Autoévaluation des cyberrisques

Les questions d'autoévaluation ci-après proposent une liste de bonnes pratiques en matière de cybersécurité. Elles vous aideront dans votre démarche de détermination des risques et d'évaluation des mesures en place pour prévenir, gérer et atténuer ceux-ci en cas d'incident. Cette évaluation devrait être effectuée de manière périodique.

Prémisse

Une analyse des menaces et des risques liés à la cybersécurité a-t-elle déjà été effectuée auparavant? ☐ Oui ☐ Non

Si oui, quand?

La situation a-t-elle évolué depuis la dernière analyse (activités exercées, systèmes utilisés, fournisseurs, etc.)? ☐ Oui ☐ Non

Les risques et menaces constatés sont-ils classés en ordre de priorité et font-ils l'objet d'un suivi afin que l'on puisse en atténuer la portée? ☐ Oui ☐ Non

Gouvernance

☐ Les politiques et procédures contiennent-elles un volet sur la cybersécurité?

Les politiques et procédures couvrent-elles les points suivants :

- ☐ Vol, perte ou bris d'appareils;
- ☐ Données non disponibles;
- ☐ Atteinte à la protection des renseignements;
- ☐ Vulnérabilité ou faille de sécurité;
- ☐ Échanges d'information;
- ☐ Appareils mobiles.

☐ Un plan de continuité d'activité a-t-il été élaboré?

☐ Un membre du personnel est-il responsable de la cybersécurité?

☐ Les personnes-ressources en matière de cybersécurité ont-elles les compétences requises pour évaluer les risques et mettre en place les mesures nécessaires? La direction ou le conseil d'administration sont-ils impliqués dans les processus liés à la cybersécurité?

☐ Un processus de destruction permanente des renseignements détenus sur des supports électroniques est-il prévu?

☐ Une formation axée sur la cybersécurité est-elle disponible et fréquemment mise à jour?

☐ Le personnel reçoit-il des directives pour travailler de façon sécuritaire au cours de ses déplacements professionnels?

Sécurité des technologies de l'information

- ☐ Un inventaire exhaustif des données détenues a-t-il été effectué? Les données ainsi répertoriées ont-elles été catégorisées selon leur degré de sensibilité?
- ☐ Le réseau sans fil est-il sécurisé?
- ☐ Une liste des appareils et des utilisateurs autorisés à se brancher au réseau est-elle disponible?
- ☐ Un processus de gestion des accès aux ressources informatiques a-t-il été mis en place (ex. : révision de la période des octrois, lors de changement de fonction, départ, etc.)?
- ☐ Quels moyens de transmission sécurisés sont-ils utilisés pour transmettre des informations confidentielles par courriel?
- ☐ Des outils de filtrage ou de blocage des pourriels, un pare-feu et une protection contre les logiciels malveillants sont-ils en place?
- ☐ Le parc informatique est-il mis à jour en temps opportun? Un processus de gestion des vulnérabilités est-il en place?
- ☐ Les accès aux locaux, aux serveurs et à l'équipement informatique sont-ils sécurisés?
- ☐ Les données sont-elles sauvegardées régulièrement?
- ☐ Des tests de restauration des données sont-ils effectués?
- ☐ L'organisation possède-t-elle une politique de gestion des mots de passe axée sur les bonnes pratiques?

Relation avec des tiers

- ☐ Les tierces parties sont-elles fiables en matière de cybersécurité (certification)? La réputation de l'entreprise est-elle validée, notamment au moyen de vérifications de références, de recherches sur le Web, etc.?

  Les ententes conclues prévoient-elles :

  - ☐ l'obligation du fournisseur de divulguer les incidents?
  - ☐ des clauses permettant d'assurer une pérennité des données ainsi que l'accessibilité ou le transfert des données dans le cas, par exemple, d'une terminaison du contrat dans le cadre duquel les données sont hébergées chez le fournisseur?
- ☐ Dans le cas où des services infonuagiques pour l'hébergement de ses données sont utilisés, l'emplacement des serveurs permettant le stockage des données est-il connu?
- ☐ Les limites de responsabilité du fournisseur de services en matière de confidentialité de l'information et de protection des renseignements personnels sont-elles connues?

Assurance

- ☐ Une assurance cyberrisque a-t-elle été souscrite?
- ☐ Si oui, que couvre-t-elle? Est-elle adaptée aux risques constatés et aux activités exercées?