L'AGEFI
mercredi 3 avril 2024 - 00:00 Europe/Paris
928 mots - ⏱ 4 min

ENTREPRISES

: L'AGEFI

Les administrateurs sont appelés à prendre à bras-le-corps la sécurité numérique

L'Institut français des administrateurs s'apprête à publier un guide dédié, invitant les conseils à dialoguer et à challenger la direction générale.

Alors que l'intelligence artificielle (IA) ouvre de nouvelles possibilités et que les cyberattaques se multiplient, les administrateurs doivent se saisir de ces sujets. Pour les y aider, le club des présidents de comité d'audit de l'Institut français des administrateurs (IFA) s'apprête à publier un guide de bonnes pratiques «sécurité numérique et gouvernance». Le guide de l'IFA sur le rôle du comité d'audit en matière de cybersécurité de 2016, très novateur à l'époque, avait besoin d'une mise à jour. D'autant que le sujet concerne tous les administrateurs. En France comme aux Etats-Unis, «les comex ont pris conscience des sujets cyber, mais pas les conseils d'administration. Ils ont tendance à se défausser sur le DSI ou sur les assureurs, la thématique étant en dehors de leur zone de confort», confie Marie-Noëlle Brisson, rapporteure du groupe de travail, et co-fondatrice de CyberReady LLC. Ce guide veut les aider à se décomplexer et à enrichir leur dialogue avec la direction générale et les investisseurs.
Demeurer au stade de la sensibilisation à ces sujets est insuffisant, d'autant que le coût de la cybercriminalité est estimé à 8.000 milliards de dollars dans le monde l'an dernier par CyberSecurity Ventures. Les administrateurs doivent pouvoir interagir «*de façon concrète et poussée, au bon niveau, avec des experts opérationnels (RSSI, DSI, Directeurs Sûreté) et des experts risques et conformité de l'entreprise*», explique le guide. Ce qui nécessite une formation minimale sur les questions de cybersécurité. Des administrateurs qui doivent se former sur de plus en plus de sujets pour les appréhender de manière pertinente. Un vrai défi pour les conseils de demain.

Pour les sociétés les plus exposées, un comité dédié (digital, numérique, technologiques...) ou un administrateur formé dans le cadre d'un parcours certifiant serait un plus pour le conseil. «*Une question largement débattue*, reconnaît Marie-Noëlle Brisson. *Attention à ne pas recréer un 'codir' au sein du conseil, avec un spécialiste de chaque sujet. Tous les administrateurs doivent comprendre les enjeux.*» Comme pour tous les «spécialistes», cela ne doit pas décharger le reste du conseil, qui demeure responsable collégialement. Le règlement intérieur du conseil doit prévoir quand et comment le comité ou l'administrateur spécialisé communique au conseil.

A lire aussi: La durabilité pousse les conseils d'administration à un engagement renforcé

Se former pour bien comprendre les enjeux

Concrètement, comment agir ? Le conseil doit formaliser son implication sur les sujets de sécurité numérique par un dialogue avec la direction générale, et vérifier sa réelle implication dans la mise en place et le déploiement du plan cyber. «*Un dialogue efficace passe par des questions pertinentes et par une bonne compréhension des réponses*, poursuit Marie-Noëlle Brisson. *La sécurité numérique est mieux traitée par les conseils des grands groupes, notamment dans les banques, même si ce traitement peut toujours s'améliorer. En revanche, elle reste encore bien moins présente dans les conseils des ETI et PME, moins armés.*» Comme pour de nombreux domaines d'actions du conseil, «*un des pièges serait de se limiter à la conformité, nécessaire mais insuffisante, et qui ne permet pas de saisir des opportunités stratégiques*», avertit Marie-Noëlle Brisson

La question de l'intrusion «*n'est plus de savoir si, mais quand elle va se produire*», souligne le rapport. Il s'agit donc pour le conseil d'anticiper. Le guide propose trois axes de réflexion.

Premièrement, la préparation. Comment la direction structure ses actions de prévention de façon dynamique (moyens techniques, organisationnels, financiers et humains sur l'identification et le suivi des risques et du contrôle interne, ainsi que la formation). Quel niveau d'information est demandé ? Quels moyens humains, techniques, financiers sont mis en œuvre, et avec quel audit ? Des exercices d'attaque cyber sont-ils régulièrement réalisés ? Alors que la sécurité numérique est un sujet à la fois stratégique et opérationnel, «*l'une des difficultés est de bien positionner le curseur entre le pilotage de la stratégie et l'ingérence managériale*, prévient Marie-Noëlle Brisson. *Tout dépend de la qualité des questions et la transparence du management. Par exemple, on ne va pas dans le détail du plan de continuité, mais on regarde s'il a été préparé, répété et pratiqué.*»

Deuxièmement, comment l'entreprise a anticipé et organisé la gestion de crise lors d'une attaque et bâti son plan de reprise de l'activité. Si les investisseurs demandent de plus en plus de transparence, la communication externe doit être maniée avec précaution. «*Les investisseurs, agences de notation, proxys ont besoin d'entendre que les procédures internes sont robustes et pratiquées*», poursuit Marie-Noëlle Brisson. Divulguer les incidents et attaques dans un cadre raisonnable n'est plus perçu négativement, puisque personne n'est à l'abri.

Troisièmement, comment la direction considère les assurances cyber. «Le transfert du risque chez l'assureur *ne règle pas tous les sujets*, constate Marie-Noëlle Brisson. *D'autant que les polices sont de plus en plus chères et que les cas d'exclusion se multiplient.*»

A lire aussi: L'IA bouscule les habitudes des dirigeants d'entreprise

Préparer l’intégration de l’IA par l’entreprise

Des conseils prêts à aborder les questions de sécurité numériques seront aussi armés pour s’adapter à l’arrivée de l’intelligence artificielle. «*La meilleure préparation passe par une bonne gouvernance des données et la mise en place de procédures*, anticipe Marie-Noëlle Brisson. *Face à la pression des régulateurs, il est essentiel de prioriser les données et de les cartographier. On ne peut pas toutes les protéger.*» Ce processus de gouvernance des données va de leur qualification (sensibles, critiques…), fiabilisation, utilisation, traitement jusqu’au stockage. Il comprend aussi une analyse de l’empreinte carbone, essentielle à la stratégie de transition climatique de l’entreprise. Rappel que les administrateurs doivent être présents sur tous les fronts à la fois.

©photo European Union -

par Brunoderoulhac@agefi.fr(bruno De Roulhac)

c879e5788c25a980c6e41b18d903e15f089A6a665Zc6G6af9cf6085