Cybersécurité : les conseils d'administration sous pression

La pression monte sur les conseils d'administration (boards) de grandes groupes mondiaux confrontés à l'augmentation de la menace cyber. Il y a cinq ans encore, le cyber-risque n'était pas toujours pensé comme une priorité de suivi par les administrateurs. Désormais, la grande majorité l'appréhende comme un enjeu clé. Le risque cyber étant considéré comme l'un des plus élevés qui pèse sur l'activité et le modèle économique des organisations.

C'est en tout cas le point de vue de chercheurs de l'Université de Californie (UC) Berkeley et de Booz Allen Hamilton (qui fut l'employeur contrarié du lanceur d'alerte Edward Snowden).

Pour cette étude* rendue publique le 15 janvier 2020, ce sont 20 membres de conseils d'administration de multionationales, principalement américaines, qui ont été interrogés. À l'issue d'entretiens réalisés en 2019, les consultants ont émis les conclusions suivantes :

5 points pour améliorer la relation avec les RSSI

1. > Les administrateurs ne considèrent plus que le **traitement du cyber-risque** soit réservé aux décisions opérationnelles prises par la direction des systèmes d'information (DSI).

Selon une autre étude anglophone (ITWeb Brainstorm), 50% des DSI relèvent directement de la direction générale de leur entreprise et disposent le plus souvent d'un siège au conseil d'administration. En revanche, 25% n'ont toujours pas d'accès direct au board.

2. > Or, les conseils peinent à organiser une **réponse** adaptée face à la multiplication et à l'évolution rapide des menaces cyber.

Les cadres standards de gouvernance des conseils d'administration « ne sont pas suffisamment spécifiques pour créer un ensemble de meilleures pratiques à déployer et mettre en oeuvre à un niveau inférieur », ont souligné les consultants de Booz Allen.

3 > La perception de l'exposition aux menaces cyber varie d'un secteur d'activité à l'autre, et dépend beaucoup de la **culture d'entreprise**, selon les auteurs du rapport.

Une organisation cherche-t-elle à impliquer quelques uns ou l'ensemble de ses collaborateurs ? S'expose-t-elle alors davantage aux impacts d'attaques informatiques, du phishing au détournement de mises à jour automatiques applicatives ?

4 > Selon l'enquête promue par Booz Allen, améliorer la **relation avec les RSSI** (responsables de la sécurité des systèmes d'information) est une nécessité.

« Les conseils d'administration ont besoin des RSSI pour traduire des concepts techniques et d'ingénierie complexes dans un langage relativement simple. » Limiter l'approche à « des exercices de conformité et des cases à cocher » n'est efficace et satisfaisant pour personne.

Selon une troisième étude internationale (Osterman Research pour Nominet), 52% des RSSI estiment que la direction de leur entreprise reconnaît leur contribution à la protection de la marque et, plus largement, aux revenus générés par l'organisation. En revanche, 18% jugent que les membres du conseil d'administration sont indifférents à l'égard de l'équipe en charge de la sécurité ou la considèrent avant tout comme une charge…

5 > Il est temps, selon Booz Allen, d'appréhender le cyber-risque comme un **risque « stratégique »**.

*(*source : « Resilient governance for boards of directors : considerations for effective oversight of cyber risk ». L'étude a été réalisée par le Center for Long-Term Cybersecurity (CLTC) de l'UC Berkely, en partenariat avec Booz Allen Hamilton.)*

(crédit photo © shutterstock)