Couvrir les cyber-risques : utile ou indispensable ?

Peut-on encore se permettre de ne pas assurer les cyber-risques ?

Personne n'imaginerait vivre sans une assurance R.C. Familiale. Toutefois, la vaste majorité des entreprises, surtout de petite et moyenne taille, ne couvrent pas de manière adéquate les risques informatiques auxquels elles sont exposées. Une certaine forme d'inconscience (« *ma petite entreprise n'est pas susceptible d'intéresser les cybercriminels* ») mais surtout une méconnaissance des risques peuvent expliquer ce constat. Les petites entreprises ont parfois des systèmes de sécurité moins performants et ne disposent pas de plans éprouvés de réaction vis-à-vis des incidents. Elles sont dès lors des proies faciles.

De l'assurance tous risques aux cyber-risques.

Bien entendu, nombre d'entre elles ont souscrit une assurance tous risques pour couvrir les dommages à leurs équipements informatiques. Pour nécessaire qu'elle soit, pareille couverture est insuffisante eu égard à l'explosion des nouvelles formes de cyber-risques. La « tous risques électroniques » classique couvre généralement les sinistres d'origine accidentelle (incendie, dégâts des eaux, vol, etc.). Toutefois, les sinistres résultant d'erreurs humaines ou d'attaques malveillantes ne sont en principe pas couverts. Même en ce qui concerne les risques accidentels, on constate que les dommages indirects (pertes d'exploitation, frais supplémentaires, frais de reconstitution de données, frais de remise en état de fonctionnement normal des systèmes, etc.) représentent le plus souvent un multiple important des seuls dommages matériels. Or, ces garanties sont souvent négligées lors de la souscription des contrats.

Puisque le paysage informatique a changé …

Le paysage informatique évolue à une vitesse si rapide que maintes entreprises et surtout leurs responsables ont du mal à la suivre. Les informaticiens recourent sans cesse à de nouvelles technologies, qui induisent des risques inconnus jusqu'alors. Le cloud computing, les technologies mobiles (smartphones, tablettes, etc.), la *dématérialisation croissante des activités* n'en sont qu'un exemple. La dépendance des entreprises de leurs systèmes informatiques ne cesse d'augmenter, de même que les conséquences d'une neutralisation de ceux-ci. Chaque dirigeant se doit de se poser, pour chacune de ses applications informatiques, la question simple suivante : quelles seraient les conséquences pour mon entreprise si cette application était indisponible une heure, un jour, une semaine, voire un mois ? Pour certains systèmes critiques, notamment industriels, une indisponibilité de quelques minutes peut déjà avoir des effets dramatiques.

Vers de nouvelles préoccupations.

Les nouvelles formes de cybercriminalité sont une source de préoccupation inquiétante : collecte de données bancaires et d'autres données confidentielles, détournements de fonds, cyber extorsion, injection de logiciels malveillants, neutralisation de sites de commerce électroniques via des attaques de déni de service, vols de matériels et de données, etc.

L'erreur humaine n'est aucunement à négliger : perte de matériels, transmission de données erronées, hameçonnage (phishing) qui peut résulter en un détournement de paiements bancaires ou en une intrusion dans le système, introduction malheureuse d'une clef USB infectée, etc.

Lorsqu'un sinistre se produit, les coûts des prestations indispensables peuvent s'avérer fort élevés : intervention de techniciens spécialisés pour restaurer les données et les logiciels et remettre le système informatique en état normal de fonctionnement, coût d'experts pour investiguer les causes et conséquences de l'incident, frais de notification éventuels à une grande quantité de personnes dont les données auraient été dérobées, frais de conseillers juridiques, etc.

Un sinistre peut avoir des conséquences très dommageables sur la réputation et l'image de marque de l'entreprise. Dès lors, il est nécessaire dans bien des cas de recourir à des conseillers en relations publiques pour gérer la communication de crise et tenter de minimiser les effets dommageables sur l'image de l'entreprise.

Des conséquences dommageables, diriez-vous ?

Un sinistre peut aussi avoir des effets dommageables pour des tiers, impliquant ainsi la responsabilité civile de l'entreprise qui en est la cause.
Après la longue période de frilosité dans le prolongement des attentats du 11 septembre 2001, un certain nombre de compagnies d'assurances ont mis au point des couvertures permettant de répondre aux préoccupations susmentionnées.

Si les géants du courtage disposent en leur sein de départements spécialisés en matière d'assurances de risques informatiques, il n'en va pas de même dans les cabinets de courtage de plus petite taille, où le besoin d'information et de formation est souvent criant.

La gestion des risques informatiques commence par une analyse approfondie des risques auxquels l'entreprise est potentiellement exposée. Ensuite, il conviendra de prendre les mesures de protection les plus appropriées pour les traiter. Enfin, cela débouchera sur l'identification des risques qu'il convient de transférer à l'assurance pour financer les coûts des conséquences d'un sinistre.
Il importe que les courtiers soient à même de comprendre la problématiques des risques informatiques de leurs clients et de leur proposer les couvertures les plus adéquates pour répondre à leurs besoins.

Ir. Luc GOLVERS,
Expert judiciaire en informatique.
Président du Club de la Sécurité Informatique Belge. luc.golvers@skynet.be

Partner du CEPOM

Pour en savoir plus

N'hésitez pas à nous communiquer votre intérêt (vos remarques et commentaires constructifs nous intéressent) en cliquant pour le moment sur http://www.cepom.be/contact/

Pour tous renseignements

Véronique Lagae – Coordinatrice de formation
Tél : +32 2 721 82 77 ou veronique.lagae@cepom.be