TONE at the TOP®

L'essentiel sur la gouvernance à destination des administrateurs, des comités d'audit et du management des organisations.

Numéro 106 | Août 2021

Cybersécurité : quelle stratégie adopter ?

Quelles que soient leur taille et leur secteur d'activité, **les organisations sont exposées à des cyber-risques** qui, manifestement, ne sont pas près de disparaître. Une enquête mondiale menée auprès d'administrateurs et de dirigeants les classe même parmi les dix risques prépondérants en 2021 – une tendance que l'on devrait toujours constater dans dix ans, d'après les sondés. En effet, la cybercriminalité mondiale devrait progresser de 15% par an, engendrant des coûts annuels de l'ordre de 10 500 milliards de dollars d'ici 2025, selon le cabinet d'étude spécialisé Cybersecurity Ventures, qui considère ce phénomène comme « le plus gros transfert de richesses de toute l'Histoire ».

Les atteintes à la cybersécurité revêtent de multiples formes : utilisation de rançongiciels, attaques affectant les postes de travail à distance ou les chaînes logistiques, hameçonnage et autres pratiques illicites diverses et variées. Ces manœuvres peuvent entraver la bonne marche de l'organisation, diminuer significativement sa valeur, et engager sa responsabilité ou porter atteinte à sa réputation en l'exposant publiquement. Les fuites de données sont de plus en plus coûteuses : 4,24 millions de dollars en moyenne en 2021, soit une hausse de presque 10% par rapport à 2020 *(source : IBM)*.

La pandémie de COVID-19 n'a rien arrangé, engendrant de nouvelles vulnérabilités que l'on est encore loin de maîtriser.

Gérer les menaces

Pour répondre à ces enjeux, le conseil d'administration peut prendre un certain nombre de mesures visant à améliorer la surveillance des cyber-risques – une démarche dans laquelle l'audit interne peut lui être particulièrement utile. En collaborant avec les experts en cybersécurité de l'organisation, l'audit interne peut s'assurer en toute objectivité que les processus mis en œuvre sont adaptés aux enjeux et correctement exécutés. « *Il peut alerter le conseil d'administration si l'organisation est fortement exposée ou si elle se pense, à tort, en sécurité* », explique Sandy Pundmann (CIA), associée senior retraitée de Deloitte Risk & Financial Advisory.

Le conseil d'administration a plusieurs stratégies à sa disposition pour traiter les cyber-risques. Sandy Pundmann, tout comme d'autres, recommandent de connaître le profil de son organisation en matière de risques cyber, d'endosser pleinement son rôle de supervision, et de faire preuve d'esprit critique pour appréhender avec clairvoyance les forces, les faiblesses et les vulnérabilités de l'organisation.

Définir les rôles de supervision et planifier des points réguliers. Si, à l'heure actuelle, moins de 10 % des conseils d'administration disposent d'un comité chargé de la cybersécurité dirigé par un administrateur compétent, cette proportion devrait atteindre 40 % d'ici 2025, selon une enquête de Gartner, Inc. Cette hausse serait portée par l'intensification de la poursuite de digitalisation des organisations durant la pandémie ainsi que par la généralisation du télétravail et des risques qu'il comporte.

À propos de l'IIA

The Institute of Internal Auditors Inc. (IIA) est une association professionnelle qui compte plus de 200 000 membres répartis dans plus de 170 pays et territoires à travers le monde. Porte-parole mondial de la profession d'audit interne, l'IIA intervient en tant que leader incontesté dans les domaines de la formation, de la recherche et de la formulation de normes.

The IIA

1035 Greenwood Blvd.
Suite 149
Lake Mary, FL 32746 USA

Abonnements gratuits

Consultez le site www.theiia.org/Tone pour vous abonner gratuitement.

Avis des lecteurs

Envoyez toutes vos questions et observations à l'adresse : Tone@theiia.org.

Pour Sandy Pundmann, il est parfois difficile de discerner qui est responsable de la supervision du volet cybersécurité dans la mesure où cette responsabilité est souvent éclatée entre la direction et plusieurs comités. Selon elle, ce rôle devrait en réalité être dévolu à un seul et unique comité, qui traiterait le sujet à chacune de ses réunions. En outre, les problématiques de cybersécurité devraient être inscrites à l'ordre du jour des réunions du conseil d'administration au moins deux fois par an.

Prendre conscience de l'ampleur du risque. La cybersécurité dépasse le simple registre de l'informatique. « *Que ce soit en amont ou au beau milieu d'un incident, mieux vaut éviter de laisser la responsabilité [de la cybersécurité] au seul directeur des systèmes d'information et à l'équipe technique* », signale John Noble, ancien directeur du National Cyber Security Centre (Royaume-Uni), dans un podcast du cabinet de conseil McKinsey. « *Les dirigeants doivent trouver un équilibre entre fonctionnalité, sécurité et coûts, et c'est sur cet aspect que le conseil d'administration doit impérativement tester et éprouver les processus*. »

Aller plus loin. Les conseils d'administration devraient savoir si leur organisation évalue périodiquement les cyber-risques et si elle améliore ses techniques d'évaluation. L'audit interne est souvent sollicité pour mener à bien une évaluation (comme un test d'intrusion, par exemple) ; mais, pour Sandy Pundmann, il ne faut surtout pas s'arrêter là. Les organisations ont besoin d'une stratégie multidimensionnelle pour prévenir, détecter et traiter les cyberattaques. Pour ce faire, il conviendrait d'évaluer i) les mesures prises par l'organisation pour appréhender les incidents, ii) l'efficacité de ces mesures, iii) les modalités de surveillance des incidents et des réponses apportées, et iv) le fonctionnement et l'efficacité de la méthode employée. Sandy Pundmann précise que si cette évaluation peut être initiée au niveau d'un comité, la question devrait tout de même être étudiée par l'ensemble du conseil d'administration.

Dans l'une de ses publications, le cabinet Deloitte indique que la première ligne de défense contre les cyber-risques se compose des unités opérationnelles et des équipes informatiques, lesquelles gèrent ces risques au quotidien par leurs décisions et leurs activités. La deuxième ligne est quant à elle constituée des responsables de la gestion des risques liés aux systèmes d'information, qui assument des fonctions de gouvernance et de supervision. Enfin l'audit interne endosse, de plus en plus fréquemment, le rôle de troisième ligne, en réalisant une revue indépendante des mesures de sécurité mises en œuvre et de leur performance.

Cerner les spécificités de ce domaine de risque. Les organisations et leur conseil d'administration sont familiers des risques. Néanmoins, les cyber risques se distinguent pour plusieurs raisons. Premièrement, il s'agit d'un domaine très technique, en évolution permanente, qui, de ce fait, se trouve en dehors du champ des connaissances de bon nombre d'administrateurs. Deuxièmement, la plupart des organisations utilisent massivement Internet. Les risques associés sont donc multiformes et complexes, tout comme leurs effets. « Pour une organisation, l'usage d'Internet est essentiel en termes de création de valeur, et toutes les opérations qui en dépendent sont, de fait, risquées », indique l'un des participants à une table ronde du Cyber Risk Director Network. « Ce n'est pas le cas dans les autres domaines de risque couverts par le conseil d'administration. »

QUESTIONS POUR LES ADMINISTRATEURS

- À quelle fréquence est-il fait état au conseil d'administration des cybermenaces qui pèsent sur l'organisation et des mesures prises pour traiter et gérer les cyber-risques ?
- L'organisation considère-t-elle la cybersécurité comme un domaine de risque transversal qui dépasse la seule sphère informatique ?
- Le conseil d'administration exerce-t-il une supervision proactive des cyber-risques ou part-il du principe que tant qu'aucun problème ne lui est signalé, tout va bien ?
- Le conseil d'administration dispose-t-il d'un comité chargé de la cybersécurité ? Sinon, un autre comité (le comité d'audit par exemple) est-il investi d'un rôle de surveillance en matière de cybersécurité ?

Se confronter à la réalité. Dans le cadre d'un exercice, qui peut être réalisé par l'audit interne, le conseil d'administration et la direction peuvent observer une attaque simulée afin d'évaluer comment l'organisation y répond, comment les investisseurs sont avertis et comment les clients ou les partenaires se trouvent affectés. (Sandy Pundmann a même collaboré avec un conseil d'administration qui a souhaité que seuls le directeur des systèmes d'information et le directeur général soient informés du caractère fictif de l'exercice, afin de le rendre aussi réaliste que possible.) Une fois que l'organisation a fait le bilan de l'exercice, le conseil d'administration peut être informé des changements apportés ou envisagés.

L'audit interne peut aussi jouer un rôle de premier plan dans un autre exercice particulièrement utile : la visualisation du modèle de maturité. Ce procédé donne une vue d'ensemble des cyber-risques qui pèsent sur l'organisation et compare sa situation actuelle à la situation souhaitée, le tout de manière simple et intelligible. Explication de Sandy Pundmann : parce qu'il est impossible de surveiller et traiter tous les risques, ces exercices peuvent également permettre d'identifier les enjeux les plus critiques pour l'organisation, de sorte que cette dernière puisse améliorer ses mesures de prévention et de détection dans ces domaines.

Ne pas se laisser surprendre par les cyber-risques. À mesure que l'usage de la technologie s'intensifie, s'accroissent également les risques associés aux technologies émergentes . Pour Sandy Pundmann, même un nouvel ERP peut poser des problèmes de sécurité. En effet, de nombreuses organisations attendent, à tort, que les défaillances d'un système soient avérées avant d'envisager d'y remédier. « Assurez-vous d'avoir un plan de sécurité dès les premières étapes de votre stratégie de cybersécurité et de contrôle », conseille l'experte.

Les organisations engagées dans des opérations de fusion-acquisition peuvent aussi être exposées à de nouvelles vulnérabilités. « Si vous achetez une entreprise, interrogez-vous sur les risques que comporte cette opération », recommande Sandy Pundmann. Les organisations qui travaillent avec une chaîne logistique ou avec d'autres tiers peuvent se retrouver exposées aux risques pesant sur ces acteurs. En outre, les organisations devraient se tenir informées de la réglementation en vigueur, telle que la réglementation de la Securities and Exchange Commission relative aux informations à produire en matière de cybersécurité.

Exploiter le potentiel de l'audit interne

Les cybermenaces peuvent être effrayantes, mais l'audit interne peut apporter un point de vue à la fois unique et indépendant sur les risques pesant sur l'organisation et les meilleures solutions de traitement. Les conseils d'administration exerçant une supervision proactive des enjeux de cybersécurité et exploitant le plein potentiel de l'audit interne devraient être en situation de mieux gérer les cyber-risques.

QUE MANQUE-T-IL À VOTRE CONSEIL D'ADMINISTRATION ?

60% des organisations n'ont pas de responsable de la cybersécurité au niveau du conseil d'administration ou de la direction générale.

59% des organisations indiquent que la relation entre la cybersécurité et les différents métiers est , dans le meilleur des cas, neutre, sinon empreinte de méfiance ou inexistante.

20% des conseils d'administration sont pleinement convaincus que les mesures de traitement des cyber-risques qui leur sont présentées suffisent à protéger l'organisation contre des cyberattaques d'envergure.

36% des organisations indiquent que, pour chaque nouvelle initiative engagée, la cybersécurité est un volet pris en compte dès l'étape de planification.

Source : *The Risky Six: Key Questions to Expose Gaps in Board Understanding of Organizational Cyber Resiliency*, IIA Global et EY, 30 mars 2021

1 *Executive Perspectives on Top Risks for 2021 and 2030*, Protiviti et ERM Initiative (NC State University), 2021.
2 *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, Steve Morgan, Cybercrime Magazine, 13 novembre 2020.
3 *Cost of a Data Breach Report*, IBM, 2021.
4 *Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025*, communiqué de presse publié par Gartner, 28 janvier 2021.
5 *Boards and Cybersecurity*, podcast de McKinsey & Company, 2 février 2021.
6 *Cybersecurity and the Role of Internal Audit: An Urgent Call to Action*, Sandy Pundmann, Deloitte, 2017.
7 *Cybersecurity: An Evolving Governance Challenge*, Harvard Law School Forum on Corporate Governance, 15 mars 2020.
8 *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, numéros 33-10459 et 34-82746, Securities and Exchange Commission, 26 février 2018.

Sondage rapide

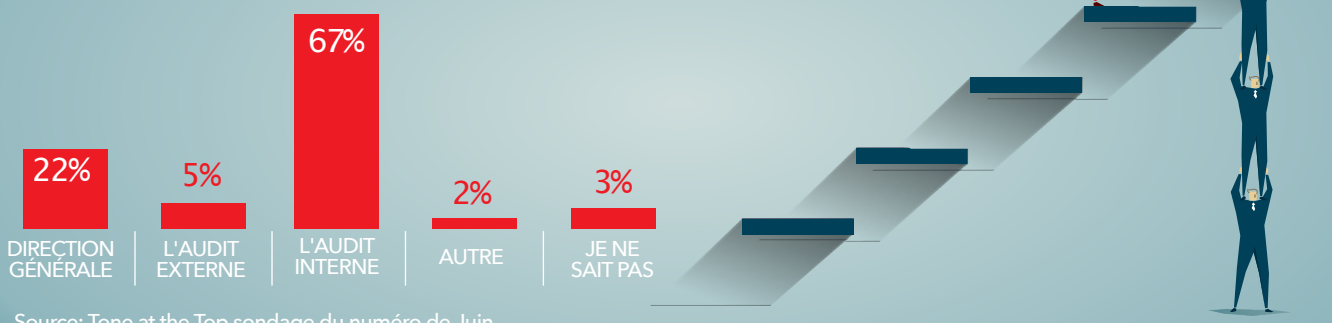
Votre conseil d'administration compte-t-il parmi ses membres un expert en cybersécurité ?

- ❑ Oui
- ❑ Non
- ❑ Je ne sais pas

Rendez-vous sur www.theiia.org/Tone pour répondre à cette question et connaître les réponses des autres.

RÉSULTATS DU SONDAGE RAPIDE

Qui le conseil d'administration sollicite-t-il en priorité pour obtenir une assurance concernant l'efficacité des processus de gestion des risques et de contrôle interne ?



Source: Tone at the Top sondage du numéro de Juin.

Copyright © 2021 de The Institute of Internal Auditors, Inc. Tous droits réservés.