TONE at the TOP®

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

Numéro 113 | Octobre 2022

Lutter contre les cybermenaces

Pan incontournable du panorama contemporain des risques, la cybersécurité représente une menace évolutive et protéiforme qui pèse de plus en plus lourd dans les attributions du conseil d'administration en matière de supervision. Selon un sondage de la National Association of Corporate Directors (NACD), 70 % des administrateurs considèrent que la cybersécurité est « *un risque stratégique pour l'entreprise* »[1]. Protection des données personnelles, lutte contre les cyberattaques (rançongiciels et autres logiciels malveillants, tentatives de *phishing* ou déni de service), adéquation effective des politiques de cybersécurité et plans d'intervention et de reprise d'activité sont autant de préoccupations diverses et majeures en lien avec cette question.

Les organisations doivent également se plier à de nouvelles réglementations qui leur imposent de communiquer en cas d'incident. L'administration Biden vient par exemple de voter le *Cyber Incident Reporting for Critical Infrastructure Act*[2] pour permettre à l'Agence fédérale de cybersécurité et de sécurité des infrastructures d'apporter son aide aux victimes de cyberattaque, mais aussi d'identifier des tendances et d'informer d'autres victimes potentielles. La Securities and Exchange Commission (SEC) a également publié des projets de règles[3] visant à harmoniser les déclarations des entreprises cotées en matière de stratégie, de gouvernance et de gestion des risques cyber et de remontée des incidents.

Dans ce contexte, le conseil d'administration peut trouver un allié précieux dans l'audit interne, dont le rôle est de fournir assurance et conseil de manière indépendante et objective. En effet, d'après un rapport de PwC, « *nombreuses sont les entreprises qui sollicitent l'audit interne pour qu'il examine leurs processus de cybersécurité et les dispositifs de contrôle associés, notamment sous l'angle de la résilience et de la capacité de réaction* »[4].

Vers plus de sécurité

Dans le cadre de l'évaluation des cyber-risques dont doit se saisir le conseil d'administration, l'audit interne pourra apporter sa pierre à l'édifice à plus d'un titre.

Appréhender le risque. Pour les entreprises, les cybermenaces dominent aujourd'hui tous les autres risques. Selon le rapport *OnRisk 2022* de l'Institute of Internal Auditors (IIA), « *par leur sophistication croissante et leur diversité, les cyberattaques continuent de faire des ravages dans les entreprises, détruisant des marques,*

ternissant des réputations, engendrant bien souvent des dégâts financiers considérables »[5]. Dans cette étude menée à partir d'entretiens avec des administrateurs, des dirigeants d'entreprise et des responsables d'audit interne, la cybersécurité figure cette année en tête du classement des risques.

Néanmoins, hélas, certains dirigeants peinent à prendre la pleine mesure de la menace. En effet, le rapport *OnRisk* pointe un écart inquiétant entre le degré de pertinence attribué à ce risque par les différentes catégories de répondants. Si 97 % des responsables d'audit interne considèrent la cybersécurité comme un risque « extrêmement pertinent » pour leur organisation (note de 6 ou 7 sur une échelle de 1 à 7), ce n'est le cas que de 87 % des administrateurs et de 77 % des dirigeants.

Ces chiffres montrent que les responsables d'audit interne sont particulièrement attentifs aux enjeux de cybersécurité. C'est tout sauf surprenant, car l'audit interne est fin connaisseur de l'organisation. Le conseil d'administration cherchant à optimiser l'assurance et à l'élargir au-delà des risques financiers et de conformité, il pourra demander à l'audit interne de l'aider à lister les préoccupations posées par le domaine cyber et à quantifier leur impact potentiel. Il s'agira alors par exemple d'identifier des lacunes dans la couverture des risques, de surveiller des risques émergents ou encore de faire le meilleur usage des technologies à des fins de cybersécurité.

Se servir du Modèle des Trois Lignes. Le Modèle des Trois Lignes[6] aide les organisations à identifier les structures et processus optimaux pour réaliser leurs objectifs et renforcer leurs dispositifs de gouvernance et de gestion des risques, y compris cyber. Ce modèle identifie les rôles clés joués par :

À propos de l'IIA

The Institute of Internal Auditors Inc. (IIA) est une association professionnelle qui compte plus de 218 000 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 401
Lake Mary, FL 32746, USA

Abonnements gratuits

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

Avis des lecteurs

Envoyez toutes vos questions et observations à l'adresse :

Tone@theiia.org.

» l'organe de gouvernance, lequel assume un devoir de rendre compte vis-à-vis des parties prenantes quant à la surveillance de l'organisation ;

» le management, lequel mène les actions nécessaires pour réaliser les objectifs de l'organisation ;

» l'audit interne, lequel fournit une assurance indépendante et objective quant à l'atteinte de ces objectifs.

Des recherches montrent que la coopération entre ces trois lignes renforce l'efficacité de la gestion des cyber-risques. Selon un article paru dans l'*ISACA Journal*[7], l'audit interne peut fournir une assurance précieuse en contribuant à l'identification des menaces et des vulnérabilités. Par exemple, la fonction est à même de dégager les tendances qui se dessinent et les attentes des parties prenantes, de procéder à un diagnostic des risques cyber et de définir des critères d'audit efficaces. En faisant part de leurs constats et de leurs conseils, « *les auditeurs peuvent fortement aider [le conseil d'administration] à s'acquitter de sa mission de supervision* ».

Optimiser l'apport de l'audit interne. Dans de nombreuses organisations, le comité d'audit a pour tâche de traiter toute une panoplie de risques, à commencer par les risques cyber[8]. Néanmoins, il arrive que ces derniers incombent à d'autres comités, et ce, pour diverses raisons. Selon le secteur d'activité de l'organisation, sa taille et les menaces qui pèsent sur elle, le comité chargé de la supervision des enjeux cyber pourra donc être un comité spécialement créé à cet effet, un comité des risques, un comité des technologies, le comité de nomination et de gouvernance, ou autre. En effet, le conseil d'administration peut très bien estimer que le comité d'audit a déjà fort à faire ou qu'il ne possède pas l'expertise nécessaire pour superviser ce type de risque, par exemple.

Bien que l'audit interne soit généralement rattaché au comité d'audit, l'organisation risque de se priver d'une assurance et de recommandations précieuses en matière cyber si sa fonction d'audit ne propose pas en parallèle ses services à un comité chargé des questions de cybersécurité. Pour l'audit interne, l'établissement de liens avec le comité compétent, quel qu'il soit, est le gage que ses points de vue seront entendus et pris en compte.

Identifier les menaces cachées. Le conseil d'administration n'a souvent pas idée du nombre de lacunes apparemment mineures et pourtant susceptibles de nuire aux efforts de cybersécurité, voire de provoquer une catastrophe. Par ses éclairages, l'audit interne peut l'aider à déterminer dans quelle mesure le plan d'audit de l'organisation permet d'identifier les menaces jusqu'ici négligées et de détecter les risques émergents. Voici d'ores et déjà un aperçu des cybermenaces que, selon un rapport de Deloitte[9], la direction générale a tendance à sous-estimer :

» le nombre d'anciens salariés encore en mesure de se connecter aux systèmes de l'entreprise et le nombre de fournisseurs ayant accès à ces systèmes. Dans un cas comme dans l'autre, les entreprises ne se doutent pas du nombre de profils non identifiés et non habilités qui peuvent s'infiltrer dans leurs systèmes.

QUESTIONS POUR LES ADMINISTRATEURS

» Exploitons-nous au mieux les points de vue et les conseils de l'audit interne dans le cadre de notre planification stratégique sur le volet cybersécurité ?

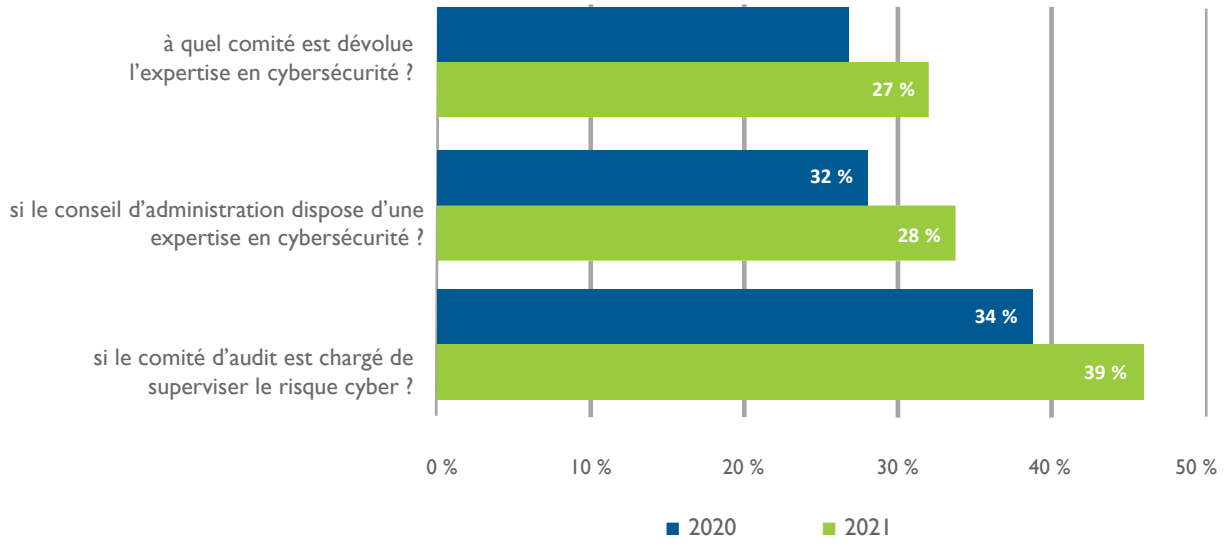
» Avons-nous alloué les ressources (humaines et financières) suffisantes à cette thématique ?

» L'organisation a-t-elle quantifié financièrement son degré de tolérance au risque cyber ?

» Existe-t-il un comité spécifiquement chargé de la cybersécurité ?

» Les administrateurs connaissent-ils les procédures à mettre en œuvre en cas de cyberincident et savent-ils quoi faire en pareille situation ?

Combien d'entreprises du S&P 500 précisent-elles :



Source : *2021 Audit Committee Transparency Barometer*, Center for Audit Quality, novembre 2021.

» le nombre de comptes *cloud* dont se sert l'entreprise. Plus les applications sont hébergées sur le *cloud*, plus le risque de cyberattaque est grand. Deloitte recommande aux organisations d'interroger leurs fournisseurs *cloud* sur des indicateurs comme la résilience de leurs infrastructures, la durée des interruptions de service et la performance, entre autres, mais aussi sur l'évaluation de la conformité réglementaire et des contrôles indépendants.

» le nombre réel d'incidents cyber subis par l'entreprise. Paradoxalement, si une structure n'a pas subi beaucoup d'attaques, c'est peut-être que celles-ci sont tout simplement passées inaperçues. Là aussi, l'audit interne peut aider l'organisation à se montrer attentive à ces signaux d'alerte.

Sécuriser les relations avec les partenaires commerciaux. Gartner prédit qu'en 2025, 60 % des organisations tiendront compte du risque cyber avant de s'engager dans une relation commerciale avec un tiers[10]. Aujourd'hui, seuls 23 % des responsables de la sécurité et de la gestion des risques suivent l'exposition des tiers en temps réel, et encore, il n'est pas exclu qu'ils limitent leur examen aux fournisseurs et sous-traitants de premier rang.

Là encore, les responsables d'audit interne, les dirigeants et les administrateurs ont des avis divergents, selon l'enquête *OnRisk 2022*. Si les premiers estiment la capacité de l'organisation dans ce domaine à 37 %, les autres la jaugent respectivement à 53 % et 57 %. Cette confiance moindre de la part des responsables d'audit interne s'explique en partie par le degré de pertinence plus élevé qu'ils attribuent à ce risque par rapport aux administrateurs (77 % contre 60 %, soit 17 points d'écart).

Dans tous les cas, il appartient au conseil d'administration de veiller à exploiter au mieux le point de vue et l'expérience de l'audit interne dans ce domaine. Parce que l'audit interne est en lien avec des équipes dans toute l'organisation, il peut signaler au conseil d'administration les risques cyber que présente un fournisseur donné ou la chaîne logistique dans son ensemble. Lorsque les partenaires commerciaux de l'entreprise réclament des garanties au sujet de ses défenses numériques et de leur fiabilité, l'audit interne est à même de leur fournir les données et l'assurance exigées.

Optimiser les ressources

Face à des préoccupations de cybersécurité majeures, les organisations vont devoir optimiser l'ensemble de leurs ressources. Pour le conseil d'administration, cerner la valeur que l'audit interne peut apporter à l'organisation tout entière grâce à l'identification d'axes d'amélioration et d'optimisation et en tirer parti, c'est faire un pas vers une entreprise plus sûre.

Références

1 *Principles for Board Governance of Cyber Risk*, National Association of Corporate Directors, Internet Security Alliance et Forum économique mondial, en collaboration avec PwC, mars 2021.

2 https://www.cisa.gov/circia

3 https://www.sec.gov/rules/proposed/2022/33-11038.pdf

4 *Overseeing Cyber Risk: The Board's Role*, PwC, janvier 2022.

5 *OnRisk 2022: A Guide to Understanding, Aligning, and Optimizing Risk*, The Institute of Internal Auditors, 2021.

6 *Le Modèle des Trois Lignes de l'IIA : Version 2020 des Trois Lignes de Maîtrise*, The Institute of Internal Auditors, juillet 2020.

7 « How Effective Is Your Cybersecurity Audit? », Matej Drašček *et al.*, *ISACA Journal*, 1er juin 2022.

8 « Cybersecurity: An Evolving Governance Challenge », *Harvard Law School Forum on Corporate Governance*, Phyllis Sumner *et al.*, 15 mars 2020.

9 *Internal Audit: Risks and Opportunities for 2022*, Deloitte, 2021.

10 « Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem », Sam Olyaei *et al.*, *Gartner*, 24 janvier 2022.

Sondage rapide

Quel comité du conseil d'administration supervise la gestion des risques cyber dans votre organisation ?

- ◯ Comité d'audit
- ◯ Comité de cybersécurité
- ◯ Comité des technologies
- ◯ Comité de nomination et de gouvernance
- ◯ Autre

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

RÉSULTATS DU SONDAGE RAPIDE

Votre organisation sollicite-t-elle l'audit interne pour obtenir une assurance en matière ESG ?