TONE at the TOP®

POWERED BY The Institute of Internal Auditors | Audit Executive Center

Numéro 82 | Juin 2017

Fournir aux cadres supérieurs, aux conseils d'administration et aux comités d'audit des informations concises sur des sujets liés à la gouvernance.

L'éclairage que l'audit interne apporte à la culture de la cyber-sécurité

La propagation rapide du rançongiciel WannaCrypt, rapidement surnommé *#WannaCry* sur les réseaux sociaux après avoir paralysé environ 200 000 ordinateurs en Europe, en Asie et en Amérique, pousse les fonctions de gouvernance et de management des risques à repenser sérieusement la manière dont elles pourraient renforcer les dispositifs de contrôle en matière de cyber-sécurité. Pourquoi donc, après tant d'années d'échecs au niveau de la cyber-sécurité, les organisations sont-elles prises de court à la moindre attaque ?

Bien involontairement, les cultures des organisations en matière de cyber-sécurité peuvent rendre ces failles plus importantes encore, écrit le Président et Directeur Général de l'IIA Richard F. Chambers (CIA, QIAL, CGAP, CCSA, CRMA) dans un article de blog peu après que *#WannaCry* a infecté la planète.
« Fournir une assurance sur le cyber-risque ne consiste pas à déterminer si les protocoles et les politiques de blocage ou dissuasion des cyber-attaques sont en place et fonctionnent efficacement », écrit-il. « Nous devons également examiner la manière dont la culture de l'organisation influence la façon dont ces mesures de protection sont appliquées ».

Par exemple, certaines organisations peuvent accepter des comportements à plus haut risque dans les échanges de courriers électroniques pour favoriser la productivité. Ou encore, les efforts consentis en matière de cryptage des données peuvent être compromis si les règles interdisant ou limitant les impressions ne sont pas mises en place ou si elles sont ignorées. Richard Chambers a également mis en garde contre la « mystification du département informatique » qui considère que la cyber-sécurité est la chasse-gardée du département informatique et ne laisse pas participer d'autres parties prenantes au débat.

La mise en place d'une coopération entre le département informatique, les responsables du management des risques, de la sécurité de l'information, les ressources humaines ainsi que les autres acteurs gérant les cyber-risques aidera les auditeurs internes à renforcer la culture de la cyber-sécurité de leur organisation. Dans le cas contraire, l'audit interne ne sera pas en mesure de comprendre ce qui engendre les cyber-risques, ni ce qui influence la culture de la cyber-sécurité de l'organisation et par conséquent, ne pourra pas partager ces points de vue avec le management et le Conseil.

A propos de l'IIA

The Institute of Internal Audtors Inc. (IIA) est une association professionnelle qui compte plus de 190 000 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 **www.theiia.org/tone** pour vous abonner gratuitement.

Avis des lecteurs

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

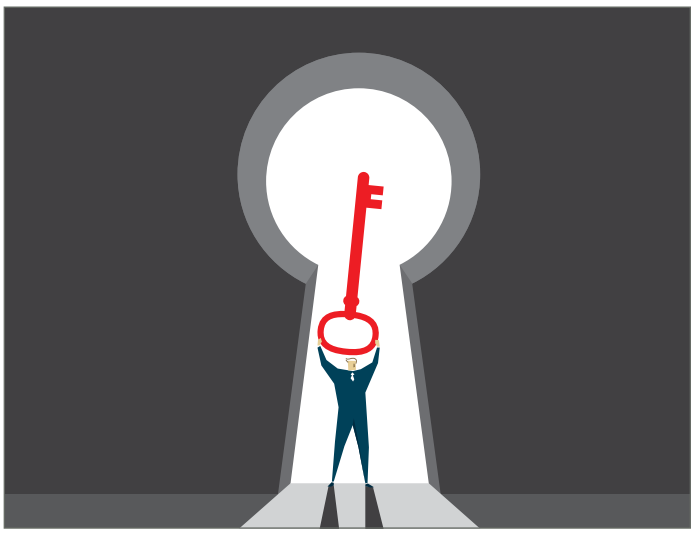
Conseil consultatif en matière de contenu

Riches de plusieurs décennies d'expérience comme membres de la direction ou du conseil d'administration, les professionnels énumérés ci-après ont revu le contenu de la présente publication :

Martin M. Coyne II

Michele J. Hooper

Kenton J. Sicchitano



Même les mises à jour de sécurité, solution évidente qui aurait pu éviter le déchainement de *#WannaCry*, disposent d'une composante culturelle qui va au-delà de leur simple désignation technologique. La mise en place d'un correctif pour combler des failles de sécurité peut être très complexe dans la mesure où l'on ne connaît pas vraiment l'impact que ce correctif aura sur les systèmes opérationnels sans test préalable, déclare Doug Anderson, le directeur général de CAE Solutions de l'IIA. « Nous ne pouvons pas systématiquement blâmer le département informatique ou ceux qui le supervisent. La situation est plus compliquée et nécessite de prendre en compte le rapport bénéfices/coûts lorsque vous analysez les risques au sein d'une organisation ».

Il existe des obstacles bien connus qui peuvent empêcher les auditeurs internes d'auditer la culture de l'organisation. L'enquête 2016 Pulse of Internal Audit de l'IIA North America a révélé que 24% des personnes interrogées pensent que l'audit interne n'a pas la liberté d'évaluer l'organisation dans son ensemble y compris le personnel. 35% considèrent qu'elles ne bénéficient pas du soutien indéfectible de la direction générale pour le faire et 23% estiment qu'elles manquent de soutien de la part du Conseil et du comité d'audit.

Avoir voix au chapitre

Tant que la direction générale considère que la cyber-sécurité relève du département informatique, la tendance à désigner le responsable, dès qu'un problème apparaît, perdurera. Et c'est un frein à une collaboration efficace qui empêche l'émergence d'une culture de la cyber-sécurité basée sur plus de coopération.
« L'audit interne est une des rares fonctions à avoir une voix qui raisonne à travers toute l'organisation. De ce fait, elle est en mesure de voir comment les différents acteurs collaborent les uns avec les autres et veille à ce que la bonne information arrive aux bons destinataires », déclare Doug Anderson. Plus l'audit interne sera en mesure d'agir

dans cette voie, plus il sera sollicité pour apporter sa contribution et sera impliqué dans la planification stratégique des activités, y compris en matière de cyber-risques.

Avoir l'opportunité d'exercer une influence sur la culture globale de management des risques de l'organisation dépend grandement de la façon dont les auditeurs internes comprennent leur rôle. Ceux qui pensent que leur objectif est d'identifier et de signaler des problèmes n'iront pas très loin, nous indique Jim Pelletier, vice-président en charge des relations professionnelles ainsi que de celles avec les parties prenantes de l'IIA. Reconnaître qu'il est en position d'aider l'organisation à atteindre ses objectifs est un signe que le responsable de l'audit interne ou le président du comité d'audit a compris le niveau de maturité de l'organisation. Ceci devrait leur permettre de mieux exploiter les ressources de l'audit interne afin d'avoir un impact positif sur l'organisation.

« Il s'agit d'imprégner la culture de l'organisation. En effet, le responsable de l'audit interne gagnera au fur et à mesure la confiance en démontrant qu'il n'est pas là pour donner des claques, vous mettre dans l'embarras et repartir comme si de rien n'était », dit Jim Pelletier. Il ajoute également que le comité d'audit sera moins enclin à utiliser l'information en provenance de l'audit interne uniquement dans le but de punir le management d'avoir manqué à ses obligations. Il y aura toujours des situations de fraude ou d'abus, lesquels devront être traités séparément, mais « le travail quotidien devrait avoir un impact positif sur l'organisation ».

Le Conseil et le comité d'audit amenés à protéger le rôle de l'audit interne en matière de cyber-sécurité

Pour le cabinet Deloitte & Touche, un engagement fréquent et proactif du Conseil, et en particulier du comité d'audit, est indispensable pour la réussite du programme de cyber-sécurité. Selon leur rapport 2015, « le président du comité d'audit peut jouer un rôle de coordination particulièrement efficace avec les autres acteurs, en faisant appliquer et en communicant les attentes en matière de sécurité et d'atténuation des risques ». Deloitte recommande également de recruter des administrateurs expérimentés en cyber-sécurité au sein du comité d'audit, qui seront en mesure de prendre des décisions avisées sur le caractère suffisant des actions qu'ils supervisent.

Le Conseil et le comité d'audit aident l'audit interne à préserver son indépendance en manifestant leur engagement dans la supervision de la fonction, explique Jim Pelletier. « Dans certaines situations, ils peuvent demander : « Où était donc l'audit interne ? » la réponse que je leur apporterais serait la suivante : « l'audit interne se trouve là où vous l'avez placé ». Il revient au Conseil et au comité d'audit de veiller à ce que l'audit interne jouisse d'un positionnement élevé garantissant un accès suffisant « sans crainte ou inquiétude quant aux sujets dont il se saisit. L'audit interne traite les sujets que le Conseil considère les plus importants ».

Peu de temps après l'attaque de *#WannaCry,* l'*Audit Executive Center* de l'IIA a publié des conseils visant à clarifier ce que le Conseil peut attendre de la part de l'audit interne pour une protection optimale contre les cyber-risques :

- Une évaluation détaillée des activités opérationnelles clés de l'organisation, identifiant l'infrastructure informatique, afin de s'assurer que le périmètre de l'évaluation des cyber-risques est adéquat. Au lieu de partir d'une liste des systèmes ou protections déjà en place, il s'agit de partir des activités essentielles et de les rattacher à une infrastructure.
- Une réévaluation de la robustesse de l'évaluation des cyber-risques, en veillant à ce qu'elle prenne en compte toutes les complexités et nuances inhérentes à ces derniers.
- Une révision des plans de continuité d'activité afin de garantir qu'ils couvrent tous les scénarios résultant de cyber-attaques et qu'ils envisagent comment les activités vont se poursuivre – et pas uniquement que les joyaux de la couronne sont protégés.
- Le lancement de programmes éthiques de piratage pour déceler les vulnérabilités dont une cyber-attaque pourrait tirer parti. Les changements technologiques rapides exigent que ces mesures soient prises de façon continue et non pas périodique dès l'apparition d'un problème.
- Une révision des opérations informatiques de base autour de la gestion des correctifs. Celle-ci est certainement déjà inscrite au plan d'audit, mais doit être accélérée compte tenu des événements actuels.
- Une révision des programmes et des efforts visant à ce que les employés soient bien formés et informés quant à leur rôle essentiel dans la prévention des cyber-attaques.

Déplacer l'accent de la sécurité vers la résilience

Le rapport Pulse 2016 de l'IIA a souligné le besoin de déplacer l'accent de la cyber-sécurité vers la cyber-résilience, compte tenu du consensus croissant des experts sur le fait qu'il s'agit plus de savoir quand l'organisation va subir une cyber-attaque que de se demander si elle va avoir lieu. Parmi les 90 % de personnes interrogées ayant indiqué que leur organisation dispose d'un plan de continuité d'activité, seulement 25 % confirment que le plan fournit des procédures claires et spécifiques pour répondre à une cyber-attaque. 17 % des personnes interrogées signalent que leur plan ne propose aucune procédure. Si un plan de continuité d'activité ne fournit pas de procédures détaillées pour répondre à une cyber-attaque, le rapport recommande que l'audit interne veille à ce que les procédures soient incluses ailleurs, comme dans un plan de résolution des incidents par exemple, pouvant être rattaché ou non au plan de continuité d'activité.

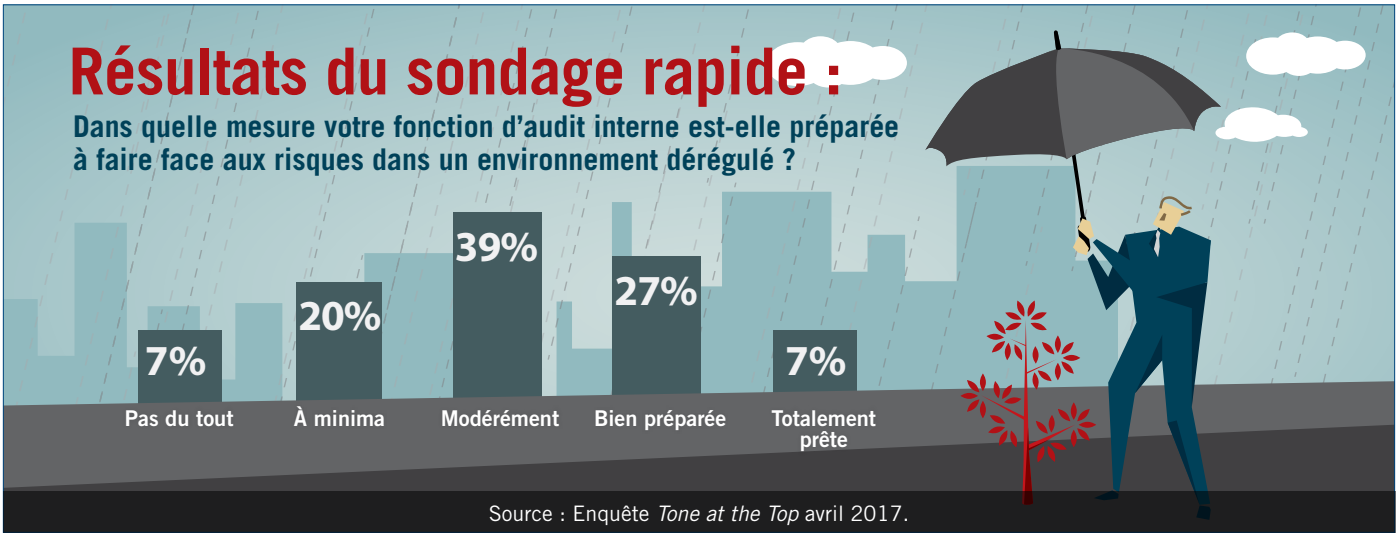
Le rapport de Deloitte & Touche, « *Cybersecurity: The Changing Role of the Audit Committee and Internal Audit* » envisage la résilience comme un des trois piliers d'un plan de défense fiable en matière de cyber-sécurité. *The Center for Audit Quality* semble également considérer que les organisations devraient se focaliser sur la façon de répondre et de rebondir suite à une attaque, au lieu de se limiter à des mesures préventives.
Le livre blanc du *Center for Audit Quality* définit le rôle du plan de continuité d'activité dans la gestion des risques en matière de cyber-sécurité : *How the auditing profession promotes cybersecurity resilience* sera bientôt publié et abordera l'évolution du rôle de l'auditeur en matière de cyber-sécurité.

Question de sondage rapide

Dans quelle mesure la culture de votre organisation a-t-elle une influence positive sur sa cyber-résilience ?

Aucune | **À minima** | **Modérément**
Grandement | **Je ne sais pas**

Visitez notre site à l'adresse **www.theiia.org/tone** pour répondre à la question et connaître les réponses des autres parties intéressées.



2017-0135