OPTIMUM®
Assurance générale

“ Protéger nos assurés et leurs actifs avec des solutions créatives et sur mesure ”

# Capsule de prévention

## Cyber Sécurité – L’importance de la vigilance et de la protection des données en entreprise

Même si la plupart des entreprises possèdent des systèmes de sécurité pour leurs réseaux informatiques depuis un certain temps, il n’est jamais superflu de sensibiliser vos équipes internes aux nombreux risques liés à la cybersécurité. Une simple négligence peut fortement salir votre image publique et teinter vos liens de confiance professionnels à long terme.

Limitez les ravages d’une violation de données ou d’une attaque informatique dans votre entreprise en adoptant les mesures préventives appropriées.

### Distinctions des termes reliés à la cyber sécurité

**Violation de données**

Que représente exactement une violation de données? C’est l’exposition non autorisée d’informations permettant d’identifier une personne.

**Attaque informatique**

Une attaque informatique (ou cyberattaque) quant à elle se manifeste soit par une personne non autorisée ayant accès au système informatique, par une personne autorisée qui accède au système informatique à des fins non autorisées, par une attaque par logiciel malveillant, ou encore par une attaque par déni de service (DDS).

**Voici différents conseils de prévention qui contribueront à réduire les risques de cyberattaques dans tous types d’entreprises :**

- Avant toute chose, assurez-vous d’avoir mis sur pied une équipe spécialisée et désigné un ou des responsables dument responsabilisés pour la gestion d’un département ou d’une équipe de sécurité et de prévention, **ainsi qu’une équipe de gestion des risques**. En ligne avec la montée graduelle des besoins technologiques de votre entreprise, cette équipe devrait s’agrandir logiquement au fil du temps.
- Outre cette même équipe responsable, il sera important d’offrir plusieurs formations et une sensibilisation continue à tous vos employés. Une vigilance collective est fortement recommandée en tout temps.
- Gestion de risque des tiers : si vos réseaux ou vos systèmes sont gérés par des tiers, il est recommandé d'évaluer leur approche stratégique face à la sécurité de vos données, **ainsi que leurs protocoles TI en lien direct avec la sécurité informatique**.
- Prioriser les mises à jour de vos systèmes de sécurité, **ainsi que les mises à jour des différents logiciels utilisés**.
- La création et **communication à l’interne** d’un plan d’intervention avec plusieurs scénarios permettra une gestion de crise optimale. Une situation fâcheuse peut facilement désorienter notre jugement et nous amener à être réactifs lors de décisions importantes. Avec un plan, vous aborderez vos décisions et votre gestion avec calme et stratégie.
- Souscrire à une assurance cyber afin de protéger ses biens, ressources et données confidentielles. Les coûts de rétablissement sont considérables lorsqu’une entreprise se remet d’une cyberattaque. Il faut également penser aux éléments suivants :
  - La gestion de l’image de marque et ses coûts, principalement liés aux relations publiques ;
  - Les envois massifs aux personnes touchées et autres communications connexes **prescrits par la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)** ;
  - L’enquête judiciaire et toutes autres dépenses juridiques associées **telles que les amendes ou pénalités imposées dans la mesure où elles sont légalement assurables suivant la législation provinciale ou fédérale applicable**.

**Pour plus de détails au sujet des produits d’assurance cyber offerts par Optimum Assurance générale, visitez notre site internet www.optimum-general.com**

optimum-general.com
optimum-general.com/linkedin

2022-03