Fraude, cybersécurité et conformité

Une triple menace pour les organisations canadiennes

Mars 2022

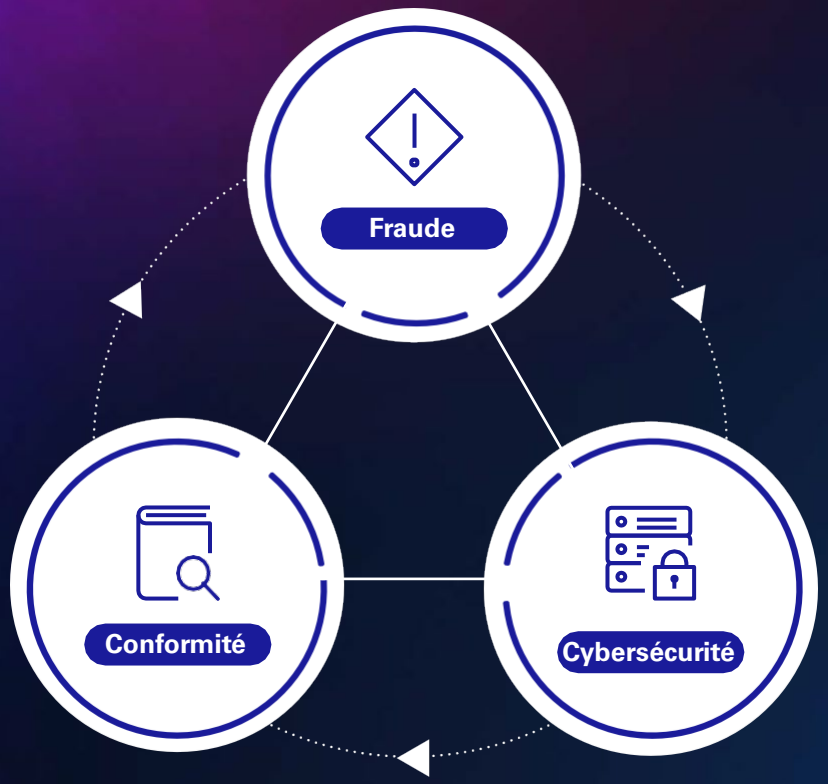
home.kpmg.ca/fr

Avant-propos

Les organisations canadiennes font face à une « boucle de menaces » composée de la fraude, des risques liés à la conformité et d'un éventail grandissant de menaces à la cybersécurité (ou cybermenaces). Pour se défendre contre cette boucle, il leur faudra non pas traiter isolément les risques qu'elle pose, mais les considérer en interrelation et agir sur l'ensemble qu'elle forme.

Un sondage de KPMG[1] mené auprès de plus de 600 dirigeants nord et sud-américains de divers secteurs confirme la teneur des témoignages informels à propos des effets de la pandémie sur ces trois menaces interreliées. C'est à la lumière des résultats de ce sondage que nous donnons dans le présent rapport notre point de vue sur leur incidence au Canada.

Les entreprises canadiennes parviennent-elles à parer à cette triple menace? Dans l'ensemble, nous constatons que bon nombre d'entre elles ne disposent que de moyens de défense limités, et que le passage au télétravail ou au travail hybride réduit l'efficacité des contrôles mis en place. Pour neutraliser cette boucle de menaces, une nouvelle approche s'impose.



Points saillants

Les fraudes, les problèmes de conformité et les cyberintrusions sont la norme (et coûteux)

La majorité des entreprises d'Amérique du Nord ont déclaré avoir subi des pertes en raison de fraudes, d'infractions à la réglementation ou de cyberattaques. Les grandes entreprises sont plus susceptibles que les petites et moyennes de subir des pertes découlant une fraude interne (commise par un employé, un gestionnaire, un cadre dirigeant ou un propriétaire) ou externe (commise par un tiers : client, fournisseur, etc.).

Les entreprises s'attendent à une intensification des fraudes, des problèmes de conformité et des cyberattaques au cours de l'année à venir.

Les deux tiers des répondants prévoient une augmentation des fraudes internes comme externes pendant cette période; une proportion encore plus élevée (77 %) s'attend même à une croissance des cyberrisques. Presque tous les répondants s'attendent à ce que le nombre d'exigences liées à la réglementation ou à la conformité augmentent au cours des cinq prochaines années en ce qui a trait à la confidentialité des données, aux relations de travail et à l'environnement.

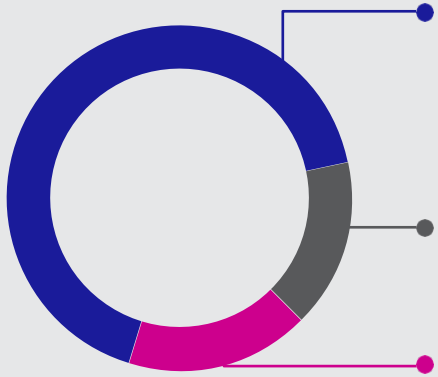
Un nombre insuffisant d'entreprises disposent des contrôles nécessaires de lutte contre la fraude, de conformité et de cybersécurité.

En examinant plus particulièrement la tenue de l'entreprise des répondants par rapport à la série de mesures prises en matière de cybersécurité, de lutte contre la fraude et de conformité, KPMG a constaté que seule une petite proportion d'entre eux affirment que des contrôles rigoureux sont mis en place à l'égard d'au moins la moitié des mesures.

Nous avons constaté que de nombreuses grandes organisations canadiennes ont l'intention d'améliorer leur cyberrésilience, leur détection des fraudes et leur conformité, mais ne ressentent pas l'urgence d'agir. Une situation malheureuse, puisqu'elles ne prennent le plus souvent conscience de cette boucle de menaces qu'à la suite d'une cyberattaque, un incident de fraude ou une infraction à la réglementation. C'est toutefois en étant proactif que l'on peut réduire les risques et atténuer les effets des incidents, qui surviendront tôt ou tard.

Fraude

À votre connaissance, votre entreprise nord-américaine a-t-elle été victime de l'un ou l'autre des types de fraudes suivants au cours des 12 derniers mois?



66,9 %

Fraude externe (fraude par carte de crédit, vol d'identité par des personnes à l'externe)

15,8 %

Aucune fraude connue

17,3 %

Fraude interne (fraude liée à l'approvisionnement, détournement de fonds par des personnes à l'interne)

Si la fraude externe fait couler beaucoup d'encre, la fraude interne est tout aussi préoccupante. Il y a aussi un type de fraude qui relève de la « collusion » entre agents internes et externes; par exemple, un acteur de menace soudoyant un employé mécontent afin d'obtenir un accès à des données sensibles. Une proportion considérable (31 %) des répondants affirment que leur entreprise a été victime d'une fraude commise par un employé au cours de la dernière année.

Les deux principaux types de fraudes internes dont les entreprises nord-américaines ont été victimes au cours des 12 derniers mois sont la demande de remboursement de fausses dépenses ou autre détournement des fonds de l'entreprise **(47,8 %)** et la fraude liée à l'approvisionnement **(45,7 %)**.

Compte tenu de la généralisation du télétravail, les contrôles mis en place avant la pandémie ne suffisent plus. Lorsqu'elles sont brusquement passées au télétravail en début de pandémie, de nombreuses entreprises se sont précipitées pour adopter des processus et des technologies sans prendre les précautions appropriées – et ne les ont peut-être même pas revus depuis. Ce basculement a exposé les organisations à de nouveaux risques. Par exemple, si un télétravailleur extrait des renseignements personnels au moyen de son adresse de courriel personnelle, le serveur de l'entreprise ne sera pas en mesure de le détecter et de le signaler.

En outre, il est plus difficile à la direction de « donner le ton » lorsque les employés travaillent à domicile. L'entreprise doit par surcroît mettre en place les bons contrôles; pour ce faire, elle doit procéder à une évaluation des risques de fraude et cartographier ses principaux risques. Si ces démarches datent d'avant la pandémie, l'entreprise devrait les faire à nouveau, puisque les risques ont changé. Enfin, il est peu probable que la situation se résorbe en raison de la prolifération du modèle de travail hybride.

L'une des façons de lutter contre la fraude consiste à recourir à l'analyse de données dans le cadre de la juricomptabilité. Ainsi, il est possible de créer des règles et de générer des rapports d'analyse des écarts afin de détecter des éléments suspects, ce qui permet habituellement de réduire le coût de la fraude, mais aussi le temps nécessaire à la déceler.

« L'entreprise doit avoir mis en place des processus rigoureux en ce qui a trait à la connaissance du client, et tous les tiers doivent faire l'objet d'un suivi afin de réduire au minimum l'exposition au risque, car divers tiers – vendeurs, fournisseurs, clients, partenaires ou employés – peuvent être à l'origine de fraudes. »

Myriam Duguay
associée, Juricomptabilité,
et leader nationale, Enquête et gestion des risques de fraude,
KPMG au Canada

Cybersécurité

Quelles répercussions d'une cyberattaque votre entreprise nord-américaine a-t-elle subies au cours des 12 derniers mois?

61,3 % Économiques (perte de fonds, perte de clients, dommagesphysiques)

40,8 % Juridiques ou réglementaires (examen ou enquête par des autorités de réglementation)

21,0 % Réputationnelles (couverture négative dans les médias)

10,5 % Aucune répercussion

Si la transformation numérique constitue déjà l'une des principales sources de cyberintrusions et de cyberattaques, la pandémie a accentué le problème. L'an dernier, des cyberattaques à grande échelle ont fait les manchettes et, dans certains cas, ont forcé des États à prendre des mesures contre des acteurs malveillants procédant par rançongiciel. Par voie de conséquence, ces groupes se scindent en groupuscules et ciblent les petites et moyennes entreprises ou des secteurs d'activité inusités afin de passer inaperçus.

La moitié des répondants nord-américains s'attendent à ce que les risques liés à la cybersécurité augmentent légèrement au cours des 12 prochains mois, tandis que **34,6 %** d'entre eux prévoient qu'ils augmentent considérablement. **Aucun des répondants** ne compte sur une baisse importante du niveau de risque.

Les entreprises sondées aux fins du rapport ont noté une augmentation de la fréquence des attaques, dont les hameçonnages (44 %), les escroqueries (33 %), les maliciels (22 %) et les rançongiciels (20 %). Les agents malveillants font également montre d'une agressivité accrue quant à l'exploitation des vulnérabilités du jour zéro. Les perturbations de la chaîne d'approvisionnement entraînent aussi l'augmentation des risques liés aux tierces et quatrièmes parties pour la cybersécurité, selon les conclusions de notre rapport *De la sensibilisation à l'action : priorité aux risques liés aux tiers*. En effet, si des fournisseurs d'une entreprise subissent une violation, il est possible que ses données aient également été violées ou qu'elle ne puisse plus offrir ses produits et services.

En parallèle, le sondage révèle que seule une faible proportion des répondants nord-américains étaient en mesure de détecter une cyberattaque en temps réel, voire en moins de 24 heures, et de la contenir. Il faut en moyenne deux semaines pour détecter une cyberattaque et deux autres semaines et demie pour la contenir. Malgré tout, ces répondants ne se préoccupent pas suffisamment de la situation, puisque 87,9 % d'entre eux se disent plutôt ou entièrement satisfaits du temps qu'il faut à leur entreprise pour déceler une attaque informatique.

Toute organisation doit mettre en place des processus et des contrôles préventifs rigoureux ainsi qu'évaluer périodiquement ses vulnérabilités pour réduire la probabilité de cyberincidents. Qui plus est, elle doit se doter d'une police de cyberassurance et dresser des plans de gestion de crise et de reprise après sinistre afin de réduire l'incidence d'une éventuelle attaque.

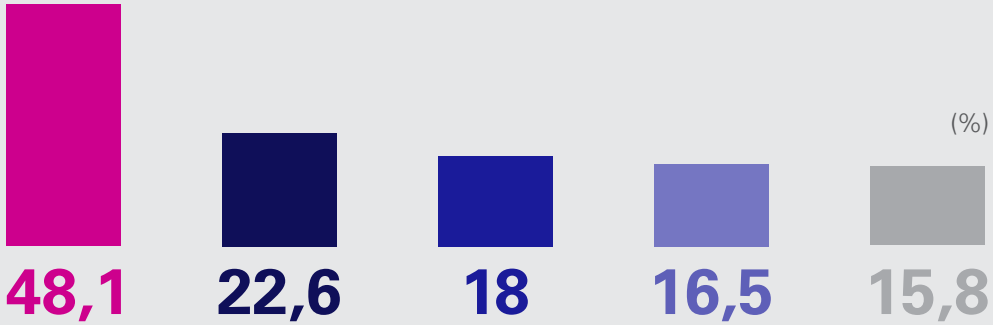
« Une approche tenant compte de l'interrelation entre la fraude, la cybersécurité et les problèmes de conformité permet de réduire non seulement la probabilité qu'un événement se produise, mais aussi l'incidence qu'il pourrait avoir sur l'entreprise. »

Alexander Rau
associé,
Cybersécurité,
KPMG au Canada

Conformité

Quels éléments parmi les suivants ont-ils été influencés négativement par l'augmentation du nombre de télétravailleurs au cours des 12 derniers mois?

- Respect des mesures de sécurité informatique par les employés
- Efficacité des programmes de formation sur la conformité, la lutte contre la corruption ou la prévention de la fraude
- Nombre d'employés participant à des programmes de formation sur la conformité, la lutte contre la corruption ou la prévention de la fraude
- Capacité d'évaluer la conformité aux contrôles touchant les finances, la lutte contre le blanchiment d'argent et la lutte contre la corruption
- Conformité des employés aux contrôles touchant les finances, la lutte contre le blanchiment d'argent et la lutte contre la corruption



La transformation numérique génère des risques supplémentaires pour les entreprises. En modifiant leurs systèmes et leurs processus sans toujours être conscientes de l'interdépendance entre certains jeux de données ou systèmes, elles s'exposent à des risques liés à la conformité. La pandémie a rendu cette situation encore plus difficile, étant donné la complexité de gérer la conformité lorsque leur main-d'œuvre travaille complètement ou partiellement à domicile.

55 % des répondants reconnaissent que leur entreprise a versé une amende ou subi des pertes financières en raison d'infractions aux règles de conformité au cours de la dernière année. Or, comme de nombreux cas ne sont pas rapportés, ces chiffres seraient vraisemblablement plus élevés encore.

Les risques de non-conformité vont toutefois au-delà des seules amendes : la réputation de l'entreprise aussi est en jeu. Ce sont même souvent les considérations relatives à la réputation – plus que les amendes ou les mesures disciplinaires – qui amènent les dirigeants à s'attarder aux enjeux de conformité. Beaucoup d'organisations canadiennes connaissent des ratés, car elles ne définissent pas de manière proactive l'ensemble de leurs exigences juridiques, réglementaires, contractuelles, internes et autres en matière de conformité, et se retrouvent à corriger le tir une fois qu'il est trop tard.

La mise en œuvre d'un solide programme de conformité démontre qu'une entreprise a pris les soins appropriés pour protéger ses actifs de données et (ou) ceux de ses clients. Un tel programme s'avère d'autant plus important vu les changements à venir en matière de réglementation et l'élargissement de la fonction conformité des entreprises, surtout en raison de l'attention accrue portée aux facteurs environnementaux, sociaux et de gouvernance (ESG).

Pour toute organisation, faire l'inventaire de ses exigences de conformité et évaluer ses risques liés à la conformité aide à cerner les risques auxquels elle est exposée et le niveau de cette exposition. Si elle entend investir du temps, des efforts et des fonds dans la mise en place de meilleurs contrôles, mieux vaut savoir précisément où elle doit investir ces précieuses ressources.

« Une organisation pourrait s'exposer à des risques supplémentaires si elle ne considère pas les contrôles internes et la conformité comme des éléments clés de tout projet de transformation d'envergure. »

Pedro Medeiros
associé,
Gouvernance, risques et conformité,
KPMG au Canada

Votre organisation est-elle parée à la triple menace?

La situation a empiré en raison de la pandémie. Près de neuf répondants sur dix affirment que le télétravail a eu une incidence négative sur l'efficacité des mesures de cybersécurité, de prévention de la fraude et d'atténuation des risques liés à la conformité de leur entreprise.

Peu de répondants affirment que leur entreprise respecte les meilleures pratiques internationales en matière de conformité aux lois de lutte contre la corruption (18 %), de conformité à la réglementation environnementale (21 %), de conformité aux lois de lutte contre le blanchiment d'argent (22 %), de contrôles de prévention de la fraude (23 %) et de contrôles de protection de la confidentialité des données (27 %).

En dépit de cette réalité, la plupart des répondants s'attendent à une intensification des fraudes, des problèmes de conformité et des cyberattaques au cours de l'année à venir. Si la plupart des entreprises au Canada se sont dotées de quelques mécanismes de défense, rares sont celles qui adoptent une approche exhaustive, hormis certaines institutions financières de niveau 1.

Pour l'avenir, KPMG au Canada recommande aux organisations de prendre les quatre mesures suivantes pour se défendre contre la triple menace :

1

Élaborer une stratégie de défense où les efforts sur les plans de la conformité, de la fraude et de la cybersécurité sont interreliés et synergiques.

2

Coordonner les fonctions relatives à la cybersécurité, à la lutte contre la fraude et à la conformité ou les intégrer en un seul poste dans le but de gérer les risques correspondants de manière unifiée.

3

Évaluer les risques dans ces trois domaines au moins une fois tous les deux ans, voire plus fréquemment en cas de changement majeur dans l'organisation (acquisition, fusion, etc.) ou d'événement majeur (pandémie mondiale, etc.).

4

Veiller à ce que l'évaluation des risques tienne compte de l'exposition à toute une gamme de risques, notamment liés à la technologie, au personnel, aux processus et aux comportements.

KPMG peut vous être utile

KPMG au Canada peut évaluer la boucle de menaces de manière exhaustive – par la combinaison d'une évaluation de la maturité en matière de cybersécurité, d'une évaluation des risques de fraude et d'une évaluation du programme de conformité – et ainsi vous aider à comprendre ses répercussions sur votre organisation. Le cabinet offre également un large éventail de services ayant trait à la fraude, à la cybersécurité et à la conformité, dont les suivants :

Fraude

- Évaluation des risques de fraude et programmes de prévention de la fraude
- Enquêtes juricomptables
- Analyse juricomptable de données
- Services juricomptables en gestion de la conformité réglementaire
- Enquêtes technologiques
- Services en matière de crimes financiers

Cybersécurité

- Évaluation de la maturité en matière de cybersécurité, formation du personnel, outils de vérification des utilisateurs, veille des menaces et surveillance en temps réel
- Externalisation de la fonction cybersécurité, en veillant à choisir les meilleures options de contrôles informatiques en fonction de la couverture et du rendement du capital investi
- Élaboration et mise à l'essai du plan d'intervention en cas de cyberincident
- Acquisition et maintien d'une police de cyberassurance

Conformité

- Mise en œuvre et amélioration du programme de conformité à la réglementation (répertoire de règlements, évaluation des risques, examens, mesures correctives et rapports)
- Audits de conformité, examens de programmes de conformité et évaluations de la maturité
- Certification de la transformation (y compris le soutien aux contrôles internes et à la conformité)

Cadre de la recherche

Le présent rapport s'appuie sur un sondage mené auprès de 642 cadres dirigeants répartis presque également dans les sept secteurs d'activité suivants :

- Fabrication industrielle
- Commerce de détail et biens de consommation
- Énergie et ressources naturelles
- Services financiers
- Assurance
- Sciences de la vie et produits pharmaceutiques
- Télécommunications, médias, divertissement et technologie

Répartition géographique des répondants

42 %
Amérique du Nord

58 %
Amérique latine

L'échantillon se compose principalement de cadres supérieurs : plus de la moitié des répondants sont des administrateurs, des cadres dirigeants ou des chefs de service. Le présent rapport se fie principalement aux réponses obtenues auprès de la portion nord-américaine de l'échantillon.

Communiquez avec nous

Enzo Carlucci
Associé, et leader national,
Services de juricomptabilité
KPMG in Canada
416-777-3383
ecarlucci@kpmg.ca

Hartaj Nijjar
Associé, et leader national,
Cybersécurité
KPMG in Canada
416-228-7007
hnijjar@kpmg.ca

Angela Moch
Associée, et leader nationale,
Gouvernance, risques et
conformité
KPMG in Canada
416-777-8093
amoch@kpmg.ca

Myriam Duguay
Associée, Juricomptabilité,
et leader nationale,
Enquête et gestion
des risques de fraude
KPMG au Canada
514-840-2161
myriamduguay@kpmg.ca

Alexander Rau
Associé,
Cybersécurité
KPMG au Canada
416-777-3450
alexanderrau@kpmg.ca

Pedro Medeiros
Associé,
Gouvernance,
risques et conformité
KPMG au Canada
416-476-2263
pedromedeiros@kpmg.ca

home.kpmg.ca/fr