Le secteur de l'énergie se prépare aux risques et aux avantages des perturbations numériques

La pandémie oblige les entreprises à passer du mode survie au mode stratégie

Par Jeff Thomas, Julie Pépin et Narmin Vasanji

La pandémie de COVID-19 a incité les organisations à entreprendre une transformation numérique rapide et généralisée. Environ le tiers des 500 petites et moyennes entreprises canadiennes sondées par KPMG ont accéléré leur intégration des technologies depuis le début de la pandémie.

Conséquence de cette mutation à vive allure (et de l'extension du télétravail), le nombre de cyberattaques s'est grandement accru – de même que leur degré de sophistication. Les comités d'audit doivent veiller à ce que la direction soit prête à faire face à une éventuelle perturbation des activités de l'entreprise et à ce qu'elle ait mis en place des plans pour répondre au risque accru de cyberattaques découlant de la transformation numérique.

Les sociétés du secteur de l'énergie et des ressources naturelles (« ERN ») accélèrent leur adoption de l'infonuagique, de systèmes de planification des ressources organisationnelles et de solutions de gestion du rendement de l'entreprise. « Nous constatons que les outils de planification, d'établissement de budget et de prévision, ainsi que la robotisation et l'automatisation des processus, gagnent en importance », affirme Narmin Vasanji, associée, Services-conseils – Management chez KPMG au Canada.

Selon elle, la pression exercée sur les coûts dans le secteur pétrolier et gazier et les problèmes de recouvrabilité dans le secteur de l'énergie et des services publics obligent les organisations à « numériser » leurs processus de base. De plus, la fonction Finances effectue encore à la main certaines opérations répétitives qui pourraient aisément être automatisées afin de réduire les dépenses. « Certains des changements les plus importants que la COVID-19 a permis d'accélérer dans ces secteurs étaient dans un premier temps élémentaires, comme être en mesure de travailler avec des documents numériques et de gérer les activités à distance. Il s'agissait ensuite de pouvoir produire de meilleures prévisions », de dire Mme Vasanji.

C'est la difficulté de prévoir malgré l'incertitude entourant la pandémie qui a stimulé l'innovation en matière de prévisions intelligentes. On conjugue de multiples sources de données et on y ajoute de l'apprentissage automatique pour examiner les tendances et les corrélations passées afin d'établir des prévisions sur certaines variables telles que les flux de trésorerie et la demande de produits. Le conseil d'administration dispose ainsi d'une bien meilleure vision sur les options offertes pour assurer la stabilité financière à long terme de l'entreprise.

Le capital est roi

« L'un des principaux facteurs qui différencient le secteur de l'énergie des autres secteurs est le degré auquel s'applique l'idée que le capital est roi. Les organisations doivent être en mesure de comprendre la façon dont elles gèrent leurs dépenses en capital et s'en servent pour stimuler l'innovation », affirme Mme Vasanji. Par surcroît, la complexité actuelle du contexte réglementaire et politique entourant l'environnement, le développement durable et les énergies renouvelables rend d'autant plus difficile la prise de décision sur la façon de gérer et de dépenser ces capitaux.

Vu l'importance primordiale du capital dans le secteur de l'énergie, les conseils d'administration doivent s'enquérir davantage sur les programmes de transformation numérique majeure, notamment sur leurs avantages quantifiables, le rendement du capital investi et le délai de récupération attendu d'un investissement dans les technologies comme l'infonuagique. Ils doivent également se tenir au courant de l'évolution des projets et, dans le cas des projets de grande envergure ou à long terme, ils pourraient exiger de la direction qu'elle produise des bilans ou réalise des examens indépendants d'assurance de la qualité.

« Du point de vue des conseils d'administration, il s'agit de poser à la direction les bonnes questions, notamment afin de savoir si l'entreprise utilise les perturbations et les technologies comme avantages stratégiques, si elle en fait assez, et comment elle se situe par rapport à la concurrence. Il s'agit pour eux d'examiner le modèle d'affaires et de se demander s'il y a autre chose que l'entreprise doit faire pour accroître sa part de marché ou pour repousser les limites », ajoute Mme Vasanji.

Les avantages de la transformation numérique

L'un des avantages de l'implémentation de nouvelles technologies est que les organisations peuvent mieux cerner la source unique de vérité de leurs données. Elle représente l'occasion, pour ces organisations, de nettoyer leurs données et de mettre en place un mécanisme de gouvernance pour gérer les données, déterminer quel est le système primaire d'enregistrement et s'assurer que la création de données est plus rigoureuse et mieux encadrée. Cet assainissement des données permet aux conseils d'administration de se faire une idée plus claire et plus fiable de la situation de l'entreprise et les aide sur le plan de la gouvernance et de la prise de décision – ce qui profite tant aux conseils d'administration qu'aux comités d'audit.

Un autre avantage est l'éventuelle mise en place de contrôles automatisés de prévention. D'ordinaire, les entreprises dépendent de rapports pour être informées après coup d'un problème ou d'une défaillance. Cependant, en employant les bonnes technologies, elles peuvent mettre en place des processus qui détectent rapidement les anomalies pour ainsi prévenir des problèmes tels que des transactions non autorisées avant qu'il ne soit trop tard. Une entreprise pourrait, par exemple, instaurer un mécanisme grâce auquel un bon de commande ne peut être traité que s'il a été dûment approuvé. En prime, il est plus facile d'auditer ce type de système : l'auditeur n'a qu'à en tester le fonctionnement plutôt qu'à vérifier manuellement chaque transaction.

Les comités d'audit devraient réfléchir à la façon dont les nouvelles technologies modifieront l'environnement de contrôle et aux risques qui en découlent. De même, une fois introduite l'automatisation robotisée des processus, ils devront comprendre comment la direction adapte ses contrôles internes. Ils doivent également se renseigner sur les risques liés à l'infonuagique et demander si l'entreprise sera plus vulnérable aux cyberrisques qu'auparavant.

« En raison du déploiement technologique récent et rapide lié au télétravail et à la transformation numérique, il est possible que certaines technologies n'aient pas été adéquatement testées en ce qui a trait aux contrôles », affirme Julie Pépin, associée, Audit interne, risques et conformité chez KPMG au Canada.

De l'avis de M^me^ Pépin, il faut également tenir compte de la part du capital humain. « Nous dépendons largement du personnel de soutien informatique, mais il est occupé à aider les employés qui travaillent à domicile. Par conséquent, il dispose de moins de temps pour exécuter les contrôles informatiques nécessaires à la présentation de l'information financière. Les comités d'audit devraient demander à la direction comment cette réalité est prise en compte dans l'environnement de contrôle », dit-elle.

Les cyberattaques et la technologie opérationnelle

Même avant la pandémie de COVID-19, les cyberattaques étaient en hausse, mais depuis la généralisation du télétravail, leur nombre a connu une hausse spectaculaire. « Les entreprises du secteur ERN ont tendance à disposer d'une imposante technologie opérationnelle, et une grande partie de leur infrastructure est gérée par un centre d'exploitation centralisé. Il arrive souvent que cette technologie n'ait pas été soumise aux mêmes protocoles de sécurité rigoureux que pour les technologies de l'information », affirme Jeff Thomas, associé, Services-conseils chez KPMG au Canada.

Jusqu'à présent, les réseaux de technologie opérationnelle et les réseaux d'entreprise ont toujours été tenus séparés, raison pour laquelle les premiers ont été la cible de peu d'attaques. Toutefois, la popularité grandissante du télétravail tend à abolir cette séparation – et les conséquences peuvent s'avérer graves.

« Si votre réseau d'entreprise tombe en panne pendant une semaine, il est fort probable que vous vous en tirerez. Mais si le secteur amont s'arrête pendant une semaine ou que la province entière est privée d'électricité, vous vous retrouvez aux prises avec d'énormes problèmes », avance M. Thomas. Du point de vue de la cybersécurité, l'un des aspects les plus importants du secteur de l'énergie est le potentiel de préjudice aux humains. En cas de défaillance d'un des systèmes de technologie opérationnelle, il pourrait en résulter des dommages qui nuisent à la communauté environnante ou causent des blessures.

Il n'est pas rare que des nations soient responsables d'attaques contre la technologie opérationnelle, et certains des principaux acteurs étatiques ont une bonne idée de l'infrastructure qui existe en Amérique du Nord, y compris les pipelines et les raffineries. Des terroristes ou des criminels aussi peuvent lancer ce type d'attaque, mais « il est presque insensé désormais de catégoriser les auteurs de menaces en fonction de leur intention. Les organisations criminelles se sont spécialisées au point où il est préférable pour des terroristes – et parfois même pour des gouvernements – de les embaucher pour faire le travail à leur place », dit M. Thomas.

Un autre type d'auteur de menace peut se révéler plus problématique encore : l'initié ou l'associé. Comme ils connaissent déjà le réseau, ils n'ont pas à utiliser les mêmes techniques qu'un pirate agissant de l'extérieur. De plus, ils savent quelle est leur cible et y ont probablement déjà accès. Étant donné que le soutien informatique représente un centre de coûts pour les entreprises du secteur de l'énergie, elles n'utilisent peut-être pas les technologies les plus sophistiquées ou récentes. Elles sont habituellement dotées de réseaux à plat, c'est-à-dire où tous les éléments sont connectés. Résultat : si un auteur de menace s'infiltre dans le réseau d'entreprise, il a accès à tout.

Les environnements de technologie opérationnelle qui contrôlent des tuyaux ou des processus fonctionnent souvent sur de vieux systèmes d'exploitation ne pouvant pas être mis à jour parce qu'ils ne sont pas compatibles avec les outils récents. Il faut séparer ces environnements (ou les surveiller d'encore plus près) de manière à réduire le risque qu'ils posent. Les entreprises doivent d'abord déterminer quels sont leurs principaux points à risque afin de mettre en place de meilleurs contrôles.

Comment les comités d'audit peuvent aborder la résilience

« Les comités d'audit doivent bien comprendre leur mandat lorsqu'ils se penchent sur la cyberrésilience. En effet, le conseil d'administration peut compter plusieurs comités – et celui d'audit n'a peut-être pas la responsabilité de veiller aux cyberrisques », précise M. Thomas.

« Les comités d'audit ont beaucoup de pain sur la planche, constate M^me^ Pépin. En fin de compte, il est possible qu'il leur incombe de surveiller un nombre considérable de risques allant au-delà de la seule information financière. Ils doivent être proactifs pour s'assurer d'avoir en main l'information dont ils ont besoin. Ils doivent aussi se demander s'ils ont l'expertise et le temps nécessaires pour surveiller ces autres domaines. »

Dans la mesure où les cyberrisques font partie de leurs responsabilités, les comités d'audit doivent savoir quels sont les risques auxquels leur entreprise est exposée, selon M. Thomas. La direction doit déterminer l'importance de chacun des risques et leur attribuer une valeur – valeur que les comités d'audit doivent connaître, exprimée tant en dollars qu'en termes d'incidence sur la gestion du risque d'entreprise. Finalement, les deux instances doivent s'entendre sur le degré de risque que l'entreprise est prête à tolérer.

Les comités d'audit devraient demander à la direction quelles sont les mesures mises en place pour gérer chaque risque et qui a confirmé qu'il s'agit ou non d'une méthode efficace d'atténuation des risques. À ce chapitre, il est préférable d'obtenir l'opinion d'un tiers qui pourra confirmer que les contrôles sont aussi efficaces que la direction l'estime. Pour ce faire, les comités d'audit peuvent faire appel à des cabinets tiers pour réaliser un test d'intrusion ou produire un rapport sur les contrôles d'une société de services (SOC), qui est une opinion d'audit sur l'efficacité des contrôles relatifs à la sécurité de l'information.

Qui plus est, les comités d'audit doivent se pencher sur ce qui pourrait potentiellement aller de travers. Prenons par exemple une société d'énergie dont le système de production d'électricité se fait pirater et provoque un événement de surtension dans le générateur qui endommage celui-ci. Quelle est la gravité d'un tel incident? Quelles sont les répercussions sur l'organisation? Y a-t-il suffisamment d'actifs de production pour couvrir cette perte?

De même, s'il s'agit d'un expéditeur qui perd brusquement sa capacité d'exploiter un pipeline, quelle sera l'incidence exprimée en dollars? Quels sont les critères d'incidence de la gestion du risque d'entreprise? S'agit-il de la santé et de la sécurité, des relations avec les fournisseurs ou de la valeur monétaire? Une fois cernées les répercussions de ce qui pourrait aller de travers, il faut déterminer précisément quelles sont les mesures prises à leur égard et qui a confirmé qu'il s'agit ou non d'une méthode efficace d'atténuation des risques.

« Il est surprenant de voir à quel point certaines entreprises demeurent peu préparées lorsqu'elles font l'objet d'une violation, et ce, même si elles ont embauché un cabinet pour les aider à réagir aux incidents. Les comités d'audit doivent amorcer la conversation avec la direction pour élaborer une position justifiable, établir ce qui pourrait aller de travers en cas de violation et s'entendre sur la réaction de l'organisation le cas échéant », affirme M. Thomas.

Les deux instances devraient convenir à l'avance des personnes qui seront tenues au courant, des incidents de sécurité devant être portés à l'attention du comité d'audit, du moment où il convient d'aviser ce dernier, de la personne chargée de le faire, de même que du montant maximal à dépenser pour remédier à une violation. (Dans le cas d'un rançongiciel, il faut en outre décider si l'entreprise paiera la rançon.)

De nos jours, le secteur ERN change rapidement. Même si cette situation exige que les comités d'audit se montrent vigilants et s'efforcent de comprendre et de surveiller ces changements, elle représente aussi l'occasion d'améliorer leurs processus et leurs données ainsi que de protéger leurs systèmes et leur infrastructure contre les cyberattaques.

Communiquez avec nous

Jeff Thomas
Associé,
Services-conseils,
KPMG au Canada
(403) 691-8012
jwthomas@kpmg.ca
Se connecter sur LinkedIn

Julie Pépin
Associée, Audit interne,
risques et conformité,
KPMG au Canada
(514) 840-8092
jpepin@kpmg.ca
Se connecter sur LinkedIn

Narmin Vasanji
Associée, Services-conseils –
Management,
KPMG au Canada
(403) 691-8125
nvasanji@kpmg.ca
Se connecter sur LinkedIn

Réalisons-le. home.kpmg/ca/fr/audit