



Le rôle du conseil d'administration et du comité d'audit dans la gouvernance des TI

Les membres du Réseau canadien des comités d'audit (RCCA) se sont réunis le 27 juin 2011 à Toronto pour discuter de la manière dont s'y prennent les conseils d'administration et les comités d'audit pour surveiller les risques de plus en plus complexes qui sont associés aux technologies de l'information (TI). Kathy Lisson, associée membre du groupe des Services consultatifs d'Ernst & Young, et Tony Ritlop, leader de gamme de services affecté au groupe canadien Risque de TI et certification de la Société, se sont joints à eux pour l'occasion. Le présent document résume les principaux faits saillants de la réunion.¹ **La liste des membres du RCCA ayant participé à cette réunion figure à l'annexe 1, à la page 14.**

Sommaire

Bien que les avancées technologiques récentes aient procuré aux entreprises un avantage concurrentiel important, l'avènement des nouvelles technologies a eu pour effet de compliquer les programmes de TI de bien des entreprises et d'exposer celles-ci à des risques avec lesquels elles ne sont pas familières. «Notre société tire des TI l'un de ses principaux avantages concurrentiels, explique un membre du RCCA, mais l'adoption des nouvelles technologies va de pair avec de nombreux risques que le conseil d'administration n'a pas l'habitude de surveiller.» Dans le cadre de la réunion, qui a amené les membres du RCCA à discuter de leurs préoccupations en matière de surveillance des risques, des pratiques efficaces en la matière et des leçons apprises, trois grands enjeux ont été signalés. Ces enjeux sont résumés ci-après, puis analysés plus en détail dans les pages subséquentes.

- **Nouveaux risques commerciaux découlant des progrès rapides dans le secteur des TI** (page 2)

De nouvelles technologies telles que l'informatique en nuage et de la prolifération des médias sociaux découlent de nouveaux avantages commerciaux pour les entreprises, lesquelles doivent désormais faire face à de nouveaux risques qui les contraignent à revoir leurs méthodes d'atténuation, y compris leurs processus de contrôle de la sécurité des données et des accès. Les cyberattaques sont devenues des menaces permanentes d'atteinte à la propriété intellectuelle des administrations publiques et des entreprises. Ces attaques informatiques, qui émanent souvent de l'extérieur de l'Amérique du Nord, sont difficilement détectables et parviennent souvent à déjouer les outils de sécurité informatique habituels.

- **La surveillance des TI, une responsabilité commune du conseil d'administration et du comité d'audit** (page 6)

La fonction dont relève la responsabilité de la surveillance des TI varie d'une entreprise à l'autre, selon si les TI jouent un rôle déterminant ou non dans l'obtention des avantages concurrentiels recherchés. Cependant, selon ce qu'affirment les membres du RCCA, le conseil d'administration doit généralement s'occuper des enjeux importants en matière de TI qui interfèrent avec la stratégie de l'entreprise, tandis

¹ La publication VantagePoint reflète l'utilisation par le RCCA de la version modifiée des règles de Chatham House, en vertu desquelles le nom de ses membres et les liens qui les unissent à leur société sont de notoriété publique, la paternité des propos tenus au cours des réunions n'étant toutefois pas attribuée à des personnes ou à des sociétés.



qu'il incombe au comité d'audit de prendre l'initiative en ce qui a trait aux enjeux qui sont davantage d'ordre tactique. Certaines entreprises qui se sont engagées dans d'importants projets de mise en œuvre de systèmes de TI ont été amenées à mettre sur pied un comité spécial du conseil d'administration ou un comité conjoint constitué d'administrateurs et de membres de la direction.

▪ **L'amélioration de la surveillance des TI par les conseils d'administration et les comités d'audit** (page 8)

Les membres du RCCA affirment que le conseil d'administration de leur entreprise a mis au point des pratiques visant à lui permettre de se familiariser avec les TI et de mieux cerner les risques qui y sont associés. L'établissement de relations avec le chef des finances, l'acquisition d'une meilleure connaissance du programme de TI et la recherche de nouvelles sources de compétences en TI comptent parmi ces pratiques. Une liste de questions que les comités d'audit doivent se poser à l'égard des TI figure à l'annexe 2, à la page 15.

Nouveaux risques commerciaux découlant des progrès rapides dans le secteur des TI

Bien que les nouvelles technologies fassent souvent miroiter aux entreprises des avantages extraordinaires, elles ont aussi pour effet de compliquer la gouvernance des TI. M^{me} Lisson et M. Ritlop soutiennent que les conseils d'administration et les comités d'audit doivent être au fait de quatre tendances : la menace d'usurpations systématiques de la propriété intellectuelle, l'informatique en nuage, les médias sociaux et l'incidence des nouvelles technologies sur les contrôles de sécurité et le contrôle des accès.

Risques importants associés aux menaces sophistiquées et persistantes

M^{me} Lisson définit une menace sophistiquée et persistante comme une menace que fait peser sur les armées, les administrations publiques et les entreprises occidentales un adversaire s'étant donné comme mission d'usurper des renseignements qu'elles détiennent en se livrant à des attaques constantes sur leurs systèmes informatiques. «Il ne s'agit pas de pirates informatiques au sens où nous l'entendons habituellement, mais plutôt de groupes bien organisés qui bénéficient d'excellentes sources de financement, qui sont généralement parrainés par un État et qui piratent et surveillent leurs cibles pendant de nombreuses années dans le but de s'emparer de leur propriété intellectuelle, explique-t-elle. Si, dans un premier temps, ces groupes se concentraient sur les organismes publics et les entreprises du secteur de la défense, ils ciblent désormais des entreprises dans tous les secteurs d'activité.» M^{me} Lisson précise que ces attaques sont particulièrement difficiles à détecter, car elles visent certains fichiers hébergés dans des dispositifs de stockage d'une entreprise afin de les en extraire en passant par le réseau. «Pour repérer ces attaques, il faut surveiller le trafic de données sur le réseau, en restant à l'affût des flux de données massifs», soutient-elle. Ce qui est encore plus troublant, c'est que les spécialistes des TI affirment que les moyens de défense habituels ne permettent pas aux entreprises de se protéger adéquatement contre les menaces sophistiquées et persistantes.²

«Après avoir été victimes de telles attaques, des entreprises occidentales constatent que des produits mis au point dans d'autres pays ressemblent à leurs propres produits, explique M^{me} Lisson. Elles sont alors amenées à établir un lien avec des attaques qui se sont produites dix ans plus tôt.» Pour contrer ces attaques, M^{me} Lisson

² William Jackson, "Are Advanced Persistent Threats Here to Stay?" *Defense Systems*, 1^{er} avril 2011.



et M. Ritlop recommandent aux entreprises d'adopter une stratégie de résistance équilibrée reposant à la fois sur des mesures de prévention, des outils de détection et un plan d'intervention en cas d'incident.

Importance pour le comité d'audit de connaître les coûts et avantages associés à l'informatique en nuage

M^{me} Lisson définit l'informatique en nuage comme «l'utilisation d'Internet pour accéder à un logiciel tiers qui est hébergé sur un dispositif matériel tiers, lequel dispositif se trouve dans un centre informatique exploité par un tiers». La possibilité d'accéder à de l'information à partir de n'importe où, la prestation rapide de services, l'abaissement des coûts unitaires du stockage de données et l'obtention de copies de sauvegardes sécuritaires permettant de prévenir les pertes de données sont au nombre des avantages associés à l'informatique en nuage. Celle-ci permet également aux entreprises d'éviter d'avoir à investir massivement dans leurs programmes d'immobilisations, de réaliser des économies de coûts au chapitre de la maintenance et de s'épargner bien des tracas. «L'informatique en nuage est populaire, elle est très accessible et elle permet de bénéficier de beaucoup de souplesse», soutient M^{me} Lisson. «Grâce à l'informatique en nuage, une entreprise qui dispose de cinq serveurs a la possibilité de bénéficier d'une capacité équivalant à 500 serveurs», explique un président de comité d'audit. En raison des avantages qu'elle offre, l'informatique en nuage ne cesse de croître en popularité. Une étude qu'Ernst & Young a réalisée en 2010 révèle que 45 % des entreprises ont déjà recours à des services d'informatique en nuage ou prévoient y recourir au cours des 12 prochains mois,³ ce qui ne manque pas d'étonner bien des membres du RCCA.

Néanmoins, l'informatique en nuage comporte des risques, et des coûts cachés pourraient s'y rattacher. M^{me} Lisson et M. Ritlop expliquent que les données qui sont hébergées sur des serveurs exploitant la technologie de l'informatique en nuage sont gérées en commun, de sorte que les données d'une entreprise sont contiguës à celles d'une autre entreprise et qu'elles ne sont pas séparées physiquement. En outre, les membres du personnel d'un prestataire de services d'informatique en nuage qui ont un profil d'administrateur peuvent accéder à l'ensemble des données hébergées sur n'importe quel serveur. Certaines entreprises s'inquiètent du fait que les prestataires de services d'informatique en nuage pourraient transmettre à leur insu leurs données à des organismes d'application de la loi ou à d'autres organismes publics. Ce qui les préoccupe, ce n'est pas que leurs données puissent être transmises – puisqu'elles sont évidemment disposées à satisfaire à toute demande en ce sens émanant des autorités – mais plutôt qu'elles puissent ne pas le savoir. L'accessibilité aux données qu'une entreprise décide de stocker dans un nuage est une question qui préoccupe l'un des membres du RCCA. M^{me} Lisson reconnaît que l'accès aux données peut poser problèmes lorsqu'il se révèle nécessaire de récupérer celles-ci, du fait que la plupart des prestataires de services d'informatique en nuage n'offrent pas de services prioritaires de récupération de données. Évoquant une question qui préoccupe particulièrement les comités d'audit, elle souligne également qu'étant donné le caractère nouveau de l'informatique en nuage, la surveillance de l'exactitude de la facturation des utilisateurs (pour les acheteurs de services d'informatique en nuage) et de la comptabilisation des revenus (pour les vendeurs) est essentielle.

³ Ernst & Young, *“Borderless Security: Ernst & Young's 2010 Global Information Security Survey.”* (Ernst & Young Global Limited, 2010), 8.



«Je crois que l'informatique en nuage va transformer le secteur, mais qu'aucune solution ne permet pour le moment de remédier aux lacunes des politiques en matière de TI sur le plan de l'accès aux données et de leur récupération», allègue M^{me} Lisson. Abondant dans le même sens, l'un des membres du RCCA tient les propos suivants : «Nous devons connaître les risques auxquels nous sommes exposés. Je compte bien demander au chef de l'information de mon entreprise si nous tirons suffisamment parti de l'informatique en nuage.»

Importance pour le comité d'audit de veiller à la mise en œuvre de directives claires sur l'utilisation des médias sociaux

Dans l'édition de l'année dernière de son étude annuelle sur les médias sociaux, la maison de sondages Burson-Marsteller a révélé que 79 % des cent entreprises les plus importantes figurant au palmarès *Fortune Global 500* ont recours à au moins un type de médias sociaux – comme Twitter, Facebook, YouTube ou des blogues d'entreprise – pour diffuser leurs messages.⁴ Or, l'édition de cette année révèle que les entreprises emploient maintenant les médias sociaux non seulement pour la diffusion systématique de leurs propres messages, mais aussi pour s'engager directement et activement dans des échanges avec les utilisateurs.⁵ En plus de favoriser les échanges entre les entreprises et leurs clients, les sites de médias sociaux peuvent aider les employés à innover davantage et à accroître leur productivité.⁶ Pourtant, les médias sociaux sont une menace pour les données des entreprises. «Il y a un risque que des employés soient à l'origine de fuites de données involontaires ou non, affirme M^{me} Lisson. Maintenant qu'un employé peut prendre la photo d'un écran à l'aide de son téléphone et l'afficher sur un site, la restriction de l'accès aux sites de médias sociaux à partir du bureau n'est plus une mesure efficace pour protéger les entreprises.»

En outre, les sites d'agrégation de documents tels que Docstoc, Scribd et SlideShare encouragent les utilisateurs à publier en ligne des documents relatifs aux politiques. «Les représentants de Docstoc ont déclaré publiquement qu'ils souhaitent que leur site devienne l'équivalent de YouTube dans le secteur des sites de publication de documents professionnels, souligne M^{me} Lisson. Si vous interrogez Internet en tapant le nom de votre entreprise et le mot *confidentiel*, des documents confidentiels de votre entreprise s'afficheront probablement à votre écran.»

La nouvelle ère des médias sociaux commande l'adoption de nouvelles politiques régissant leur utilisation. M^{me} Lisson et M. Ritlop recommandent aux entreprises de se doter d'une politique globale claire prévoyant des sanctions en cas d'utilisation inappropriée des médias sociaux : «Il y a lieu pour les entreprises de procéder à la mise à jour de leur politique de façon à ce qu'elle balise l'utilisation des médias sociaux et des tablettes électroniques. Il faut également que ces politiques aient du mordant. Si personne n'a de comptes à rendre aux cadres hiérarchiques à cet égard, c'est probablement parce que les politiques sont inadéquates.»

⁴ Burson-Marsteller, "2010 Fortune Global 100 Social Media Study," *The Burson-Marsteller Blog*, 23 février 2010.

⁵ Burson-Marsteller, "2011 Fortune Global 100 Social Media Study," *The Burson-Marsteller Blog*, 15 février 2011.

⁶ Kristin Burnham, "Social Media Safety: Acceptable-Use Policies Are Critical," *CIO*, 8 avril 2010.



Importance grandissante du contrôle de la sécurité des données et des accès

Bien que les enjeux relatifs au contrôle des accès ne soient pas nouveaux, la prolifération des systèmes dans les entreprises fait en sorte que ce contrôle devient de plus en plus complexe et difficile à surveiller. «Auparavant, la priorité était d'accorder en temps opportun les privilèges d'accès appropriés aux bons utilisateurs, commente M^{me} Lisson. C'est maintenant l'inverse : la principale priorité doit être de retirer rapidement aux utilisateurs les privilèges d'accès qu'ils ne devraient pas avoir.» «Le contrôle des accès repose beaucoup sur les interactions humaines, rappelle un membre du RCCA. Bien des employés affirment que leur supérieur ne sait même pas à quels systèmes ils ont accès.»

Le foisonnement des dispositifs mobiles permettant d'accéder aux réseaux des entreprises a pour effet d'amplifier ces risques. «Dans mon entreprise, nous avons récemment dressé l'inventaire des dispositifs mobiles de nos employés, relate un président de comité d'audit membre d'un autre réseau. Mon entreprise compte quelque 7 000 employés. Nous avons constaté que ceux-ci ont à leur disposition environ 31 000 dispositifs à partir desquels ils peuvent accéder à notre réseau.» «L'un des principaux changements auxquels procèdent les entreprises pour améliorer le contrôle des accès consiste à mettre en œuvre des politiques fondées sur les rôles, plutôt que d'accorder des accès uniques à chaque employé, signale M^{me} Lisson. De plus en plus, les entreprises demandent à leur service des TI d'expliquer clairement aux gestionnaires en quoi consistent les privilèges d'accès qu'ils sont appelés à approuver pour leurs employés.»

Les entreprises peuvent aussi déroger à leur contrôle des accès lorsque des employés quittent leur emploi. Ainsi, 75 % des répondants à un sondage réalisé par Ernst & Young affirment être préoccupés (33 % se disant très préoccupés) quant à la possibilité que des employés ayant récemment quitté leur entreprise aient recours à des représailles.⁷ «Il semble y avoir là un problème de modèle de fonctionnement, signale un membre du RCCA. Le service des TI et les RH ne communiquent pas assez efficacement lorsque des employés quittent l'entreprise.» «C'est un problème qui ne se pose pas que pour les employés; les contractuels ont également accès à toutes sortes de systèmes», rappelle un autre membre du RCCA. Les membres du RCCA conviennent que l'amélioration des communications entre le service des TI et les RH permettrait de bonifier considérablement le processus de contrôle des accès.

M^{me} Lisson et M. Ritlop soutiennent que les privilèges d'accès accordés à des hauts dirigeants à titre exceptionnel peuvent parfois poser problèmes, du fait que ces dirigeants peuvent même ignorer qu'ils disposent de tels privilèges et qu'ils sont aussi habituellement autorisés à accéder à de l'information confidentielle à partir de leur domicile ou à l'aide de leur iPad. «Nous, les administrateurs, nous sommes dans une situation similaire, en ce sens qu'une foule de données confidentielles sont stockées dans nos tablettes électroniques», rappelle un membre du RCCA.

⁷ Ernst & Young, *Outpacing Change: Ernst & Young's 12th Annual Global Information Security Survey* (Ernst & Young Global Limited, 2009), 6.



Questions à poser au chef de l'information

M^{me} Lisson, M. Ritlop et plusieurs membres du RCCA suggèrent diverses questions que les administrateurs devraient poser au chef de l'information de leur entreprise au sujet des nouveaux risques de TI :

- Quels sont les éléments d'actif informationnel les plus importants pour notre entreprise? Quels sont les moyens mis en œuvre pour les protéger contre les menaces sophistiquées et persistantes? Comment effectuons-nous la surveillance des réseaux de façon à assurer le repérage des transferts de paquets de données volumineux hors des systèmes de l'entreprise?
- Quel pourcentage du budget du service des TI de notre entreprise est affecté à l'atténuation du risque de TI et à la sécurité informatique?
- En quoi consiste la stratégie de notre entreprise en matière d'informatique en nuage? Cette stratégie est-elle appropriée pour toutes les unités fonctionnelles? En quoi consiste notre stratégie de sortie en cas de problème avec un prestataire de services informatique en nuage? Sur le plan des coûts, des avantages et des risques, comment notre relation avec notre prestataire de services d'informatique en nuage se compare-t-elle à celles que nous entretenons avec les prestataires de services impartis traditionnels?
- De quels types de services d'informatique en nuage notre entreprise se prévaut-elle actuellement? Notre entreprise dispose-t-elle d'une politique relative aux achats de services d'informatique en nuage par des secteurs d'activité ou des fonctions individuels?
- De quels privilèges d'accès les dirigeants de notre entreprise bénéficient-ils à titre exceptionnel? Les dirigeants se prévalent-ils des privilèges d'accès qui leur ont été accordés? Quelle est l'incidence de ces privilèges d'accès sur le profil de risques de l'entreprise? Quels sont les moyens utilisés pour assurer la protection de l'information de l'entreprise à laquelle les dirigeants accèdent à partir de leur domicile?
- En quoi consiste la politique de notre entreprise en matière d'utilisation des médias sociaux? À quand remonte sa plus récente mise à jour? Dans quelle mesure s'agit-il d'une politique claire et efficace?
- À quand remonte les plus récentes recherches effectuées par l'équipe des communications et/ou l'équipe d'audit interne sur les principaux sites de médias sociaux et sites d'agrégation de documents dans le but de détecter des fuites d'informations confidentielles ou des commentaires sur l'entreprise ou ses dirigeants susceptibles de porter atteinte à notre marque?
- Des exercices de simulation d'incidents ou de brèches de sécurité graves ont-ils été effectués? Quel est le pire scénario envisagé?
- Notre entreprise fait-elle appel aux services de tiers pour tester l'efficacité de ses dispositifs de défense? Ces tiers ont-ils recours à la fois à des processus automatisés et à des processus manuels dans le cadre de leurs tentatives d'intrusion dans nos systèmes?



La surveillance des TI, une responsabilité commune du conseil d'administration et du comité d'audit

L'infrastructure de surveillance des TI est propre à chaque entreprise, et plusieurs membres du RCCA conviennent qu'elle dépend vraiment de la mesure selon laquelle les TI sont étroitement arrimées à la stratégie organisationnelle ou selon laquelle elles sont importantes pour que l'entreprise puisse conserver son avantage concurrentiel. «Les questions relatives aux TI doivent figurer à l'ordre du jour du conseil d'administration et du comité d'audit, allègue l'un des membres du RCCA. Le conseil d'administration doit déléguer au comité d'audit une partie de ses activités de surveillance, notamment la production des rapports d'audit interne sur les TI, mais il revient au conseil d'administration de se pencher sur les tendances et les risques importants.» Les membres du RCCA insistent sur l'importance d'établir une nette distinction entre les responsabilités, quelle que soit la fonction responsable de la surveillance. Quelques conseils d'administration se sont dotés d'un comité spécial chargé de surveiller les projets de TI exigeant une supervision étroite de la part des administrateurs.

Surveillance générale des TI par les conseils d'administration

Bien des membres du RCCA conviennent que le conseil d'administration dans son ensemble doit conserver la plupart des responsabilités à l'égard de la surveillance des TI, étant donné que ces dernières jouent un rôle crucial dans l'exécution de la stratégie organisationnelle. «Aux réunions du conseil d'administration, il est question des TI et de leur arrimage à la stratégie de l'entreprise, de la nécessité d'en tirer parti de façon à accroître notre avantage concurrentiel ou du risque que nous perdions cet avantage si nous tardons trop à prendre les mesures qui s'imposent, explique un membre du RCCA. Il ne suffit pas de débattre que de la stratégie en matière de TI, car celle-ci est en lien avec la stratégie des ventes, la stratégie d'exploitation et la stratégie de gestion.»

Plusieurs membres du RCCA s'entendent quant à la nécessité que les conseils d'administration assument la responsabilité à l'égard de la stratégie globale en matière de TI, mais certains conseils d'administration se chargent aussi de la surveillance des grands projets de TI de leur entreprise. «Quand il est question de projets de TI, le conseil d'administration a tendance à s'intéresser surtout aux questions relatives aux échéances et au budget, précise l'un d'eux. À cet égard, les projets de TI ne sont pas traités différemment des grands projets d'immobilisations. Le conseil d'administration est tenu au courant de leur avancement à l'occasion des séances de mise à jour; il vérifie alors si le calendrier d'exécution et le cadre budgétaire sont respectés. Il est très rare qu'il soit amené à examiner un projet en détail, à moins qu'il y ait un problème.»

Responsabilités particulières en matière de surveillance des TI qui incombent généralement aux comités d'audit

Selon les membres du RCCA, les activités de surveillance des TI dont s'occupe le comité d'audit sont généralement axées surtout sur les processus et contrôles entourant les TI, de même que sur les enjeux d'ordre tactique. Ils considèrent que le comité d'audit est le mieux placé pour comprendre dans quelle mesure les enjeux en matière de TI peuvent avoir une incidence sur l'information financière et les contrôles internes, étant donné qu'il s'intéresse de près aux états financiers de l'entreprise. D'autres membres du



RCCA soutiennent que les comités d'audit pourraient avoir un rôle plus important à jouer dans la surveillance des TI, mais qu'«il s'agit d'une question extraordinairement tributaire du secteur et de l'entreprise». Quelle que soit l'étendue de la surveillance exercée par le comité d'audit, bien des membres du RCCA affirment que les TI ont grimpé dans la liste des priorités de leur propre comité d'audit. À preuve, l'un d'eux a tenu les propos suivants : «Alors que l'étude des rapports relatifs à la sécurité de l'information figurait auparavant au verso du programme des activités de mon comité d'audit, elle y occupe maintenant une place de choix.»

Cependant, certains membres du RCCA s'inquiètent de la possibilité que l'accroissement des responsabilités du comité d'audit en matière de TI ait pour effet d'amoindrir sa capacité d'exercer une surveillance efficace. «Bien qu'il puisse être judicieux d'attribuer la responsabilité des TI au comité d'audit, cela ne va pas nécessairement de soi», allègue l'un d'eux. «Il vient un moment où il faut cesser d'alourdir la tâche du comité d'audit sur le plan de la surveillance, souligne un autre membre du RCCA. Si nos responsabilités en la matière continuent de s'accroître, nous finirons par surveiller tout ce qui représente un certain risque pour l'entreprise.»

Surveillance ponctuelle des TI par des comités spéciaux

Plusieurs membres du RCCA expliquent que leur entreprise a confié à un comité spécial le mandat de surveiller certains aspects des TI. Selon eux, l'excellence des orientations communiquées à la direction et la franchise des commentaires transmis au conseil d'administration, particulièrement dans le cadre de séances à huis clos, figurent parmi les avantages qui découlent de l'affectation d'administrateurs compétents à de tels comités. D'après eux, voici les deux principaux volets dont la responsabilité peut être confiée à un comité spécial :

- **Grands projets de TI** – Les membres du RCCA allèguent qu'il est rare que les administrateurs se réunissent assez fréquemment ou qu'ils disposent d'assez de temps pour assurer une surveillance étroite des grands projets de TI, ce qui amène certains conseils d'administration à mettre sur pied un comité spécial auquel ils confient cette responsabilité. «Les projets de TI peuvent rapidement échapper à notre contrôle lorsqu'ils ne sont pas suivis de près, explique l'un d'eux. Un comité qui se consacre entièrement à la surveillance des progrès accomplis contribue réellement à rassurer le conseil d'administration.»
- **Stratégie en matière de TI** – Le conseil d'administration auquel siège l'un des membres du RCCA «a établi un comité spécial qui se concentre sur la nouvelle stratégie en matière de TI de l'entreprise». Le comité spécial des TI de l'entreprise d'un autre membre du RCCA, qui «est constitué d'administrateurs et de dirigeants qui collaborent avec les membres de la direction concernés», est le fer de lance de la surveillance des programmes de TI.

Dans un seul cas, le conseil d'administration dont fait partie un membre du RCCA a mis sur pied un comité ayant pour mandat de surveiller les grands projets d'immobilisations de l'entreprise, dont les projets de TI : «Nous avons un comité de surveillance qui surveille les projets d'immobilisations d'envergure, et c'est à ce comité qu'il incomberait de suivre tout projet de TI important. En l'absence de tels projets, ce comité est



inactif. Il comprend des administrateurs et des dirigeants, et il relève du conseil d'administration dans son ensemble.»

Amélioration de la surveillance des TI par les conseils d'administration et les comités d'audit

D'après une étude de cas rapportée dans la publication *Harvard Business Review*, les modifications réglementaires ont eu une incidence sur la composition, le rôle et les responsabilités des conseils d'administration du monde entier. Selon cette étude, bien qu'il en ait résulté de meilleurs cadres de gestion des responsabilités fiduciaires des administrateurs, ces modifications ont fait en sorte que l'on accorde maintenant beaucoup moins d'attention qu'auparavant à l'analyse de la nature des systèmes d'information et de actifs de TI des entreprises, ou à leur gouvernance des TI, ainsi qu'au devoir de diligence concomitant. C'est ce qui expliquerait que les conseils d'administration n'ont pas démontré les compétences ou le niveau d'attention que requiert la bonne gouvernance des TI.⁸ Certains membres du RCCA sont d'accord avec ces constatations, l'un d'eux allant jusqu'à émettre le commentaire suivant : «Les conseils d'administration ne s'intéressent pas aux TI autant qu'ils le devraient; dans leurs programmes d'activité, les questions touchant les TI sont relativement sous-représentées.» Pourtant, bien des membres du RCCA affirment que leur conseil d'administration et leur comité d'audit ont adopté des pratiques qui leur permettent d'avoir une meilleure compréhension des programmes de TI de leur entreprise.

Établissement de relations plus étroites avec le chef de l'information

Reconnaissant que les conseils d'administration souffrent d'un manque de compétences en TI, bien des membres du RCCA allèguent que les administrateurs dépendent du chef de l'information «pour soulever les bonnes questions et communiquer la bonne information». Toutefois, au sein des équipes de haute direction, beaucoup de chefs de l'information n'ont pas la stature voulue : «Le chef de l'information joue un rôle plus important que jamais dans la réussite des entreprises, en raison du rôle déterminant que les TI jouent maintenant dans tous les aspects de leurs activités. Cependant, dans la plupart des entreprises, le chef de l'information n'est toujours pas considéré comme un pair par les autres membres de la haute direction, qui voient en lui un spécialiste dépourvu de l'ensemble des compétences en gestion dont il aurait besoin pour qu'ils puissent l'admettre comme l'un des leurs.»⁹

Bien que les membres du RCCA conviennent qu'il puisse en être ainsi dans certaines entreprises, ils sont nombreux à croire que les chefs de l'information de la nouvelle génération «réussissent à faire le pont entre les TI et les affaires», ce qui contribue à rehausser le rôle du chef de l'information. «Le rôle du chef de l'information est assurément beaucoup plus en vue maintenant qu'auparavant, affirme l'un des membres du RCCA. Le chef de l'information a maintenant sa place au sein de l'équipe de haute direction.» Certains membres du RCCA sont portés à croire que les chefs de l'information dont le rôle est maintenant mieux considéré sont ceux qui ont acquis une expérience des affaires et qui sont dotés d'aptitudes en leadership, qu'il ne s'agit donc pas de spécialistes ne détenant que des connaissances approfondies en TI. «Un excellent chef de l'information est en mesure de communiquer avec les administrateurs de façon à les rassurer quant à

⁸ Michael Parent et Blaize Horner Reich, *Governing Information Technology Risk* (Boston: Harvard Business School Press, 2009).

⁹ Peter S. Delisi, Dennis Moberg et Ronald Danielson, «Why CIOs Are Last Among Equals,» *Wall Street Journal*, 24 mai 2010.



sa capacité de faire progresser la stratégie de l'entreprise, en les convainquant qu'il n'est pas bon qu'à s'occuper des problèmes du passé, fait valoir l'un d'eux. Le chef de l'information doit d'abord avoir de bonnes aptitudes en affaires; ses compétences techniques viennent au second plan.»

Souvent, le niveau des interactions que le chef de l'information a avec le conseil d'administration et le comité d'audit dépend de l'importance des TI par rapport au modèle de fonctionnement et à la stratégie de l'entreprise. Certains membres du RCCA affirment que le chef de l'information de leur entreprise ne se présente devant le conseil d'administration qu'une fois par année (quand ce n'est pas moins), tandis que d'autres soutiennent que, dans leur entreprise, le chef de l'information assiste à presque toutes les réunions du comité d'audit. La majorité des membres du RCCA sont cependant d'accord avec l'un de leurs pairs qui souhaite avoir davantage d'occasions de rencontrer le chef de l'information de son entreprise. «J'aimerais mieux comprendre les exigences, les défis et les priorités concurrentes avec lesquels doit composer le chef de l'information de mon entreprise, explique un autre membre du RCCA. Il faudrait que je consacre davantage de temps à l'établissement d'une relation plus étroite avec lui.»

Les membres du RCCA évoquent deux moyens favorisant l'établissement de relations avec le chef de l'information :

- **Séances à huis-clos dans le cadre de réunions du conseil d'administration** – «Je crois que le conseil d'administration devrait s'entretenir en privé avec le chef de l'information, avance l'un des membres du RCCA. Il pourrait ainsi lui demander s'il dispose de ressources adéquates et s'il bénéficie du soutien de l'équipe de direction. À ma connaissance, de telles discussions n'ont pas lieu avec le chef de l'information.»
- **Interactions informelles** – «Je compte bien inviter à manger le chef de l'information de mon entreprise et en profiter pour aborder avec lui certains des enjeux dont nous avons discuté aujourd'hui», affirme l'un des membres du RCCA. «Je n'ai jamais eu de rencontres informelles avec le chef de l'information de mon entreprise, mais j'entends bien commencer à y remédier prochainement», allègue l'un de ses pairs.

Amélioration au chapitre de l'évaluation des programmes de TI

Plusieurs membres du RCCA ont fait part à leurs pairs de la façon dont le conseil d'administration et le comité d'audit procèdent pour se familiariser avec les programmes de TI de leur entreprise et pour les évaluer, en proposant l'adoption des mesures suivantes :

- **Analyse de la stratégie d'appui des TI aux objectifs de l'entreprise** – Les nouvelles initiatives de TI devraient surtout émaner des unités fonctionnelles, et non pas du service des TI : «Il revient aux unités fonctionnelles de prendre en charge leur stratégie et de réclamer les nouveaux outils dont elles ont besoin, explique l'un des membres du RCCA. Les TI devraient collaborer avec les leaders de l'entreprise et aider les unités fonctionnelles à atteindre leurs objectifs, en mettant à leur disposition les outils technologiques qu'il leur faut. Lorsque les unités fonctionnelles ne sont pas à l'origine de ce processus, elles ne font pas une utilisation adéquate ou optimale de ces outils.»



- **Recherche d'informations proactives** – Aux dires des membres du RCCA, les rapports sur les TI sont trop souvent réactifs : «Le conseil d'administration n'entend parler des TI que lorsque surviennent des brèches de sécurité.» Au lieu de rapports réactifs, certains comités d'audit souhaitent obtenir des rapports faisant le point sur les améliorations apportées par le service des TI et sur les plus récentes menaces auxquelles l'entreprise a été exposée. Dans l'entreprise de l'un des membres du RCCA, «le chef de l'information et le directeur des ressources humaines présentent un rapport conjoint au conseil d'administration. Ils discutent des tendances dans le secteur des TI ainsi que des systèmes et des compétences dont nous aurons besoin dans l'avenir.»
- **Remise en question du budget des TI** – Même s'ils n'ont pas besoin de comprendre chaque poste du budget des TI, les conseils d'administration et les comités d'audit peuvent avoir une bonne idée de l'adéquation de celui-ci en demandant au chef de l'information de leur exposer notamment les changements auxquels il procéderait si le budget des TI était augmenté d'un certain pourcentage. M. Ritlop suggère également de vérifier auprès du chef de l'information quel est le pourcentage du budget des TI affecté à la sécurité. «Les entreprises dont les pratiques en matière de sécurité de l'information sont de calibre mondial consacrent à la sécurité de 8 % à 10 % de leur budget des TI», explique-t-il.
- **Sollicitation de la rétroaction des utilisateurs** – En cherchant à recueillir de la rétroaction directement auprès des utilisateurs des systèmes de TI internes, tels que les leaders d'unité fonctionnelle, le conseil d'administration peut obtenir un meilleur éclairage sur le programme de TI de l'entreprise et sur la valeur qui en découle. «Il est approprié de s'entretenir avec les leaders d'unité fonctionnelle pour comprendre leurs frustrations ainsi que les aspects du programme de TI de leur entreprise dont ils sont satisfaits», soutient un membre du RCCA.

Importance de tirer parti des connaissances internes et externes

Les membres du RCCA conviennent que bien des administrateurs «n'ont tout simplement pas les compétences nécessaires pour comprendre toute l'étendue des risques de TI. Les TI peuvent parfois faire penser à une boîte noire.» Des membres du RCCA proposent des ressources qui pourraient aider les conseils d'administration et les comités d'audit à mieux de familiariser avec les TI :

- **Audit interne** – La fonction audit interne est une ressource utile dans la détection des problèmes de TI, particulièrement en ce qui a trait aux systèmes d'information financière et aux contrôles internes. Du fait qu'elle a une vue d'ensemble des activités de l'entreprise, elle est en mesure de relever les risques individuels pouvant indiquer la présence de risques systémiques. «La fonction audit interne recense en permanence les enjeux relatifs au contrôle des accès à l'échelle des diverses unités fonctionnelles, relate un membre du RCCA. Au lieu de détecter 17 petits problèmes, elle peut mettre ceux-ci en lien avec un enjeu donné révélant une déficience importante». «La fonction audit interne peut toutefois être limitée par son manque de connaissances en TI», signale un autre membre du RCCA. Pour remédier à la situation, l'entreprise d'un membre du RCCA met à contribution un modèle de cosourçage tirant parti des compétences en TI de l'un des Quatre Grands cabinets d'experts comptables : «Notre modèle de cosourçage est très efficace, car le tiers auquel nous faisons appel nous fait bénéficier de certaines



compétences en TI. Ce modèle nous a réellement permis de faire évoluer notre façon de voir les choses et d'intégrer les TI à notre stratégie.»

Auditeurs externes – Plusieurs membres du RCCA considèrent que les auditeurs externes pourraient communiquer davantage d'informations sur les TI au conseil d'administration et au comité d'audit. L'un d'eux pense que les auditeurs externes pourraient conseiller le conseil d'administration relativement aux nouvelles tendances, aux positions qu'il devrait prendre et aux questions qu'il devrait poser.

- **Exécution de tests de sécurité informatique par des tiers** – Plusieurs membres du RCCA affirment que leur entreprise a eu recours aux services de *pirates informatiques éthiques*, à savoir des prestataires de services de TI chargés d'effectuer des tentatives d'intrusion visant à détecter les faiblesses dans les systèmes des entreprises et à permettre à celles-ci de cerner certaines de leurs vulnérabilités. La plupart des membres du RCCA conviennent que les spécialistes de ce type permettent de vérifier l'efficacité des mesures de sécurisation que la direction affirme avoir mises en œuvre. Cependant, l'un des membres du RCCA se demande s'il est approprié que le conseil d'administration recrute lui-même de tels pirates informatiques : «Il est souhaitable que le conseil d'administration n'ait recours aux services de pirates informatiques que dans des circonstances exceptionnelles.»
- **Autres conseillers externes** – L'un des membres du RCCA croit que les conseils d'administration devraient pouvoir se tourner vers un tiers très compétent quand ils considèrent qu'ils ont besoin d'obtenir plus d'information. L'un de ses pairs explique que certaines entreprises font appel aux services des conseillers en TI d'un cabinet d'audit : «Nous avons recours à un cabinet d'audit pour renforcer l'effectif de notre équipe d'audit interne lorsque nous devons examiner un projet de TI». «Nous avons demandé à un cabinet d'audit d'examiner la sécurité des TI de notre entreprise, relate un président de comité d'audit rattaché à un autre réseau. Après nous avoir proposé trois solutions, ce cabinet a aidé la direction dans l'élaboration d'un tableau de bord des TI, dont le comité d'audit assure le suivi.» Cependant, des membres du RCCA conviennent que le recours à des conseillers externes n'est pas une solution courante et que le conseil d'administration ne s'y résout que lorsqu'il a besoin de se faire rassurer.
- **Administrateurs dotés de compétences en TI** – Bien que la plupart des conseils d'administration ne comptent pas d'administrateurs dotés de compétences particulières en TI, celui de l'entreprise de l'un des membres du RCCA cherche à recruter des administrateurs ayant de telles compétences : «Nous considérons que les compétences en TI font partie intégrante des qualifications de nos administrateurs. Ces compétences ont toujours figuré sur notre liste de critères, mais elles n'ont jamais été prioritaires... Or, il est maintenant plus important que jamais que les administrateurs soient dotés de ce type de compétences.» «Pourtant, il est difficile de découvrir des aspirants administrateurs compétents dans le secteur des TI; idéalement, il faudrait recruter un dirigeant qui assume toujours un rôle au sein de la fonction TI d'une entreprise ou qui soit à la tête d'une entreprise de TI, explique un autre membre du RCCA. Les administrateurs d'une telle trempe sont très peu nombreux.»



Conclusion

Une étude publiée récemment par Ernst & Young avance que, d'ici 2014, les dispositifs intelligents pourraient être davantage utilisés que les ordinateurs traditionnels pour accéder à Internet.¹⁰ Dans le cadre de la même étude, un consultant prédit que toutes les entreprises figurant au palmarès *Forbes Global 2000* auront recours aux services d'informatique en nuage.¹¹ Dans un avenir pas si lointain, il faudra pouvoir compter sur des compétences en TI encore plus pointues. Dans quelle mesure les conseils d'administration parviendront-ils à s'adapter à ces progrès technologiques et aux risques qui y sont associés? Les services de formation et de soutien dispensés aux administrateurs par des ressources internes et des ressources externes seront-ils suffisants ou les conseils d'administration devront-ils recruter des administrateurs dotés d'une expérience directe en TI? Comme l'affirme l'un des membres du RCCA, «les TI sont réellement devenues un moteur des entreprises, mais les conseils d'administration sont toujours dépourvus d'administrateurs dotés de compétences générales dans le domaine. Je ne sais trop si de telles compétences sont requises immédiatement, mais je constate que la situation évolue en ce sens.» Le moment où les conseils d'administration devront rehausser leur niveau de connaissance des TI approche peut-être davantage que bien des administrateurs sont portés à le croire.

Au sujet du présent document

Le Réseau canadien des comités d'audit (RCCA) est un groupe de présidents de comités d'audit de grandes sociétés qui se sont engagées à améliorer la performance des comités d'audit et à promouvoir la confiance envers les marchés des capitaux. Les réunions du RCCA, qui sont organisées par Ernst & Young et orchestrées par Tapestry Networks, visent à faciliter l'accès aux nouvelles meilleures pratiques ainsi que le partage des connaissances sur les principaux enjeux auxquels font face les comités d'audit dans le nouvel environnement où ils sont appelés à œuvrer.

La publication *VantagePoint* est publiée par Tapestry Networks afin de favoriser les discussions de fond en temps opportun au sein du conseil d'administration sur les choix auxquels les membres du comité d'audit, les dirigeants et leurs conseillers font face alors qu'ils s'évertuent à s'acquitter de leurs responsabilités respectives envers les investisseurs. Le principal mérite de la publication *VantagePoint* réside dans le fait qu'elle aide tous les membres du RCCA à préciser leur propre point de vue éclairé sur les enjeux importants de ce genre. Tous ceux et celles qui l'ont reçue sont invités à la mettre à la disposition des membres de leur propre réseau. Plus les administrateurs, les membres de la direction et leurs conseillers prendront systématiquement part au débat, plus la valeur qui en découlera pour tout le monde sera importante.

Les points de vue exprimés dans le présent document vont dans le même sens que ceux que défend le Réseau canadien des comités d'audit (RCCA). Ils ne coïncident pas nécessairement avec l'opinion individuelle des membres du réseau, ni avec le point de vue de leur société, d'Ernst & Young ou de Tapestry Networks. Pour obtenir un avis particulier, veuillez consulter vos conseillers. Ernst & Young désigne l'ensemble des membres d'Ernst & Young Global, y compris la société membre Ernst & Young LLP, aux États-Unis.

Le présent document a été préparé par Tapestry Networks, et les droits d'auteur qui y sont associés sont la propriété d'Ernst & Young. Son contenu peut être reproduit et diffusé, mais uniquement dans son intégralité, avec toutes les notices relatives à la protection des droits d'auteur et des marques de commerce.

¹⁰ Ernst & Young, *Tracking Global Trends: How Six Key Developments Are Shaping the Business World* (Ernst & Young Global Limited, 2011), 21.

¹¹ *Ibid.*, 22.



Annexe 1 : Participants à la réunion

Les membres suivants du réseau ont participé à la réunion :

- Bev Briscoe, présidente du comité d'audit de Goldcorp
- John Caldwell, président du comité d'audit d'IAMGOLD
- Peter Case, président du comité d'audit de Fortis
- John Clappison, président du comité d'audit de la Financière Sun Life
- Alan Horn, président du comité d'audit de Fairfax Financial Holdings
- Michel Labonté, président du comité d'audit de Metro
- David Leslie, président du comité d'audit d'Enbridge
- Eileen Mercier, présidente du comité d'audit de Groupe CGI
- Bob Steacy, président du comité d'audit de Domtar
- Barb Stymiest, présidente du comité d'audit de Research In Motion
- Ron Tysoe, président du comité d'audit de la Banque CIBC
- Paul Weiss, président du comité d'audit de BCE

Ernst & Young était représentée par les personnes suivantes :

- Richard Greisch, associé, Services de certification, Ernst & Young
- Tom Kornya, associé directeur, région du Grand Toronto, Ernst & Young Canada
- Kathy Lisson, associée, Services consultatifs, Ernst & Young Canada
- Tony Ritlop, leader de gamme de services, Risque de TI et certification, Ernst & Young Canada
- Rob Scullion, associé directeur, CSCE, Ernst & Young Canada

Les membres suivants ont pris part aux discussions avant et/ou après la réunion :

- Tom O'Neill, président du comité d'audit de Loblaw
- Jane Peverett, présidente du comité d'audit d'EnCana
- Ted Reevey, président du comité d'audit de Bell Aliant
- Stuart Smith, président du comité d'audit de Fonds de revenu Pages Jaunes



Annexe 2 : Questions que les comités d'audit doivent se poser

- ?** Quels enjeux et tendances en matière de TI ont le plus d'incidences sur les décisions d'ordre stratégique et tactique de notre entreprise? Quels sont ceux qui représentent les plus grands défis à relever et les principales possibilités à exploiter?
- ?** Dans quelle mesure les enjeux et les risques en matière de TI de notre entreprise évoluent-ils au fil du temps?
- ?** Quelles sont les modifications les plus importantes ayant été apportées à la politique de TI de notre entreprise au cours des dernières années?
- ?** Comment les responsabilités de surveillance des TI sont-elles réparties au sein du conseil d'administration, du comité d'audit et des autres comités du conseil d'administration? Dans quelle mesure le rôle du comité d'audit dans la surveillance des TI a-t-il changé au cours des dernières années?
- ?** Dans quelles circonstances le conseil d'administration pourrait-il envisager de mettre sur pied un comité permanent ou temporaire des TI constitué d'administrateurs?
- ?** Au cours des douze derniers mois, le temps que le conseil d'administration consacre aux enjeux en matière de TI a-t-il augmenté, a-t-il diminué ou est-il resté inchangé? À cet égard, quels changements prévoyez-vous au cours de la prochaine année?
- ?** Quels sont les signes permettant de croire que le chef de l'information de notre entreprise est celui dont elle a besoin? Quels sont les signes pouvant laisser croire que ce n'est pas le cas?
- ?** À quelle fréquence le chef de l'information se présente-t-il devant le conseil d'administration ou le comité d'audit? Quel type d'informations leur communique-t-il alors? Quels autres types d'informations pourraient leur être utiles?
- ?** Comment le conseil d'administration peut-il s'y prendre pour recenser les points forts et les vulnérabilités des ressources de la fonction TI? Dans quelle mesure est-il important pour le conseil d'administration de se familiariser avec la stratégie de relève des principaux professionnels des TI?
- ?** De quelles sources de compétences techniques les conseils d'administration et les comités d'audit ont-ils besoin dans l'analyse des enjeux en matière de TI? À cet égard, quelles doivent-être les attentes du conseil d'administration face au cabinet d'audit externe?
- ?** Comment les spécialistes internes et les spécialistes externes pourraient-ils offrir un meilleur soutien au conseil d'administration ou au comité d'audit dans le cadre de la surveillance des TI? Quels sont les obstacles à l'amélioration du soutien offert?
- ?** Notre entreprise cherche-t-elle à faire en sorte que le conseil d'administration augmente son niveau de compétences en TI? Quelles sont les activités de formation offertes aux administrateurs?