LE RÔLE DE L'AUDIT INTERNE FACE AUX CYBERISQUES

IMPORTANCE D'UNE APPROCHE GLOBALE

Face aux risques actuels de cyberattaques, la plupart des organisations concentrent leurs ressources de cybersécurité sur la prévention.

Ainsi, selon Gartner, leader mondial des études et du conseil en systèmes d'informations (SI), les dépenses de sécurité des SI devraient atteindre 77 milliards de dollars en 2015, soit une hausse de 8 % par rapport à l'année précédente.

Toutefois, ce serait un calcul à courte vue, voire désastreux, de se contenter de barrer la route aux cyberpirates. Les brèches récentes, aussi bien dans les grandes entreprises que dans les administrations, ont révélé l'incapacité de ces organisations à empêcher les attaques même lorsque des moyens considérables étaient investis dans la cyberdéfense. La question n'est pas tant de savoir si une telle attaque aura lieu, mais plutôt de savoir quand. Il faut donc envisager la cybersécurité sous un angle global, afin d'être parfaitement préparé, en amont, pendant, et après l'attaque.

Une fonction d'audit interne robuste, dotée de ressources suffisantes et bénéficiant des formations nécessaires constitue, pour les Conseils et les comités d'audit, l'un des principaux atouts pour l'élaboration et l'amélioration des stratégies, politiques et protocoles destinés à protéger l'ensemble de l'organisation face aux cybermenaces.

Une fonction d'audit interne efficace dispose en effet de la vision à 360 degrés nécessaire pour aider l'organisation à anticiper les cyberattaques, leur résister et rebondir. En outre, cette fonction offre, en tant que prestataire d'assurance indépendant, l'expérience, les compétences et les connaissances requises pour déterminer les forces et les faiblesses de l'organisation en matière de cybersécurité et pour évaluer et renforcer ses capacités en la matière.

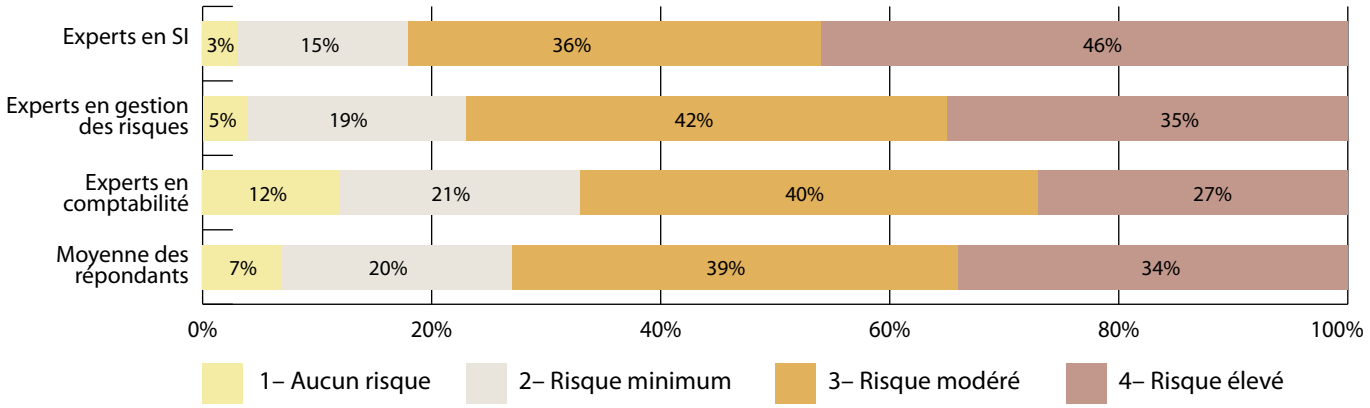
Il n'est donc pas surprenant que les auditeurs internes entrevoient déjà clairement les conséquences dommageables que pourraient avoir, pour leur organisation, d'éventuelles cyberattaques. Sept répondants sur dix à l'enquête mondiale « *Common Body of Knowledge* » (CBOK) sur les pratiques de l'audit interne menée par l'IIARF *(Institute of Internal Auditors Research Foundation)* jugent modérés à élevés les risques inhérents de violation de données susceptibles de porter atteinte à l'image de marque de leur organisation (voir graphique 1).

« *Je ne pense pas, à en juger par mon expérience, que les organisations aient adopté une approche globale en matière de sécurité des données* », indique James Reinhard (CPA, CIA, CISA), responsable de l'audit chez Simon Property Group.

James Reinhard, qui enseigne également l'audit des SI, estime que les responsables de l'audit interne sont

Copyright © 2015. All rights reserved.

Graphique 1 : Niveaux du risque relatif à la violation de données susceptibles de porter atteinte à l'image de marque



Note : D'après l'édition 2015 de l'enquête mondiale CBOK sur la pratique de l'audit interne menée par l'IIARF. Q.93 : À votre avis, quel est le niveau de risque inhérent de votre organisation pour les domaines émergents des systèmes d'information suivants ? Ensemble des répondants à travers le monde. Les réponses « Sans objet/Je ne sais pas » n'ont pas été prises en compte. Pour des raisons d'arrondi, le total peut parfois différer de 100 %. n = 9 426.

particulièrement bien placés pour former les membres du Conseil et du comité d'audit sur les différents efforts à envisager pour lutter contre les cybermenaces, en identifiant notamment les failles existantes.

« *Le problème, en ce qui concerne la cybersécurité est que la nature du risque reste inconnue. C'est pourquoi les Conseils et les comités d'audit ne l'envisagent pas de la même manière que les autres risques susceptibles de perturber l'activité* », indique James Reinhard. « *Il incombe au responsable de l'audit interne d'impliquer le directeur des systèmes d'information (DSI) ou un membre de la direction de la communication pour commencer à sensibiliser les équipes sur ce qui a déjà été fait au sein de l'organisation.* »

Les Conseils et les comités d'audit doivent, par conséquent, être tenus informés des technologies qui peuvent non seulement aider à atteindre les objectifs opérationnels, mais également rendre l'organisation plus vulnérable face aux attaques. L'audit interne, une fois obtenus les ressources et le support nécessaires, développera les compétences et les approches nécessaires pour effectuer des revues et fournir des services d'assurance dans ce domaine.

La DSI peut s'appuyer sur la gouvernance des SI, qui définit clairement les procédures et les rôles et attributions de chacun au sein de l'équipe, pour mieux gérer ses responsabilités et son soutien à l'organisation. La mise en place d'un tel cadre permet à la DSI de mieux repérer les anomalies potentielles au quotidien et à partir de certaines tendances, d'où une meilleure identification des causes sous jacentes.

Source : GTAG 17 : Auditing IT Governance - IIA, 2012.

La préparation aux cyberattaques s'articule autour de cinq grands axes. L'audit interne peut contribuer à chacun d'entre eux de la façon suivante :

PROTECTION :

Etre un allié pour maintenir à distance les intrus

L'audit interne offre une approche globale qui permet d'identifier les zones de vulnérabilité de l'organisation. Qu'il s'agisse de tester les politiques « Apportez vos outils personnels » (*Bring Your Own Device* ou BYOD) ou de vérifier la conformité aux protocoles de sécurité des contrats avec les sous-traitants, l'audit interne apporte un précieux éclairage en matière de protection. L'efficacité de la gouvernance des SI est également essentielle, et l'audit interne peut fournir des services d'assurance également dans ce domaine.

DÉTECTION :

Identifier les signes manifestes de brèches dans la sécurité

L'analyse des données, lorsqu'elle est efficace, donne souvent aux organisations un premier indice que quelque chose cloche. L'analyse des données et d'autres technologies sont de plus en plus intégrées aux travaux d'audit interne. Selon l'édition 2015 de l'enquête CBOK sur les pratiques de l'audit interne, cinq répondants sur dix s'appuient sur l'extraction et l'analyse des données pour la surveillance des risques et des contrôles. Ces techniques servent également à l'identification de fraudes et à bien d'autres activités (voir graphique 2). Les responsables de l'audit interne devraient travailler en collaboration avec la DSI pour développer et suivre les principaux indicateurs de risque et établir des relations professionnelles étroites avec le DSI et le responsable de la sécurité des systèmes

d'information pour s'assurer que des contrôles appropriés et efficaces sont en place.

CONTINUITÉ D'ACTIVITÉ :

Poursuivre l'activité coûte que coûte

Une planification adéquate est importante pour pouvoir gérer et surmonter tous les scénarios susceptibles d'avoir un impact sur les opérations courantes de l'organisation, qu'il s'agisse d'une cyberattaque, d'une catastrophe naturelle, ou d'un changement de dirigeant. Il est essentiel, pour la survie de l'organisation, que les clients et autres parties prenantes continuent de bénéficier des services de l'organisation, quelles que soient les circonstances. L'audit interne peut fournir une assurance concernant l'efficacicité et l'efficience des plans de continuité à l'échelle de l'organisation.

GESTION DE CRISE / COMMUNICATION :

Ne pas céder à la panique

À l'instar des plans de continuité d'activité, la préparation, en matière de gestion et de communication de crise peut avoir un impact sensible et positif sur les clients, les parties prenantes et la réputation de l'organisation. L'audit interne peut contribuer au développement d'un tel plan, en vérifier l'efficacité et le caractère opportun des délais de réaction, et, à terme, fournir une analyse critique du plan une fois mis en œuvre.

AMÉLIORATION CONTINUE :

Se relever des cendres

C'est à ce stade que l'audit interne peut offrir le plus de valeur. En effet, compte-tenu de son périmètre de responsabilité étendu, l'audit interne peut mettre à profit les informations glanées au fil de ses différentes missions. Une bonne préparation aux cyberattaques permet de survivre à de telles attaques, mais de telles victoires sont vaines si l'organisation n'évolue pas et n'améliore pas ses stratégies et ses protocoles pour mieux se préparer aux attaques suivantes.

Comment les auditeurs internes peuvent-ils optimiser le plan de continuité d'activité ?

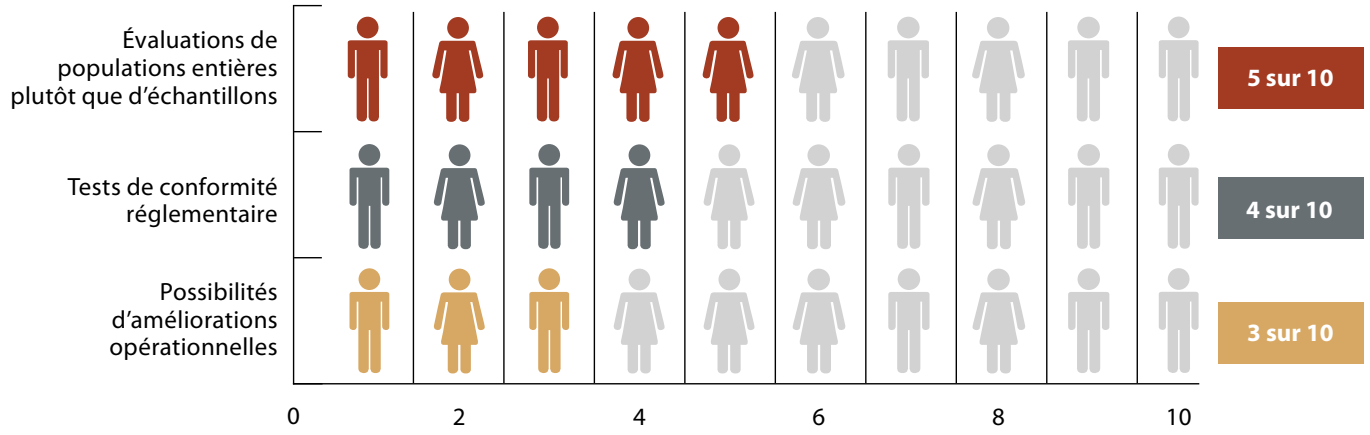
1. En collaborant avec le management pour comprendre le plan et ses objectifs.
2. En échangeant des idées avec le management afin d'améliorer constamment le processus.
3. En aidant le management à définir un cadre afin de prendre les bonnes décisions pour limiter les risques et accroître la résilience de l'organisation.

Source : GTAG 10 : Gestion de la continuité d'activité - IIA, IFACI, 2008.

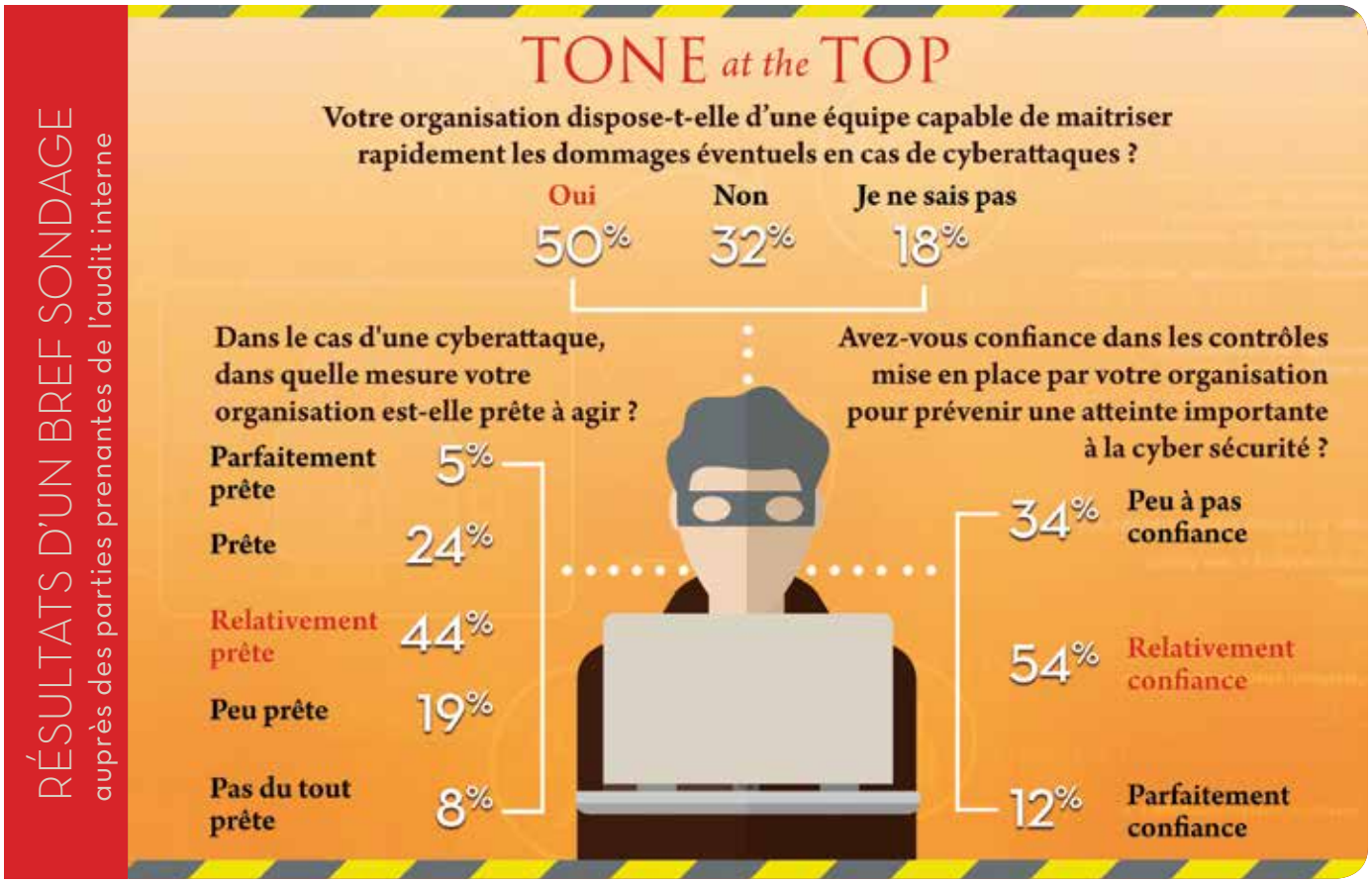
CONCLUSION

Les cyberattaques sont indissociables de la réalité économique actuelle, et les risques inhérents aux nouvelles technologies continueront d'émerger, à un rythme de plus en plus soutenu. L'audit interne peut jouer un rôle important en aidant l'organisation à survivre dans un monde en proie aux cyberattaques, notamment en aidant les Conseils à se poser les bonnes questions en matière de cybersécurité. Seules les organisations qui développent les compétences requises pour faire face à de telles menaces tant au niveau stratégique que tactique pourront survivre et prospérer. Et une fonction d'audit interne bénéficiant du soutien et des ressources nécessaires constitue à cet égard un partenaire essentiel.

Encadré 2 : Utilisation de l'exploitation et de l'analyse de données



Note : D'après l'édition 2015 de l'enquête mondiale CBOK sur la pratique de l'audit interne menée par l'IIARF. Q96 : Votre département d'audit interne utilise-t-il l'extraction ou l'analyse de données pour les activités suivantes ? Ensemble des répondants à travers le monde. n = 10 088.



Source : Tone at the Top (Altamonte Springs, Floride : The Institute of Internal Auditors, mars/avril 2014 et janvier/février 2015).

AMÉLIORER L'ACCÈS DU CONSEIL À LA CYBEREXPERTISE

Développer l'expertise en matière de cybersécurité ou de sécurité des SI au niveau du Conseil devient un impératif pour un nombre croissant d'organisations. L'explication est simple. Selon la Public Company Governance Survey de la National Association of Corporate Directors, 87 % des répondants déclarent que la compréhension, par le Conseil, des risques liés aux SI doit être améliorée.

Les comités de nomination et de gouvernance doivent réaliser de nombreux arbitrages pour pourvoir les postes d'administrateurs vacants, et tenir compte notamment de l'expertise sectorielle des candidats, de leurs connaissances financières, de leur expérience internationale, ou encore d'autres compétences requises, suivant les besoins stratégiques de l'organisation et les circonstances.

Qu'ils décident ou non d'opter pour un administrateur doté d'une expertise spécifique en matière de cybersécurité, les dirigeants peuvent mettre à profit d'autres moyens d'attirer l'attention du Conseil sur des perspectives bien éclairées dans ce domaine :

- en programmant des entretiens approfondis avec des experts extérieurs, notamment des entreprises spécialisées en cybersécurité, des administrations publiques, des associations professionnelles, etc. ;
- en capitalisant sur le réseau existant de conseillers indépendants du Conseil, comme les auditeurs externes et les avocats, qui disposent d'une vision étendue, à l'échelle du secteur dans son ensemble et de différentes entreprises, des tendances en matière de cyberisques ;
- en participant à différents programmes de formation des dirigeants, en interne ou à l'extérieur.

Source : Cyber-Risk Oversight, Director's Handbook Series (Washington, DC : National Association of Corporate Directors, 2014), disponible à l'adresse : https://www.nacdonline.org/cyber