

Les cyber-risques, tout le monde en parle enfin !

Internet

Posté par : JerryG

Publié le : 4/4/2012 14:00:00

Comme tous les "nouveaux " risques, il aura fallu du temps pour **prendre la mesure des dangers**, d'autant plus que nous avons tous le sentiment que l'informatique et Internet font partie de notre vie personnelle et économique depuis toujours.

De ce fait, nous sommes plus sensibles à leurs avantages qu'aux risques de plus en plus importants auxquels ils nous exposent.

Plus aucune entreprise, quelle que soit sa taille, ne peut plus envisager de fonctionner sans Internet, encore moins sans informatique. Le retour en arrière est impossible, c'est pourquoi il est indispensable de bien appréhender les risques qui accompagnent ces nouvelles technologies pour les maîtriser, nous confie **Dominique d'ACHON**, Directeur Commercial de Cyberprotect

En réalité les cyber-risques sont nouveaux dans leurs formes et leur origine mais pas dans leurs conséquences qui demeurent très traditionnelles:



- risques de dommages:

Le plus important reste celui de l'arrêt d'activité, partiel ou total, qui se traduit en Pertes d'Exploitation ou Frais Supplémentaires d'exploitation. Ce sont aussi les frais de décontamination du matériel, les frais de reconstitution des médias, le vol de fichiers...autant de garanties "classiques" mais qui ne fonctionnent pas dans les cas de sinistres découlant de la cybercriminalité !

- risques de Responsabilité Civile:

La transmission de ver ou de virus, vol de données confiées (ou hébergées) par des tiers : clients, fournisseurs, sous-traitants, salariés..., prise de contrôle à distance du réseau informatique de l'entreprise (botnet) ...

- risques d'atteinte à l'image, risques d'extorsion... :

Même sans additionner les conséquences financières qui découlent de ces événements, on réalise l'impact dramatique qu'ils peuvent avoir sur l'entreprise et sa survie. Le sinistre SONY en est une parfaite illustration !

Pourtant les cyber-risques ne sont pas une fatalité. On peut désormais les gérer au même titre que les autres en appliquant les mêmes méthodes.

- prise de conscience, évaluation du risque
- prévention, réduction du risque
- traitement du risque résiduel, transfert, achat de garanties financières

1) La prise de conscience

C'est comme toujours, la phase la plus importante. Beaucoup de chefs d'entreprise sont encore sceptiques: "il ne m'est jamais rien arrivé", "je suis trop petit pour que l'on s'intéresse à moi !", "j'ai une sécurité informatique très efficace"...

Ces réactions ne sont pas anormales, car la cybercriminalité, qui est le risque majeur des cyber-risques, est de plus en plus sournoise. En effet, on peut en être victime sans le savoir. Ainsi la provocation ludique des premiers "hackers" s'est transformée en véritable business très lucratif. Il s'agit désormais de voler des données pour les revendre, de contrats passés contre des concurrents, d'espionnage industriel... il est donc essentiel d'agir sans être vu, ni pris !

2) La prévention

Elle est possible mais encore trop souvent assimilée à la seule sécurité informatique. La sécurité informatique est indispensable mais plus suffisante. Il faut en contrôler l'efficacité pour l'adapter et la faire évoluer, à l'identique de ce que l'on fait pour les systèmes de sécurité des biens matériels: télé-surveillance, alarme, alerte...

Les comportements à risque: ils sont à l'origine de plus de 50% des sinistres et souvent sans qu'il y ait d'intention malveillante. Il faut informer, sensibiliser, former les utilisateurs. Il faut savoir qu'une sécurité informatique très stricte, si elle limite les risques de malveillance interne et externe, restreint les possibilités d'action des utilisateurs et conduit assez souvent au développement de systèmes parallèles mis en place par ces mêmes utilisateurs pour contourner les restrictions d'utilisation du réseau informatique. Ces pratiques, de bonne foi, exposent gravement l'entreprise qui considère avoir pris les mesures adéquates à sa sécurité informatique.

3) Le transfert du risque résiduel.

Au même titre que pour les risques traditionnels tels que l'incendie, le vol, la responsabilité civile, la prévention des cyber-risques permet de les réduire significativement. Le risque résiduel devient donc transférable, donc assurable.

2011 a été une année riche en sinistres liés à la cybercriminalité. Les médias ont largement évoqué ceux touchant les grandes entreprises (Sony) ou les organisations étatiques (Bercy) mais le tournement d'un réseau téléphonique, le vol de données confidentielles, le tournement de flux financiers... dont les PME, les TPE, les professions réglementées sont de plus en plus fréquemment victimes, ont des conséquences dramatiques pour elles et sont moins connus.

La médiatisation a néanmoins favorisé la prise de conscience des dangers liés à ces

nouvelles technologies et l'Émergence de solutions.

Il est désormais possible de faire surveiller son réseau informatique comme on fait surveiller ses locaux et d'intervenir en temps réel pour se protéger des malveillances détectées. Il est également devenu possible de s'assurer contre les conséquences financières de ces intrusions et malveillances.

Plusieurs assureurs proposent depuis peu des contrats spécifiques pour garantir les cyber-risques. Cependant tant la nature des garanties, que leur montant et les primes sont très dépendants du niveau de prévention mis en place par l'entreprise.

Il y a donc encore de grandes marges de progrès mais la route est ouverte.