# LA **CYBERSÉCURITÉ** POUR LES PETITES OU MOYENNES ENTREPRISES

**UNE ENTREVUE AVEC**

## PETER WHITTAKER

DIRECTEUR
DÉVELOPPEMENT DES ENTREPRISES,
SÉCURITÉ SPHYRNA

**Q : La pandémie de la COVID-19 a soulevé un urgent besoin de leadership collectif parmi tous les secteurs afin de s'attaquer aux toutes dernières cybermenaces. Que prévoyez-vous comme changements au cours des cinq ou dix prochaines années dans l'approche générale du Canada en matière de cyberrésilience?**

R : En trois mots, la future cyberrésilience dépend de vitesse, d'agilité et de jugement.

La COVID-19 a forcé les organisations à modifier leur vitesse de cybersécurité : elles ont dû se retourner complètement, délaissant le travail au bureau pour la maison, et ce, très rapidement. Cette situation a demandé une attention particulière, une évaluation brève des options et une volonté de changer d'approches tout aussi promptement. Un exemple de ce dernier point est lorsqu'une multitude d'entreprises ont laissé tomber un système de vidéoconférence en raison de failles de sécurité perçues chez un acteur dominant.

Ces changements en matière de vitesse nécessitent une certaine agilité organisationnelle et individuelle, à la fois pour les habiletés de réflexion et d'adaptation rapides qu'ils requièrent, mais aussi pour la transformation du fonctionnement d'une entreprise et, pour plusieurs, de ce qu'elle fait : les entreprises et les services qui réussissent à l'heure actuelle sont en mesure de voir un éventail de possibilités et de se concentrer sur ce qui est réalisable, significatif et utile.

Cette attention nécessite une appréciation commerciale et un jugement du risque : « Pourquoi sommes-nous réellement ici et comment pouvons-nous trouver le meilleur équilibre entre une atténuation des risques et des résultats opérationnels utiles, le tout dans un court délai, et sans risquer une exposition à long terme ni une perte d'actifs? »

Les organisations doivent institutionnaliser et opérationnaliser cette vitesse, cette agilité et ce jugement, et ce pour le long terme. Les entreprises et les services qui « reprennent forme » risquent une ossification en tentant de tout codifier ce qui a été fait dans une journée, sans penser au fait que ce sera à refaire le lendemain.

# LA **CYBERSÉCURITÉ** POUR LES PETITES OU MOYENNES ENTREPRISES

**Q : Quelles sont les considérations en matière de cybersécurité qui doivent être prises en compte par les organisations pendant la pandémie et à la suite de la reprise?**

R : À court terme, les organisations doivent être en mesure de prendre des décisions d'ordre de gestion des risques en peu de temps sans paniquer ni vouloir trop en faire : à grande vitesse, elles doivent pouvoir absorber de l'information sur leurs vulnérabilités en matière de technologie et de processus ainsi que décider s'il est mieux de ne rien faire ou d'apporter des changements, et s'ils sont spécifiques et techniques ou de nature plus générale et vague. Cela demande une idée précise de la valeur temporelle de l'information, tant pour l'organisation que pour ses adversaires, afin que les atténuations soient choisies en fonction de la façon dont les actifs informationnels apportent de la valeur à l'organisation aujourd'hui et pourront éventuellement en apporter aux adversaires.

À long terme, les organisations doivent être en mesure de régulièrement réexaminer des décisions prises concernant la valeur de l'information et d'entamer avec diligence un processus d'atténuations : « Continuons-nous de protéger cette information ou est-ce que les coûts entraînés surpassent sa valeur? Si tel est le cas, est-ce que nous la supprimons? » Cela peut être une décision difficile, puisque les entreprises cherchent un revenu prévisible et récurent, et l'aiment davantage lorsqu'il nécessite peu d'efforts. Historiquement, la tendance a toujours été de maximiser les bénéfices provenant d'actifs existants en réduisant les coûts associés à l'entretien, en particulier ceux concernant la sécurité, ce qui mène en fin de compte à des atteintes à la sécurité. Une entreprise peut être confrontée à la décision d'interrompre une source de revenus dans le but d'éviter une future atteinte à la sécurité.

En fait, plus fondamentalement, la sécurité des réseaux et des systèmes informatiques ne dépend que des gens. Protéger les secteurs d'activités et les actifs informationnels signifie réellement de veiller à ce que les employées puissent prendre de bonnes décisions.

La cybersécurité de demain dépendra en grande partie des cultures d'entreprise saines qui estiment leurs employées en tant qu'humains et qui s'assurent qu'ils ont tout ce dont ils ont besoin pour accomplir leurs tâches, y compris la santé et du soutien.

**Q : En tant qu'expert en cybersécurité et contributeur actif au comité technique sur la cybersécurité du Conseil, pourriez-vous partager vos observations sur l'élaboration d'une norme nationale qui permet d'améliorer la posture en matière de cybersécurité des petites et moyennes entreprises? En quoi pensez-vous qu'elle pourrait aider les organisations à gérer les risques actuels reliés à la cyberdéfense?**

R : Les grandes entreprises possèdent le luxe comparatif de pouvoir mettre sur pied des équipes multidisciplinaires pour résoudre des problèmes tactiques, opérationnels et stratégiques. Ces experts ont la capacité de saisir la complexité d'une norme, de l'intégrer à la direction et à la politique de l'entreprise, de distribuer le travail à des experts en la matière (EM), de gérer les questions et d'interpréter les intentions, etc.

Plus une PME est de petite taille, plus elle est concentrée sur l'entreprise en soi. Bref, il y a bien moins de temps, d'énergie et d'attention pour toute autre préoccupation. Il ne faut pas non plus oublier que, à moins qu'elle œuvre dans le domaine, elle n'aura sans doute pas accès à des EM en cybersécurité.

Nos normes doivent donc être précises et claires. Nous, en tant que contributeurs, devons nous assurer que nous comprenons exactement ce que nous voulons dire et que ce soit exprimé le plus simplement possible. Comme les experts de tous les domaines, nous ne faisons pas exceptions : nous avons tendance à utiliser du jargon et des acronymes en trois lettres. Nous nous devons de les éviter dans la mesure du possible, mais aussi de reconnaitre qu'un même mot peut corresponde à une définition très différente dans un autre contexte — et il est fort probable que les employés et les propriétaires de petites ou moyennes entreprises abordent les situations de façon très différente. Ces dissemblances peuvent mener à des interprétations complètement opposées à ce que nous, les EM, pensions clair et net.