Gouvernance efficace et contrôle du conseil d'administration dans un environnement d'information mondialisé

La gouvernance de la technologie et de la cybersécurité devient de plus en plus une priorité stratégique majeure en raison de la dépendance des entreprises, des clients et des fournisseurs à l'égard des technologies orientées vers l'internet qui introduisent des risques de tierce partie et de quatrième partie. La plupart des entreprises modernes disposent de systèmes orientés vers l'internet et interagissent avec les consommateurs, les vendeurs et les partenaires au moyen d'une interface web. De nombreuses entreprises utilisent des services en nuage sous une forme ou une autre, ce qui signifie que certaines de leurs données sont transportées et stockées dans le nuage sur des serveurs dispersés dans le monde entier, faisant partie d'un environnement d'information mondialisé. Le recours à des fournisseurs de services en nuage ne fait qu'exacerber l'exposition aux risques de cybersécurité.

Les entreprises prospères sont dirigées par des cadres qui parviennent à trouver un équilibre entre l'exploitation des opportunités et la gestion des risques liés à la mise en œuvre des stratégies qu'ils ont choisies. Le conseil d'administration (CA) supervise la gestion afin de s'assurer que les gestionnaires mettent en œuvre les stratégies approuvées dans le cadre de l'appétence pour le risque établi. Le conseil d'administration a pour rôle de responsabiliser la direction générale et de s'assurer que celle-ci fournit les informations nécessaires pour aider le conseil d'administration à prendre des décisions optimales en tenant compte des risques. En ce qui concerne la technologie et la cybersécurité, le conseil d'administration participe à l'approbation des budgets et soutient la gestion indépendante des risques et l'audit interne. Le conseil d'administration doit également s'assurer que ses membres sont capables d'assurer une surveillance adéquate en examinant la stratégie, en déterminant l'appétence pour le risque et en supervisant d'autres responsabilités importantes de l'entreprise.

L'environnement mondialisé de l'information se caractérise par l'évolution des technologies et la rapidité de l'innovation. Par conséquent, pour préserver la confidentialité, l'intégrité et la disponibilité des données utilisées dans les opérations génératrices de revenus, les membres du conseil d'administration doivent comprendre comment les progrès technologiques affectent la sécurité des données et de l'information de l'entreprise et comment le risque pris par la direction affecte les actifs informationnels :

> *Le conseil d'administration étant l'élément clé de la gouvernance d'entreprise, il est évident que sa composition doit répondre aux fonctions de base qui lui sont assignées : superviser et contrôler, éviter les comportements opportunistes des dirigeants et conseiller les décideurs afin d'améliorer la gestion de l'entreprise.*[1]

Le conseil d'administration doit être composé de personnes dont les compétences fondamentales comprennent la planification stratégique, la finance d'entreprise, la gestion des risques et une bonne compréhension de la conformité légale et réglementaire. La plupart des entreprises ont des conseils d'administration dotés d'équipes spécifiquement chargées de superviser les risques liés à la technologie et à la cybersécurité. Les plus courants sont les comités d'audit, de risque et technologiques.

Un groupe de chercheurs a mis en lumière les perceptions des administrateurs et des cadres supérieurs concernant le rôle d'un conseil

ALLEN ARI DZIWA | CISA, CRISC, CCSP, CEH, CISSP

Spécialiste du risque et expert en la matière (SME) pour la Banque fédérale de réserve américaine de Cleveland. Il travaille depuis 15 ans dans le domaine du conseil en technologie et en cybersécurité. Il a précédemment siégé au comité consultatif sur le piratage éthique de l'Association pour la sécurité des systèmes d'information (ISSA), section du nord du Texas (États-Unis), et a été SME du Consortium international pour la sécurité des systèmes d'information (ISC)[2]. Il est un hacker éthique certifié et un analyste de renseignements sur les menaces. Cet article ne représente pas le point de vue de ses employeurs actuels ou précédents.

d'administration dans la supervision des risques et de la conformité, de la stratégie, de la gouvernance, du développement des cadres supérieurs et des relations avec les parties prenantes. Ils ont constaté que les administrateurs et les dirigeants estimaient que différentes combinaisons de ces rôles déterminaient l'efficacité.[2] En raison de la complexité des technologies et de la cybersécurité, une compréhension superficielle des concepts techniques n'est plus suffisante. Une compréhension plus approfondie de ces questions est nécessaire pour que le conseil d'administration puisse assurer une surveillance adéquate et veiller à ce que des mesures appropriées soient prises pour gérer les risques.

Les comités du conseil d'administration axés sur la technologie et la cybersécurité, lorsqu'ils sont correctement constitués, peuvent assurer une gouvernance efficace et un contrôle critique, permettant ainsi à la direction d'identifier et d'atténuer les cyberrisques.

Comité d'audit

Bien que le comité d'audit soit largement connu pour sa supervision de la fonction d'audit interne, de l'audit externe et de l'information financière, il supervise également les audits en matière de technologie et de cybersécurité. Idéalement, certains membres du comité d'audit devraient avoir une formation financière et au moins un membre devrait être un expert-comptable (CPA). Compte tenu de la complexité croissante des questions de cybersécurité, il est impératif que les membres des conseils d'administration aient des connaissances techniques approfondies dans le domaine de l'informatique ou des technologies de l'information. L'idéal est d'avoir au moins un membre titulaire du titre de Certified Information Systems Auditor® (CISA®) Les membres qui ont des connaissances techniques dans leur domaine, comme l'audit financier ou technique, sont habilités à remettre en question les hypothèses et les méthodologies utilisées par la direction.

Une équipe d'audit techniquement compétente peut facilement identifier des problèmes tels que ceux qui ont conduit au scandale Enron :

> *Le conseil d'administration d'Enron n'a pas protégé les actionnaires d'Enron et a contribué à l'effondrement de la septième plus grande entreprise publique des États-Unis, en permettant à Enron de s'engager dans une comptabilité à haut risque, dans des transactions inappropriées liées à des conflits d'intérêts, dans de vastes activités non divulguées n'apparaissant pas dans les livres de comptes et dans une rémunération excessive des dirigeants.*[3]

Une compréhension plus approfondie de ces questions est nécessaire pour que le conseil d'administration puisse assurer une surveillance adéquate et veiller à ce que des mesures appropriées soient prises pour gérer les risques.

Si les membres du comité d'audit du conseil d'administration sont en mesure de lire et de comprendre les rapports d'audit, ils peuvent demander des comptes à la direction générale, en particulier à la troisième ligne de défense. Alors qu'un auditeur technique peut diriger le comité d'audit dans l'examen des audits techniques, ce membre du conseil d'administration peut également être une personne qui comprend les questions commerciales, juridiques et de conformité. Les problèmes techniques ne sont pas isolés, mais s'inscrivent dans un contexte commercial, qui inclut les avantages commerciaux et la conformité réglementaire.

La pratique traditionnelle consiste à nommer des membres du conseil d'administration qui sont d'anciens ou d'actuels dirigeants sans tenir compte de leur expertise dans les domaines techniques. Cela doit changer.

Comité des risques

Les membres du conseil d'administration doivent faire preuve d'une compréhension claire de la manière dont les risques liés à la technologie et à la cybersécurité affectent les opérations. Le comité des risques est responsable des politiques de gestion des risques et de la surveillance. Il doit être en mesure de comprendre et de remettre en question les mises à jour des risques fournies par la deuxième ligne de défense (c'est-à-dire les gestionnaires). Le Responsable de la gestion des risques (CRO) doit pouvoir accéder directement au comité des risques du conseil d'administration pour signaler les activités qui représentent un risque sérieux pour l'entreprise, sans interférence de la part du Président directeur général (CEO). L'indépendance du CRO est importante pour permettre à l'entreprise d'identifier, de contrôler et d'atténuer les risques de manière efficace. Le comité des risques veille à cette indépendance.

Les membres du comité des risques doivent être dotés de compétences en gestion de projet, d'une expérience en gestion du changement, d'une compréhension raisonnable des risques juridiques et de conformité, et d'une connaissance des plans d'urgence et de la cybersécurité. Ils doivent éviter les conflits d'intérêts, maintenir et mettre à jour des chartes écrites et rendre compte à l'ensemble du conseil tous les trimestres pour discuter des questions liées à leurs domaines d'intervention. Outre les compétences techniques, les membres du comité des risques doivent être en mesure de comprendre les états financiers et les processus. Le comité des risques doit s'engager à préserver l'indépendance de la fonction de gestion des risques de l'entreprise.

Le futur conseil d'administration devra équilibrer les activités de création de valeur et gérer les risques dans le cadre de l'appétence pour le risque établi.

En ce qui concerne la conformité légale et réglementaire, les membres du conseil d'administration du comité des risques peuvent contrôler et suivre la conformité en examinant les rapports de gestion avec les paramètres appropriés. Les membres du conseil d'administration qui n'ont qu'une connaissance périphérique des exigences réglementaires peuvent approuver les rapports sans demander des comptes à la direction si les mesures indiquent que l'organisation n'est plus en conformité.

Comité technologique

Un comité technologique examine, approuve et supervise les acquisitions et les déploiements technologiques majeurs. Les membres de ce comité doivent comprendre les états financiers et être en mesure d'examiner et d'approuver les budgets technologiques. Lorsque de nouvelles acquisitions sont prévues, le comité technologique doit être en mesure de discuter avec le comité des risques des risques associés à la nouvelle technologie. Les membres du comité doivent avoir une bonne compréhension de la gestion de projet, de la gestion du changement et des avantages et inconvénients de l'acquisition de nouvelles technologies. Ils doivent demander des comptes aux cadres supérieurs qui sont responsables de la première ligne de défense.

Conclusion

L'évolution rapide des technologies et les progrès prévus en matière d'intelligence artificielle (IA), d'apprentissage automatique (ML) et d'informatique quantique créent des perturbations dans l'espace de la cybersécurité. Par conséquent, les entreprises doivent disposer de membres du conseil d'administration tournés vers l'avenir, prêts à procéder à des ajustements et à s'adapter à l'évolution de l'environnement mondial de l'information. Les membres du conseil d'administration doivent posséder des compétences dans des disciplines telles que la finance, la technologie et la gestion du personnel pour les aider à voir les problèmes au-delà de leurs responsabilités immédiates au sein du comité, afin qu'ils puissent remettre en question les hypothèses formulées par la direction générale avant qu'elle ne prenne des décisions ayant une incidence sur les risques technologiques et de cybersécurité pour l'entreprise.

Le futur conseil d'administration devra équilibrer les activités de création de valeur et gérer les risques dans le cadre de l'appétence pour le risque établi. L'époque où les membres des conseils d'administration ne savaient pas se servir d'un ordinateur, mais prenaient des décisions importantes en matière de technologie et de risque de cybersécurité est révolue. Le futur conseil d'administration devrait être composé d'experts techniques capables de faire le lien entre les questions de technologie et de cybersécurité et les fonctions de l'entreprise, y compris la conformité réglementaire. Les membres des conseils d'administration qui siègent dans les comités d'audit, de risque et technologiques doivent être à l'aise pour interpréter les indicateurs clés de performance (KPI) et les indicateurs clés de risque (KRI) et doivent être convaincus que les entreprises qu'ils gouvernent sont en mesure de mettre en œuvre les contrôles nécessaires et appropriés, d'élaborer des mesures et de rendre compte des risques liés à la technologie et à la cybersécurité.

Le futur conseil d'administration doit être composé de membres avisés, capables de discuter facilement de questions épineuses et de clarifier les attentes en matière de culture d'entreprise et de cybersécurité de leur organisation. Ils doivent être capables de s'auto-évaluer et d'accepter la responsabilité en cas d'échec de la stratégie et de la culture qu'ils établissent depuis le sommet. Si leur contribution ne permet pas d'éviter des attaques de cybersécurité majeures qui entraînent des problèmes juridiques et de réputation pour l'entreprise, ils doivent être prêts à renoncer au privilège de siéger au conseil d'administration. Les membres du conseil d'administration ne doivent pas se contenter d'entériner les propositions de la direction, mais plutôt utiliser leurs compétences et leur expertise critiques pour examiner et remettre en question les hypothèses formulées par la direction et tenir les décideurs responsables de toutes les activités de prise de risque. Le futur conseil d'administration sera très analytique, technique, avisé et diversifié.

Bibliographie

1 Martin, C. J. G.; B. Herrero; « Boards of Directors: Composition and Effects on the Performance of the Firm, » *Economic Research-Ekonomska Istraživanja*, vol. 31, iss. 1, 1er mai 2018, *https://www.tandfonline.com/doi/full/10.1080/1331677X.2018.1436454*

2 Nicholson, G.; C. Newton; « The Role of the Board of Directors: Perceptions of Managerial Elites, » *Journal of Management and Organization*, vol. 16, iss. 2, mai 2010, *https://www.cambridge.org/core/journals/journal-of-management-and-organization/article/abs/role-of-the-board-of-directors-perceptions-of-managerial-elites/96D707EB8F784ABC95EB39F5A08C0B2C#*

3 Commission des affaires gouvernementales du Sénat américain, *The Role of the Board of Directors in Enron's Collapse,* États-Unis, juillet 2002, *https://www.govinfo.gov/content/pkg/CPRT-107SPRT80393/html/CPRT-107SPRT80393.htm*