Questions-clés pour la Gouvernance

Cybersécurité : quel rôle pour le Conseil d'Administration ?

KPMG Board Leadership Center

Les dirigeants des entreprises et les membres de conseil d'administration ont compris depuis plusieurs années que des cyberattaques pouvaient entraîner des dommages très significatifs pour les entreprises.

Exemples d'impacts :

- **Divulgation d'informations confidentielles** (R&D, stratégie, M&A…)
- **Atteinte à la réputation**
- **Pertes d'exploitation, pertes de commandes, pertes de parts de marché**
- **Perte de confiance par les clients et les partenaires**
- **Incapacité à délivrer des services aux métiers ou aux clients**
- **Incapacité à produire des biens**
- **Non-respect d'engagements contractuels**
- **Sanctions sous forme d'amendes légales ou réglementaires**

A ces impacts s'ajoutent les **coûts de gestion de crise** et de **remise en état** en cas de cyberattaque.

En outre, le sujet de la cybersécurité n'est plus confiné aux limites de l'entreprise, et les impacts d'une cyberattaque pour une entreprise peuvent se faire sentir chez ses clients, B2B ou particuliers, ou ses partenaires. Au-delà des impacts opérationnels, une cyber attaque peut entraîner des atteintes fortes à l'image de l'entreprise. Les régulateurs, les clients, les investisseurs ont tous des **attentes élevées concernant la capacité des entreprises à résister à des cyberattaques**.

Il est donc tout à fait justifié que les conseils d'administration se saisissent du sujet de la cybersécurité.

> « les administrateurs sont aujourd'hui des acteurs à part entière dans la lutte contre les cyber menaces.

Vincent Maret
Associé Cybersécurité,
Connected Tech,
KPMG France

Le conseil d'administration doit s'assurer que l'entreprise a identifié les risques cyber qui menacent l'entreprise et mis en place un dispositif permettant de réduire ces risques.

- Cartographie des actifs critiques de l'entreprise et des cyber menaces qui peuvent les affecter.
- Cartographie des lois et règlements cybersécurité qui concernent l'entreprise dans le monde.
- Programme cyber décrivant les actions et projets à 3-5 ans permettant de réduire les risques et de se conformer aux réglementations.
- Ressources et budgets dédiés et suffisants.
- Prise en compte de la cybersécurité dans les projets de transformation, le développement de nos nouveaux produits et services, les projets de croissance externe, les partenariats et sous-traitances.
- Implication du senior management et des équipes opérationnelles dans le dispositif de cybersécurité.
- Formation et sensibilisation du personnel.

Le conseil doit également s'assurer que des **plans de contrôle sont en place** pour vérifier l'efficacité du dispositif cyber, et que des **plans de gestion de crise existent**, au cas où un cyber attaquant réussirait à percer les lignes de défense.

Face à un sujet parfois technique et incompréhensible pour des non spécialistes, les administrateurs doivent s'assurer qu'ils **obtiennent les bonnes réponses à leurs questions**. Ils doivent être en mesure de challenger efficacement le dispositif en place. Dans certaines entreprises, le responsable cybersécurité assure une séance d' « onboarding » des nouveaux administrateurs. Dans d'autres, le conseil se fait assister par des spécialistes cyber. D'autres enfin créent des comités spécialisés.

Questions à se poser pour les administrateurs

- La cartographie des risques cyber est-elle à jour ?
- Une programme de cybersécurité est-il défini, et est-il en mesure de maîtriser les risques cyber aujourd'hui et demain ?
- Sommes-nous conformes aux lois et règlements en matière de cybersécurité ?
- La cybersécurité est-elle prise en compte dans les processus métiers ?
- Le dispositif de protection contre les cyber menaces est-il adapté ?
- L'efficacité du dispositif cyber est-elle régulièrement évaluée ? Les points de faiblesses sont-ils connus ?
- Les ressources (budget, humains, outils) affectées à la cybersécurité sont-elles suffisantes ?
- Les investissements en cybersécurité sont-ils efficaces ?
- Est-ce que certains de nos partenaires dans la chaîne d'approvisionnement présentent un risque pour nous ?
- Sommes-nous en mesure de réagir efficacement en cas de cyber attaque ?
- Quel est notre degré de résilience face aux attaques cyber ?
- Avons-nous une vision de notre maturité cyber au regard de ceux de nos pairs ?
- Est-ce que les indicateurs qui nous sont remontés sont pertinents ?

Nous contacter

Jean-Marc Discours
Associé, Président du BLC France
KPMG
+33 1 55 68 68 83
jdiscours@kpmg.fr

Vincent Maret
Associé Cybersécurité, Connected Tech
KPMG
+33 1 55 68 26 64
vmaret@kpmg.fr

Site : home.kpmg/fr/board-leadership-center
E-mail : fr-kpmgblc@kpmg.fr