NOTE D'INFORMATION DU PARTENARIAT RISK DOCTOR

# LE MANAGEMENT DU RISQUE DE LA CYBERCRIMINALITÉ

***© May 2014, Ben Rendle***

*ben.rendle@rioscaconsulting.co.uk*

La cybercriminalité présente une menace croissante pour l'économie mondiale. Elle est, par contre, mal définie et souvent confondue avec la guerre cybernétique ou le cyber-terrorisme. Comme professionnels du risque nous avons besoin de comprendre la cybercriminalité et le rôle du management du risque car nous pouvons fournir une aide précieuse pour contrecarrer cette menace significative pour le commerce et pour la société.

Certains professionnels du risque ont l'impression que la cybercriminalité ne concerne que le personnel technique et qu'il devrait être traité par le département informatique. Au contraire, la cybercriminalité représente un risque à l'organisation toute entière car elle a une influence sur sa capacité à atteindre ses objectifs stratégiques et opérationnels. Malheureusement, beaucoup d'organisations ne savent pas de quoi la cybercriminalité a l'air, ni la probabilité d'en être victimes, ni l'amplitude de l'impact, ni la meilleur façon d'y répondre.

La cybercriminalité peut avoir de nombreux type d'impacts sur l'organisation, parmi lesquels :

- le vol ou la fraude en ligne
- le vol d'identité
- l'extorsion
- le vol de données clients
- le vol de propriété intellectuelle
- l'espionnage industriel

Le degré d'exposition à la cybercriminalité dépend du niveau d'activité en ligne pratiquée par une organisation, ainsi que de l'étendue de sa présence en ligne, de l'ampleur des actifs et des informations précieuses stockées en ligne, de l'efficacité de sa sécurité électronique et du degré de conscience du risque dans la culture de l'organisation.

Pour pouvoir gérer le risque de la cybercriminalité, nous devons d'abord identifier le niveau de nos activités en ligne et déterminer lesquels des actifs et des activités pourraient souffrir de la cybercriminalité. Nous pourrons alors commencer à évaluer et à gérer nous risques de la cybercriminalité. Les étapes suivantes y-contribueront :

- **Comprendre et définir clairement les objectifs opérationnels des activités en ligne**. Il faut également prendre en compte les environnements variés et spécifiques de nos parties prenantes et évaluer leur appétit pour le risque en ligne.
- **Répondre aussi bien aux facteurs culturels que techniques.** Ceux-ci comprennent les barrières culturelles, les difficultés de communication et les effets de partis-pris sur la façon de percevoir le risque de la cybercriminalité.
- **Reconnaitre aussi bien les menaces internes que les menaces externes de cybercriminalité.** Les menaces internes peuvent provenir d'erreurs du personnel, de la perte accidentelle de données ou des fuites par malveillance de données sensibles de l'entreprise. Les menaces externes peuvent venir de pirates, de groupes de pression, de concurrents, même de gouvernements étrangers hostiles, ainsi que de virus, de vers, de chevaux de Troie, etc.
- **Définir le propriétaire, les responsables et des méthodes d'incitation à affronter les risques de la cybercriminalité.** Tous les cadres supérieurs devront être garants de la gestion des risques de la cybercriminalité dans leur domaine de responsabilité, et nous devons demander des comptes aux parties prenantes qui considèrent que « ce n'est pas mon problème ».
- **Gérer les risques de la cybercriminalité dans le cadre de la gestion du risque de l'entreprise.** Les risques de la cybercriminalité peuvent avoir un effet sur l'entreprise dans son ensemble dans des domaines tels que la réputation, le maintien des opérations, et les effets secondaires sur les filiales et sur les fournisseurs ; ils doivent donc être gérés d'une façon cohérente, intégrée à notre réponse globale au risque.
- **Développer une vue globale sur les impacts des risques de la cybercriminalité.** Beaucoup d'entreprises dépendent d'économies d'outre-mer pour le commerce et les exportations, et pour générer de la richesse. Ceci les rend vulnérables à des risques de cybercriminalité étrangère qui doivent être pris en compte.

En tant que professionnels, nous devons intégrer la cybercriminalité à notre façon de penser et de travailler, pour pouvoir offrir des conseils pratiques et ciblés à nos organisations dans le but de réduire les menaces et protéger notre entreprise.