, une étude publiée en 2015 par le Groupe Allianz démontre que les entreprises sont confrontées à un nombre croissant de scénarios perturbants et les Cyber-risques enregistrent la plus importante progression dans le classement.

Les risques de cyber-attaques et de pannes informatiques, poursuivant leur rapide progression dans le Baromètre des risques d'Allianz, comptent pour la première fois parmi les 5 facteurs de risques majeurs pour les entreprises à l'échelle mondiale (les cyber-risques occupaient la 8ème position en 2014 et la 15ème en 2013).

APPROCHE PREVENTION

Nous pensons avant tout que la solution pour les entreprises ne se trouve pas directement dans la mise en place d'un contrat d'assurance.

Nous estimons en effet que la conscientisation des chefs d'entreprise est un préalable avant toute autre forme d'intervention.

Pourquoi ?

- Méconnaissance, fausses croyances (« J'ai un antivirus je crains rien » , « pas de risque pour moi j'ai pas de site de e-commerce »,…)
- Peu de conscience des modes de contamination
- Simple clé usb infectée
- BYOD : Smartphones, tablettes perso utilisées au bureau sur l'infrastructure de l'entreprise
- PC portables utilisés en privé également et reconnectés au réseau
- E Mails et réseaux sociaux…

Notre bureau propose donc d'intervenir avec un consultant pour assurer un service de prévention et d'audit destiné à :

- Mettre en place des mesures de prévention simples et pouvant être appliquées par tout un chacun.
- Organiser une politique de sécurité et de bonnes pratiques (ex : politique gestion pwd, mises à jour, gestion des back up, cloud …)
- Organisation optimum de l'outil informatique :
- Matériel : firewall
- Logiciel : antivirus

APPROCHE ASSURANTIELLE

L'approche assurantielle doit être analysée sur l'ensemble des aspects liés aux risques encourus :

- Les Risques lié à la Responsabilité Civile : lorsque l'assuré est à l'origine de la transmission du problème (transmission virus – négligence dans le traitement de données – atteinte à la sécurité des réseaux etc …) les contrats RC Professionnelles New Generation (clauses IT étendues) couvrent globalement dans les limites habituelles du droit commun (exclusion des actes volontaires).
- Les Dommages au système (hardware) : généralement couvert par le contrat TRE / TRI (à clarifier et préciser l'étendue).

- Les risques liés à l'accompagnement dans la gestion et la maitrise des impacts d'un Cyber-risque tout en permettant la continuité de l'activité de l'entreprise.

VOICI le véritable enjeu qui combine à la fois un produit d'assurance classique, un outil de gestion des risques et un accès à un réseau d'experts indépendants.

Gestion de crise	✓ Coûts des experts chargés de déterminer si une atteinte aux données s'est produite et identifier la cause ✓ Coûts des experts chargés de remettre en marché les systèmes et de restaurer les pare-feux pour faciliter le retour à la normale suite aux violations de la sécurité ; ✓ Coûts de notification aux clients victimes y compris les frais de collecte d'information ✓ Honoraires des experts chargés d'évaluer les possibilités de récupération ou de reconstitution de données ; ✓ Honoraires d'experts chargés de minimiser les conséquences médiatiques ou des atteintes à la réputation.
Garanties civiles	✓ Frais de défense lorsque l'entreprise est victime d'un vol de codes d'accès ; ✓ Frais de défense si l'entreprise est victime d'un vol de matériel contenant des données personnelles ; ✓ Frais de défense si un employé de l'entreprise divulgue des données confidentielles.
Enquêtes et sanctions	✓ Frais de conseil et de représentation juridique dans le cadre d'une enquête liée à la compromission de données personnelles ; ✓ Amendes et pénalités assurables imposées par des autorités de protection des données personnelles

Caractéristiques intrinsèques du produit d'assurance :

L'objectif à atteindre est de convaincre un assureur de proposer une solution de protection plus proche d'un service d'assistance que d'un contrat de dommage classique.

C'est-à-dire :

- Un module de gestion de crise couvrant les frais de consultants ;
- Une perte d'exploitation liée à l'interruption d'un réseau ou à des services de cloud-computing.

Cette approche nécessite pour l'assureur de s'entourer :

1. De conseillers juridiques ;
2. D'experts en informatique ;
3. D'experts en communication de crise ;
4. D'experts comptables pour le volet perte d'exploitation.

SOLUTION RETENUE

Suite à la consultation du marché nous avons retenu un contrat proposant cette nouvelle approche :

Garanties proposées :

Gestion d'un évènement assuré

Mesures d'urgence

Frais d'enquêtes administratives

Responsabilité

Frais d'interruption de réseau

Responsabilité Multimédia

Extorsion Cybernétique

Vol Cybernétique

Piratage du système téléphonique

Capitaux assurés :

3 options sont retenues :

Option 1 : 500.000 € par évènement

Option 2 : 1.000.000 € par évènement

Option 3 : 2.000.000 € par évènement

Garanties assurées	*Sous-Limites*	*Franchises*
Gestion d'un évènement assuré	*500.000 €*	*2.500 €*
Mesures d'urgence	*48 heures*	*Pas de franchise*
Enquête administrative	*500.000 €*	*2.500 €*
Amendes Administratives	*500.000 €*	*2.500 €*
Interruption de réseau	*50 % du montant assuré*	*8 heures*
Responsabilité Multimédia	*50 % du montant assuré*	*2.500 €*
Extorsion Cybernétique	*50 % du montant assuré*	*2.500 €*
Vol Cybernétique	*100.000 €*	*2.500 €*
Piratage du système téléphonique	*100.000 €*	*2.500 €*

Calcul des Primes :

Les primes sont calculées en fonction de plusieurs critères liés à la taille de l'entreprise (Chiffre d'affaire) et le secteur d'activité.

Notre bureau se tient à la disposition des gérants d'entreprise pour rédiger une proposition chiffrée.

Conditions d'assurabilité :

Remplir un questionnaire type (voir annexe)

Remplir une simple déclaration de non sinistralité

Fait à Wavre le 20 octobre 2015

Maxel sa

Baudouin Poncelet

Baudouin.poncelet@maxel.be