Les Echos

N° 23976
vendredi 9 juin 2023
Édition(s) : Supplément 1
Page 2
582 mots - 2 min

Sensibiliser les Comex

Les cybermenaces gagnent en visibilité dans les sphères dirigeantes et les services d'audit interne ; mais une stratégie nouvelle doit être impulsée pour acculturer les comités exécutifs.

La cybermenace est en tête des risques les plus probables, selon l'enquête Risk In Focus 2023 de la Confédération européenne des instituts d'audit interne (ECIIA). Mais ces risques sont-ils inscrits à l'agenda des comités exécutifs ? Pas si sûr. « La frontière a été franchie en 2017, dans les grandes entreprises, lorsque deux virus, NotPetya, et Wannacry, ont créé de gros dégâts financiers », constate Marie de Fréminville, présidente-fondatrice de Starboard Advisory, société de conseil en gouvernance, finance et cybersécurité.

Les directeurs de système d'information, qui échangeaient rarement avec les comités exécutifs et les conseils d'administration, ont alors été conviés à présenter des solutions et une feuille de route pour limiter l'impact de potentielles nouvelles attaques. « Dans les plus petites sociétés, la prise de conscience est plus lente, par manque de temps, manque de budget, ou parce que le dirigeant ne sait pas par où commencer », ajoute Marie de Fréminville.

Manque d'alignement

Malgré une prise de conscience accrue de la menace, dans de nombreuses PME et ETI, le directeur du système d'information et le prestataire informatique restent les responsables du cyber-risque. « Les dirigeants ont conscience qu'ils peuvent du jour au lendemain connaître un incident majeur, mais la cybersécurité est encore perçue comme un sujet purement technique. Les Comex doivent être impliqués afin de se positionner dans la prise de décision (priorités, budget, organisation, procédures) et la préparation des crises », insiste Marie de Fréminville.

Ce manque d'alignement du Comex sur la cybersécurité se ressent dans la connaissance superficielle du risque que les directions et les administrateurs en ont. « Les DSI sont trop rarement invités dans les Comex ou dans les Conseils, et ont donc peu d'occasions de partager les informations et les projets. Cela s'apprécie dans la qualité des questions posées par le comité de direction et les administrateurs, la granularité des informations demandées, qui restent assez pauvres », constate Anne-Hélène Monsellato, administratrice indépendante, membre de l'IFA (Institut français des administrateurs) et présidente de comités d'audit.

Tout l'écosystème

Lorsque les entreprises s'emparent du sujet, cela se matérialise par l'intégration du risque cyber dans la cartographie des risques et par la présentation au Comex d'une situation actualisée, d'un plan de contrôle et d'audit intégrant un test d'intrusion, et de prise en compte du facteur humain. C'est le cas dans les groupes bancaires et d'assurance, particulièrement réglementés, mais également dans les entreprises qui ont connu des failles informatiques provoquées, par exemple, par l'attaque d'un sous-traitant, voire des destructions physiques causées par l'intrusion de systèmes informatiques industriels.

« Cette cartographie reste parfois insuffisante, car elle ne prend pas en compte tout l'écosystème de l'entreprise, à savoir la chaîne des fournisseurs, des sous-traitants et des clients. Cela a un impact significatif sur l'élaboration d'un budget, tant que le Comex n'a pas pris la mesure des risques numériques », observe Marie-Noëlle Brisson, administratrice indépendante et cofondatrice de la société CyberReady. D'autres entreprises intègrent des indicateurs de performance « pour renforcer le contrôle interne dans un processus d'amélioration continue et casser les silos entre les différentes fonctions », constate Marie-Noëlle Brisson. Les DSI obligent ainsi les comités de direction à s'intéresser à la question. Si la prise de conscience germe, le risque cyber doit encore être vulgarisé auprès du Comex, des administrateurs et plus largement auprès de tous les utilisateurs.

Mallory Lalanne ■

par Mallory Lalanne

Parution : Quotidienne
Audience : 135 089 ex. (Diff. payée Fr.) - © ACPM PV 2020-2021

397f25048e55538a16c41798c50dd18152258921331364c7142fbcc