Cyber (in)sécurité

Hartaj Nijjar, associé, Cybersécurité, KPMG au Canada
416-228-7007 | hnijjar@kpmg.ca

La cybersécurité est une source permanente (et croissante) d'inquiétude pour les organisations canadiennes. Devant l'escalade des attaques abondamment commentées dans les médias et l'urgence d'adopter de nouvelles technologies, les chefs de la direction ne peuvent ignorer les menaces virtuelles qui les guettent. Près des deux tiers (60 %) de nos chefs d'entreprise conviennent qu'ils devront tôt ou tard défendre leurs frontières numériques contre une cyberattaque, ce qui représente une hausse de 10 % par rapport aux résultats de 2018 et un écart marqué par rapport au pourcentage de leurs homologues étrangers qui se préparent à l'inévitable (53 %).

Ce constat est très révélateur. Il démontre que les organisations canadiennes ont atteint un niveau de maturité numérique qui les expose à des cyberrisques avec lesquels leurs contreparties américaines, britanniques ou chinoises, par exemple, ont déjà appris à naviguer. Il explique également pourquoi 59 % des dirigeants canadiens estiment qu'ils sont suffisamment préparés pour affronter une cyberattaque, soit 7 % de moins qu'en 2018, alors que leurs homologues étrangers, qui ont eu davantage de temps pour s'adapter aux nouvelles technologies et aux risques connexes, expriment un niveau de confiance supérieur (68 %).

Désavantage concurrentiel

La montée des inquiétudes en matière de cybersécurité a parallèlement accru l'importance accordée à la sécurité de l'information. La majorité des leaders canadiens (64 %) considèrent la sécurité de l'information comme une fonction stratégique et un facteur d'avantage concurrentiel de premier plan, contre 71 % à l'échelle mondiale. Il y a cependant une importante distinction à faire. En discutant avec nos clients, nous constatons que pour un grand nombre d'entre eux, les investissements en cybersécurité ne constituent pas tant un moyen de générer des bénéfices concrets que d'éviter de subir un désavantage concurrentiel dans un monde de plus en plus numérique.

L'évolution de la réglementation sur la protection des données contribue également à diriger les projecteurs sur ce problème. Le Règlement général sur la protection des données (RGPD) de l'Union européenne a resserré les règles et intensifié les contrôles relatifs à l'utilisation et à la protection des données des citoyens européens. Au Canada, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) a accru la pression sur les entreprises canadiennes pour qu'elles renforcent leur défense à défaut de quoi elles s'exposent à de lourdes pénalités financières et à des atteintes sévères à leur réputation.

Les résultats de cette année tendent à démontrer que les organisations canadiennes sont en train de rattraper leurs concurrents plus avancés sur le plan technologique. Et à mesure que les entreprises de chez nous continuent à intégrer l'intelligence artificielle, la chaîne de blocs, l'analyse de mégadonnées et d'autres outils novateurs à leurs activités, elles prennent de plus en plus conscience des menaces et des dangers qu'ils comportent.

Faire front commun

Apprendre à naviguer au milieu de ces risques demeure un défi de taille. Malgré la confiance qu'elles affichent dans leur capacité à contrer les cyberattaques, les organisations canadiennes ont de la difficulté à définir et à mettre en place les deux premiers remparts d'une manière efficace. Les professionnels de la sécurité, les responsables de la gestion des risques et les organismes de réglementation ont parfois des visions divergentes des mesures pratiques à mettre en œuvre pour surveiller les cyberrisques, ce qui nuit à l'élaboration de stratégies fiables.

Malheureusement, il n'existe pas de solution miracle. Pour trouver la réponse – ou la combinaison de réponses – adéquate, les chefs de la direction canadiens doivent faire l'inventaire de leurs actifs numériques les plus précieux, analyser l'ensemble des menaces dont ils sont l'objet et surveiller attentivement l'évolution des tendances dans le cyberespace. C'est ce qui leur permettra d'engager leurs équipes à prendre les mesures nécessaires, en matière de contrôle, de formation et de programme d'urgence, pour protéger les données, la propriété intellectuelle et les actifs numériques critiques contre les cyberattaques.

Dans quelle mesure votre organisation est-elle préparée à faire face à une cyberattaque :

BIEN PRÉPARÉE

58 % 69 %

NEUTRE

27 % 14 %

NON PRÉPARÉE

15 % 18 %

64 %

des répondants considèrent la sécurité de l'information comme une fonction stratégique et un facteur d'avantage concurrentiel

71 %

59 %

estiment qu'une solide stratégie de cybersécurité est essentielle pour établir un lien de confiance avec les parties prenantes

69 %

60 %

conviennent que leur organisation sera tôt ou tard la cible d'une cyberattaque

53 %

54 %

voient la cybersécurité comme une importante source d'inquiétude

42 %