Renforcement des capacités de cyber-sécurité Boîte à outils pour les organisations financières

Guide au niveau du conseil : encadrement de la cyber-sécurité

Principes fondamentaux de la gouvernance des cyber-risques

Confirmez que vous pouvez répondre positivement aux questions suivantes :

1. Votre organisation **a-t-elle satisfait aux exigences légales et réglementaires pertinentes**?

2. Votre organisation **a-t-elle quantifié ses cyber-expositions et testé sa résilience financière?**

3. Votre organisation a-t-elle un **plan d'amélioration** en place pour garantir que les expositions s'inscrivent dans votre appétit au risque convenu?

4. Le conseil **discute-t-il régulièrement des informations concises, claires et exploitables relatives à la cyber-résilience de l'organisation et fournies par la direction**?

5. Votre organisation a-t-elle **des plans de réponse aux incidents en place qui ont récemment été testés**, y compris au niveau du conseil?

6. Les **rôles des personnes clés responsables de la gestion des cyber-risques** sont-ils clairs et alignés sur les trois lignes de défense?

7. Avez-vous obtenu **une validation et une assurance indépendantes** de la posture de cyber-sécurité de votre organisation?

Supervision

Au niveau le plus élevé de la direction de votre organisation, le conseil d'administration assume la responsabilité ultime de la gestion des cyber-risques et doit donc superviser la stratégie, les politiques et les activités de l'organisation dans ce domaine. Plus précisément, le conseil doit :

⇒ Assumer la responsabilité ultime de la supervision des cyber-risques et de la résilience, que ce soit en tant que conseil complet ou par délégation de supervision à un comité du conseil spécifique.
⇒ Assigner à un responsable de l'entreprise, généralement le RSSI, la responsabilité de signaler la capacité de votre organisation à gérer la cyber-résilience et les progrès dans la mise en œuvre des objectifs de cyber-résilience. S'assurer que ce responsable dispose d'un accès régulier au conseil d'administration, d'une autorité suffisante, de la maîtrise du sujet, de l'expérience et des ressources pour remplir ces obligations.
⇒ Définir annuellement la tolérance au risque de votre organisation ; assurer la cohérence avec votre stratégie d'entreprise et l'appétit au risque.
⇒ S'assurer qu'un examen formel et indépendant de la cyber-résilience de votre organisation est effectué chaque année.
⇒ Superviser la création, la mise en œuvre, les tests et l'amélioration continue des plans de cyber-résilience, en s'assurant que l'ensemble de votre organisation est aligné et que votre RSSI ou autre cadre responsable les signale régulièrement au conseil d'administration.
⇒ Intégrer la cyber-résilience et l'évaluation des risques dans la stratégie commerciale globale de votre organisation, la gestion des risques, la budgétisation et l'allocation des ressources, dans le but d'intégrer pleinement les cyber-risques au risque opérationnel global.
⇒ Passer régulièrement en revue vos performances pour ce qui précède et tenir compte des conseils indépendants pour une amélioration continue.

Rester informé

La surveillance efficace du cyber-risque du conseil dépend de la maîtrise du sujet par les membres et des informations à jour.

⇒ Assurez-vous que toutes les personnes qui rejoignent le conseil disposent des compétences et connaissances appropriées et actualisées pour comprendre et gérer les risques posés par les cyber-menaces.
⇒ Sollicitez des conseils réguliers de la part de la direction sur l'exposition au risque actuelle et future de votre organisation, les exigences réglementaires pertinentes, et les références du secteur et de la société pour l'appétit au risque. De plus, participez à des séances d'information régulières sur les derniers développements en ce qui concerne le paysage des menaces et l'environnement réglementaire, la planification commune et les visites aux pairs et aux leaders de la meilleure pratique en matière de cyber-sécurité, ainsi que dans des échanges au niveau du conseil sur la gouvernance et les rapports.
⇒ Donnez à la direction la responsabilité de signaler une évaluation quantifiée et compréhensible des cyber-risques, menaces et événements comme un élément permanent à l'ordre du jour lors des réunions du conseil d'administration.
⇒ Poursuivez la sensibilisation aux problèmes systémiques constants tels que les vulnérabilités de la chaîne d'approvisionnement, les dépendances courantes et l'écart dans le partage des informations entre les tableaux sur la gouvernance des cyber-risques.

Donner le ton

Parallèlement à la haute direction, le conseil doit définir et illustrer les valeurs fondamentales de votre organisation, la culture du risque et les attentes en ce qui concerne la cyber-résilience.

⇒ Favorisez une culture dans laquelle le personnel, à tous les niveaux, reconnaît ses responsabilités importantes pour garantir la cyber-résilience de votre organisation. Dirigez par l'exemple.
⇒ Supervisez le rôle de la direction dans la promotion et le maintien de la culture du risque de votre organisation. Favorisez, surveillez et évaluez la culture du risque, en tenant compte de l'impact de la culture sur la sécurité et la solidité, et apportez des changements si nécessaire.
⇒ Indiquez clairement que vous attendez de tout le personnel qu'il agisse avec intégrité et qu'il fasse remonter rapidement le non-respect observé au sein ou à l'extérieur de votre organisation.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE