Quatre-vingt-cinq pour cent des entreprises ne sont pas préparées en cas de cyberattaque, disent les dirigeants financiers

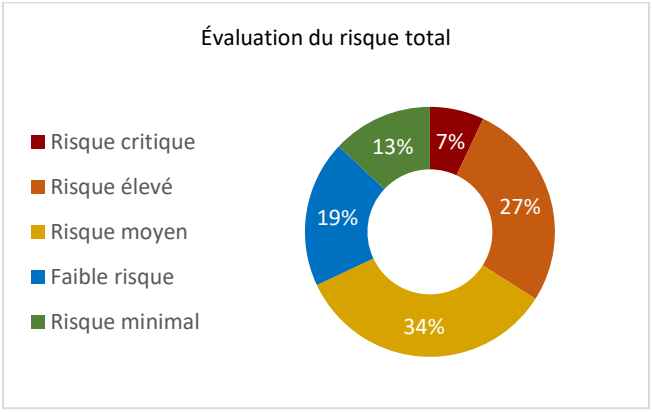
Une enquête menée par FEI Canada révèle que 98 % des répondants s'inquiètent d'une intrusion possible, mais que seuls 15 % d'entre eux s'y sont préparés.

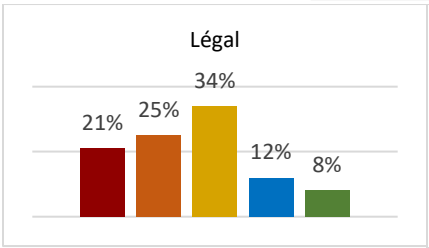
TORONTO, le 25 novembre 2019 : Une enquête menée par les Dirigeants financiers internationaux du Canada (FEI Canada) auprès de dirigeants financiers révèle que les entreprises ne sont pas préparées à répondre à une cyberattaque qui pourrait affecter leurs opérations de manière significative. Bien que 98 % des participants à l'enquête aient exprimé leur inquiétude concernant l'éventualité d'une cyberattaque, seuls 15 % d'entre eux s'y sont préparés en mettant en place suffisamment de protections dans trois domaines essentiels :

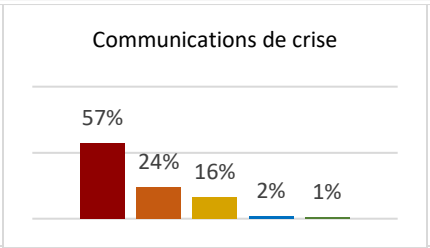
1. Obligations juridiques
2. Communications en cas de crise
3. Cyberassurance

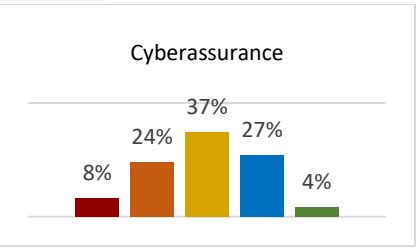
Les participants ayant répondu à des questions visant ces trois domaines, ont ensuite reçu les résultats pour chacune des sections, ainsi qu'une indication du niveau de risque général pour leur entreprise.

« Les résultats indiquent que 34 % des entreprises ont été victime d'une intrusion au cours des cinq dernières années », explique Catherine Fels-Smith, présidente de FEI Canada. « Les entreprises et leurs dirigeants doivent adopter une position proactive, sans quoi elles risquent de subir des dommages importants qui vont au-delà de la confidentialité des données. »









Principales constatations

Les résultats ont révélé un manque de cohérence significatif entre ce que les dirigeants financiers perçoivent et la réalité de la cyberpréparation actuelle de leur entreprise.

- **Les entreprises n'évaluent pas leurs risques en matière de cybersécurité.** Les résultats ont montré que 55 % des entreprises n'ont pas évalué leurs risques en matière de cybersécurité au cours des 12 derniers mois, tandis que 59 % d'entre elles ne testent pas leur plan tous les ans.
- **Les entreprises ne font pas de préparatifs pluridisciplinaires.** 72 % des entreprises sondées n'ont pas d'équipe d'intervention pluridisciplinaire en place en cas de cyberattaque.
- **Les équipes d'intervention ne sont pas suffisamment formées.** Un pourcentage inquiétant (75 %) des entreprises ne font pas d'exercices d'intervention en cas d'intrusion ou ne donnent pas de formation à leur équipe d'intervention.
- **Les petites entreprises sont les moins susceptibles d'être préparées.** Les entreprises qui comptent moins de 99 employés ont obtenu les résultats les plus faibles concernant leur état de préparation, avec seulement 4 % d'entre elles se disant préparées dans les domaines des obligations juridiques, des communications et des assurances.

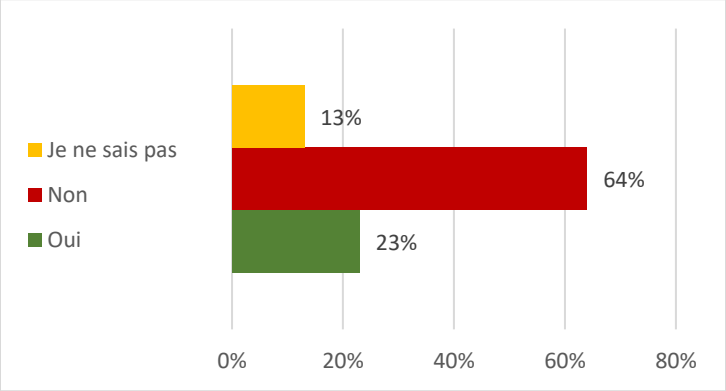
Dans les trois domaines essentiels de préparation à une intervention, les résultats de l'enquête montrent que :

- 51 % des entreprises ne disposent pas d'un conseiller juridique externe pour les soutenir en cas d'intrusion.
- 45 % des entreprises n'ont pas de plan de communication pour situation de crise en place, et seulement 20 % en préparent un actuellement.
- 35 % des entreprises n'ont pas de cyberassurance, et 10 % ne savent pas si elles en ont une.

Obligations juridiques

En cas de cyberattaque, 51 % des participants n'ont pas de conseiller juridique externe pour les soutenir. Par ailleurs, 64 % des entreprises ne procèdent pas à une vérification préalable de leurs fournisseurs ou distributeurs tandis que seuls 23 % des entreprises disent protéger leur hygiène informatique contre des tiers.

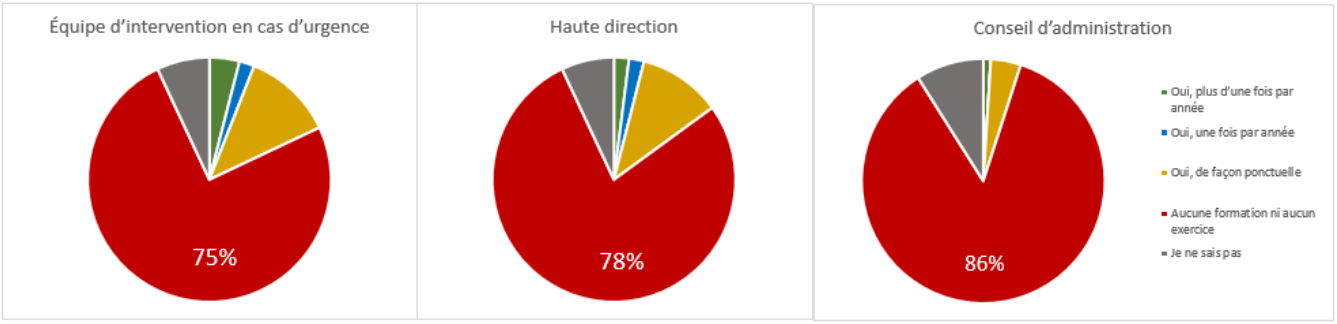
Votre organisme fait-il une vérification diligente auprès de ses fournisseurs afin de s'assurer qu'ils ont des pratiques exemplaires en matière de cybersécurité?



« Les distributeurs et fournisseurs représentent un point d'accès fréquent pour les pirates informatiques, il est donc très important de procéder à une vérification préalable », explique Imran Ahmad, associé dans le cabinet d'avocats Blake, Cassels & Graydon LLP. « En cas de cyberattaque, il est essentiel que les entreprises comprennent les lois et les réglementations qui s'appliquent à elles, que ce soit au Canada ou ailleurs dans le monde. »

Communications en cas de crise

Tandis que 62 % des entreprises disent disposer des ressources internes pour gérer les communications en cas d'intrusion, seuls 27 % d'entre elles ont un plan de communications en cas de crise en place, et 75 % n'ont qu'un plan de communications général ou aucun plan.

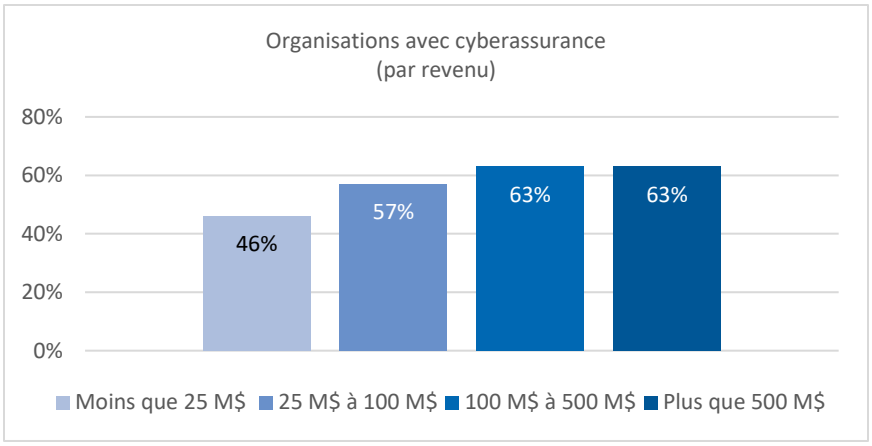


	Oui, plus d'une fois par année	Oui, une fois par année	Oui, de façon ponctuelle	Aucune formation ni aucun exercice	Je ne sais pas
Équipe d'intervention en cas d'urgence	4%	2%	12%	75%	7%
Haute direction	2%	2%	11%	78%	7%
Conseil d'administration	1%	0%	4%	86%	9%

« Si elles devaient réagir à une intrusion en moins de 30 à 60 minutes, seuls 26 % des entreprises se disent capables de gérer cette situation », remarque Anne Lachance, associée directrice chez Kaiser Lachance Communications. « Ainsi, bien que les participants au sondage puissent estimer que leur propre équipe de communications sera en mesure de gérer la crise en cas d'intrusion, la triste réalité est que cela n'est pas le cas. »

Assurances

Tandis que 82 % des participants indiquent avoir des pare-feu et des logiciels antivirus automatiquement mis à jour, 25 % ont remarqué qu'ils n'avaient pas de politique établie pour une mise à jour ou un correctif critique des logiciels, et 41 % des participants sont sans le savoir. De plus, seuls 55 % des participants détenant une cyberassurance ont indiqué avoir identifié un conseiller juridique externe en mesure de leur apporter une assistance en cas de cyberincident.



« Une police de cyberassurance autonome charge un conseiller juridique externe d'agir en tant qu'accompagnateur en matière d'intrusion au nom du client; conséquemment, 100 % de ceux qui ont souscrit une cyberassurance auraient dû répondre par l'affirmative », note Greg Markell, président chez Ridge Canada. « La proportion des entreprises qui ne sont pas conformes à cette exigence indique une tendance inquiétante en matière de manque d'éducation sur la façon d'utiliser correctement leur police de cyberassurance. »

Renforcer l'état de préparation

Tous les cadres supérieurs, y compris les dirigeants financiers, doivent agir de manière proactive et efficace pour se préparer et préparer leurs entreprises à une cyberattaque. Il est recommandé aux entreprises de tenir compte des conseils suivants concernant des pratiques exemplaires :

1. Mettre en place une équipe pluridisciplinaire d'intervention en cas d'intrusion.
2. Toujours effectuer une vérification préalable des principaux distributeurs ou fournisseurs extérieurs.
3. Préparer un plan de communications en cas de crise en interne et en externe, désigner des porte-paroles, des points de contact pour les médias, les employés et les intervenants et définir des plans d'intervention pour chaque rôle.
4. Identifier clairement les renseignements que détient l'entreprise, notamment où ils se trouvent et comment ils sont stockés.
5. Mettre à jour le plan d'intervention pluridisciplinaire en cas d'intrusion tous les 6 à 12 mois, et organiser des exercices de simulation de crise pour les équipes d'intervention.

Méthodologie

Cette enquête a été menée auprès de membres et d'intervenants de FEI Canada. Elle comptait 43 questions divisées en 3 catégories pour évaluer l'état de préparation des entreprises sur le plan des obligations juridiques, des assurances et des communications en cas de crise. Les participants ont obtenu un résultat pour chaque partie de l'enquête et une évaluation générale de l'état de préparation de leur entreprise contre une cyberattaque, à partir des réponses de chacun d'eux.

Cette enquête a été préparée en association avec Blakes, Cassels & Graydon LLP, Kaiser Lachance Communications et Ridge Canada. Il s'agit de la première itération de celle-ci. Le groupe compte poursuivre la collecte de réponses à ce sujet et de partager les résultats qu'il obtient.

Participez à l'enquête pour connaître vos résultats quant à votre état de préparation :
FEI Canada - Évaluation de la cybervulnérabilité

À propos de FEI Canada

Dirigeants financiers internationaux du Canada (FEI Canada) est une importante association sectorielle pour les principaux dirigeants financiers. Avec 12 sections régionales et plus de 1 600 membres, FEI Canada propose des occasions de perfectionnement professionnel, de réseautage, de leadership éclairé et de services de représentation à ses membres. www.feicanada.org

À propos de Blakes, Cassels & Graydon LLP

Le cabinet d'avocats Blakes, Cassels & Graydon LLP (Blakes) fournit des services juridiques de qualité exceptionnelle à de grandes entreprises du Canada et du monde entier. Notre réseau intégré de cabinets

répartis dans le monde entier permet à nos clients d'accéder à l'ensemble des compétences du cabinet dans pratiquement tous les domaines du droit commercial. www.blakes.com

À propose de Kaiser Lachance Communications
Kaiser Lachance Communications Inc. est une entreprise de communications avec des bureaux à Toronto et à Montréal. Nous offrons un ensemble de services de communications stratégiques et intégrés avec une spécialisation dans les communications d'entreprises, de marketing et financières. www.kaiserlachance.com

À propos de Ridge Canada
Ridge Canada est une agence générale de gestion cofondée par Tom Ridge, le premier secrétaire de la Sécurité intérieure, qui travaille exclusivement avec des courtiers en assurance sur les cyberrisques et les risques liés à la confidentialité. Ridge aide ses clients à comprendre, évaluer et obtenir une police de cyberassurance adaptée à leur entreprise. www.ridgecanada.insure

Traductions fournies par Alexa Translations. Alexa Translations est un partenaire de traduction de confiance qui fournit régulièrement des services de traduction de qualité aux entreprises des secteurs juridique et financier. Elle offre une technologie de traduction de pointe sécuritaire qui complète les services de traduction assurés par des personnes afin de répondre aux besoins toujours changeants des clients et de l'industrie dans son ensemble.

-30-

Pour tout renseignement supplémentaire concernant cette enquête et FEI Canada, veuillez communiquer avec :
Thomas Rigg
au 416-366-3007, poste 5105
trigg@feicanada.org

Pour toute demande de renseignements des médias, veuillez communiquer avec :
Kelly Morgan
au 647-725-2520, poste 225
kelly.morgan@kaiserlachance.com