OSLER

Problèmes liés à la gouvernance d’entreprise et aux données

29 MAI 2017 1 MIN DE LECTURE

Expertises Connexes

- Cybersécurité et intervention en cas d’incident lié à la sécurité
- Services professionnels

Auteurs(trice): Lawrence E. Ritchie, Lauren Tomasich

Dans une ère où il ne s’agit pas de savoir si un incident lié à la sécurité des données surviendra, mais plutôt de savoir quand il surviendra, les conseils d'administration sont sous pression pour faire de la sécurité des données une priorité majeure. Une stratégie de cybersécurité doit être mise en place pour établir la priorité des données critiques et des systèmes d'information de l’organisation et les protéger, et pour gérer le risque associé aux incidents liés à la sécurité des données. Le résumé graphique qui suit donne un aperçu de ce à quoi votre stratégie de cybersécurité devrait ressembler.

Votre stratégie de cybersécurité

Votre stratégie de cybersécurité doit :

- attribuer les ***rôles et les responsabilités*** aux différents groupes au sein de votre organisation;
- ***coordonner et intégrer*** les activités collectives aux fins de protection contre les lacunes en matière de sécurité;
- faire en sorte que ces groupes aient à ***rendre des comptes*** quant à leurs responsabilités.

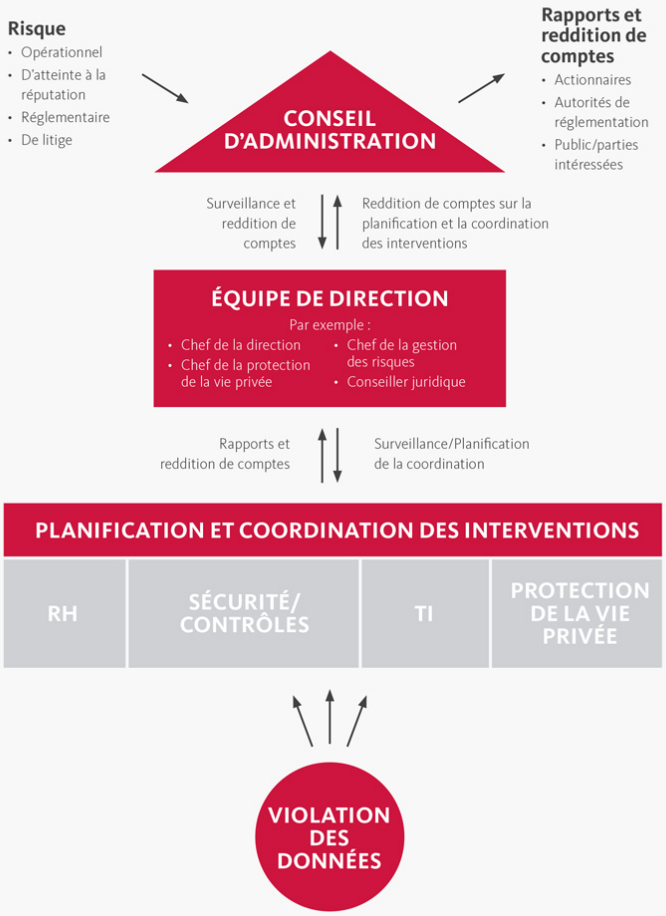
La stratégie de cybersécurité doit comprendre un plan d'intervention évolutif en cas d'atteinte à la protection des données, de façon que la société soit ***prête à intervenir***, et pas seulement préparée à un incident de cette nature. Votre plan doit également fournir le cadre nécessaire à la mise en œuvre d'une intervention coordonnée et intégrée en cas de violation des données.

Il incombe au conseil d'administration de votre société de surveiller la mise en œuvre de la stratégie de cybersécurité de votre entreprise, y compris son plan d'intervention en cas de violation des données; le conseil devrait recevoir ***des rapports*** périodiques sur l'intégrité des données et des systèmes d'information de l'entreprise, ainsi que sur les risques connexes.

Questions auxquelles le conseiller juridique devrait être prêt à répondre lorsqu'il fournit des avis au conseil d'administration :

- ☑ Quelle est la tolérance au risque de la société?
- ☑ Quelles sources de risque lié à la cybersécurité sont applicables à la société? Un contrôle préalable adéquat a-t-il été effectué pour évaluer le risque?
- ☑ Quels sont les actifs, l'information et les données qui sont vulnérables?
- ☑ Qui est responsable de la sécurité des données au sein de la société?
- ☑ La société a-t-elle une stratégie de cybersécurité coordonnée et intégrée? Les cloisonnements ont-ils été éliminés de la gestion de la stratégie et du plan d'intervention en cas d'atteinte à la sécurité des données? Les membres du personnel se sont-ils fait attribuer les responsabilités appropriées et ont-ils des comptes à rendre à l'égard de leurs responsabilités?
- ☑ Les incidents relatifs à la sécurité et le coût des interventions font-ils l'objet d'évaluations?
- ☑ Les politiques sur la sécurité, la sensibilité de l'information et l'éthique ont-elles été documentées et communiquées au sein de l'organisation?
- ☑ Les initiatives en matière de sécurité reçoivent-elles un financement adéquat compte tenu de la tolérance au risque de la société?
- ☑ Y a-t-il un plan en place pour évaluer en permanence l'efficacité du programme relatif au cyberrisque?
- ☑ Comment les initiatives de l'organisation en matière de sécurité seront-elles divulguées?

Cadre de la surveillance par le conseil, de la reddition de comptes et de la coordination au sein de l'entreprise



Télécharger l'infographique