MASTERCARD RISKRECON • ANALYSE DE NIVEAU DE RISQUE
CANADA • JUILLET 2025

Cyberrisques au Canada

Tendances du secteur et observations

Table des matières

L'importance de la gestion des cyberrisques

La gestion des cyberrisques est essentielle pour permettre aux organisations canadiennes de protéger leurs ressources et de renforcer la confiance de leurs clients. Face à l'avènement de cybermenaces sophistiquées comme les rançongiciels, l'hameçonnage et les violations de données, il est essentiel que les entreprises adoptent des stratégies de sécurité proactives pour atténuer les risques financiers et d'atteinte à leurs activités et à leur réputation.

Dans ce livre blanc, RiskRecon se penche sur des observations et faits de cybersécurité essentiels englobant plus de 4 900 organisations établies au Canada fondés sur l'analyse des données de cyberhygiène recueillies*. Plusieurs des secteurs d'activité concernés comprennent des infrastructures importantes et sont essentiels à la sécurité des entreprises canadiennes. Ainsi, ce rapport se concentre sur les cyberrisques les plus importants de tous les secteurs pour démontrer l'importance croissante d'intégrer des stratégies d'atténuation des cyberrisques au sein des organisations afin de contrer les risques lorsqu'ils surviennent.

En adoptant une approche proactive, les entreprises canadiennes peuvent renforcer leur niveau de sécurité et instaurer une culture de cyberconfiance et d'innovation. RiskRecon et Mastercard s'engagent à aider les entreprises à se protéger contre les cyberrisques en constante évolution pour ainsi garantir la sécurité et la résilience de l'écosystème canadien.

*Sondage mené en 2024 par le biais d'une analyse des entités canadiennes au sein de RiskRecon.

Ce rapport vise à fournir un aperçu des pratiques de cybersécurité qu'emploient les organisations privées, publiques et gouvernementales dans 14 secteurs d'activité au Canada, notamment:


Agriculture/sylviculture/ pêche/chasse


Arts et spectacles


Construction/ entreposage


Éducation


Finance/assurance


Soins de santé


Information/ informatique/logiciels


Fabrication


Pétrole et gaz


Commerce de détail


Science/secteurs techniques


Transport


Services publics


Commerce de gros

RiskRecon a évalué passivement les mesures de protection et les lacunes en matière de sécurité et d'infrastructure d'organisations canadiennes en fonction de plus de 40 critères dans neuf domaines de sécurité, notamment :


Sécurité des courriels


Événements de violation de données


Filtrage des réseaux


Sécurité des services DNS


Réputation des systèmes


Chiffrement Web


Sécurité des applications


Application de correctifs logiciels


Hébergement de systèmes

Ces renseignements ont ensuite été évalués en fonction de l'incidence de chaque vulnérabilité relevée afin de déterminer l'évaluation finale de cyberrisque d'une organisation.

Observations quant aux cyberrisques dans les différents secteurs d'activité au Canada

La section suivante présente une analyse des tendances en matière d'hygiène et d'efficacité de cybersécurité par secteur dans 4 900 organisations au sein de RiskRecon. Pour chaque organisation évaluée, RiskRecon génère une cote de cyberrisque dérivée d'une combinaison de la valeur des actifs et de la gravité des problèmes. Ces résultats ont été regroupés à l'échelle du Canada et par secteur d'activité afin de fournir des observations pertinentes sur les cyberrisques.

Observation 1:

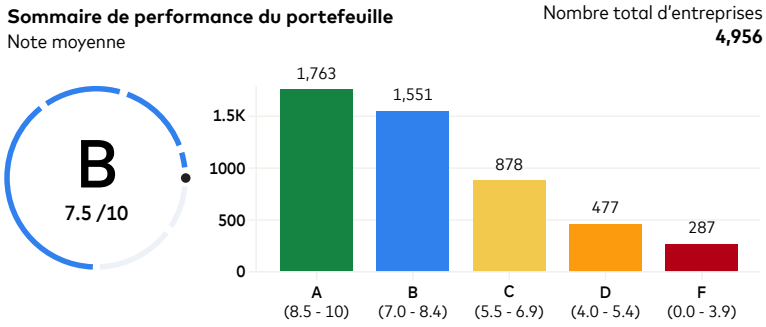
Les organisations canadiennes ont une bonne cyberhygiène, bien qu'elles soient considérées comme des adopteurs dans le domaine de la cybersécurité

RiskRecon évalue la qualité de l'efficacité d'une organisation en matière de cyberrisques à l'aide d'une échelle de A à F et d'une échelle numérique de 0 à 10. La cote est fondée sur l'évaluation et la priorité en matière de risque des problèmes présents dans l'environnement, comme observés par la technologie d'évaluation passive des risques de RiskRecon.

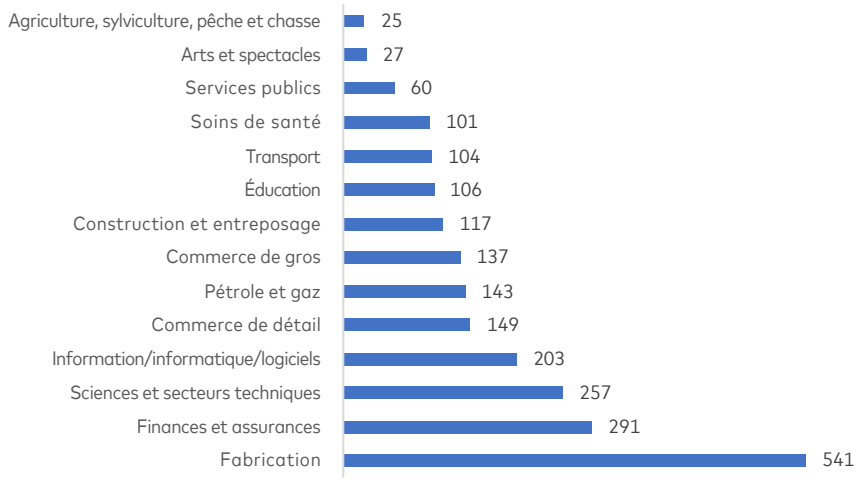
Les organisations canadiennes sondées ont une cote de cybersécurité moyenne (B/7,5), et 36 % d'entre elles ont obtenu une cote élevée (A/8,5 à 10). De manière générale, 66 % des organisations ont une cote moyenne à élevée (A/B), ce qui indique que les entreprises canadiennes ont une bonne cyberhygiène qui tient compte de leurs actifs publics.

L'autre tiers des organisations canadiennes est réparti de façon décroissante dans les cotes C à F, ce qui indique la présence de problèmes de cyberrisques plus prioritaires. Il est important de noter qu'une partie de ces résultats peut être influencée par une forte concentration d'organisations de petite et moyenne taille, qui se situent généralement aux extrémités de l'échelle d'évaluation.

Figure 1: Distribution des évaluations de cybersécurité de RiskRecon auprès de 4 956 organisations canadiennes sur une échelle de A à F (0 à 10)



RiskRecon Distribution des organisations au Canada par secteur d'activité



Observation 2:
La cyberhygiène est relativement stable d'un secteur d'activité à l'autre, avec quelques nuances découlant de facteurs propres à chaque secteur

Le tableau ci-dessous présente la répartition des notes et des évaluations au sein des différents secteurs d'activité. De nombreux secteurs ont montré des résultats positifs en moyenne, les secteurs de l'assurance et des services financiers, du commerce de détail et des services publics ayant les meilleurs résultats en matière de cyberhygiène. Certains secteurs présentent une importante variation dans la distribution des cotes, ce qui suggère que le secteur peut être confronté à des problèmes de cybersécurité qui font baisser cette cote. Ces problèmes sont expliqués plus en détail dans le rapport.

Si tous les secteurs d'activité comprennent des organisations ayant de bons résultats, certains secteurs comptent un plus grand nombre d'organisations ayant de moins bons résultats ou qui présentent actuellement des risques élevés. Ces problèmes à haut risque sont classés par ordre de priorité en fonction de leur gravité et de leur incidence globale.

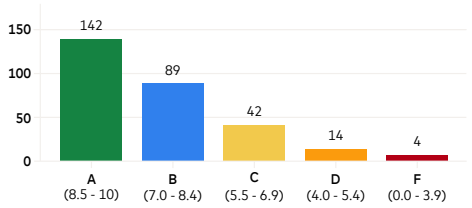
Figure 2: Distribution des évaluations de cybersécurité de RiskRecon par secteur d'activité sur une échelle de A à F (0 à 10)

Assurance et services financiers

Sommaire de performance du portefeuille
Note moyenne

B
8.2 /10

Nombre total d'entreprises
291

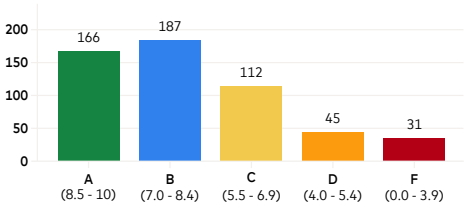


Fabrication

Sommaire de performance du portefeuille
Note moyenne

B
7.5 /10

Nombre total d'entreprises
541

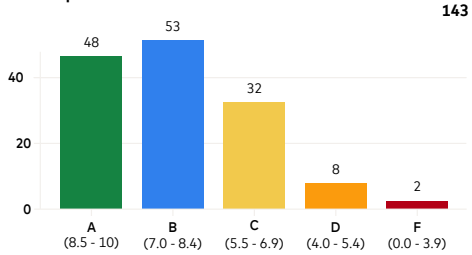


Pétrole et gaz

Sommaire de performance du portefeuille
Note moyenne

B
7.8 /10

Nombre total d'entreprises
143

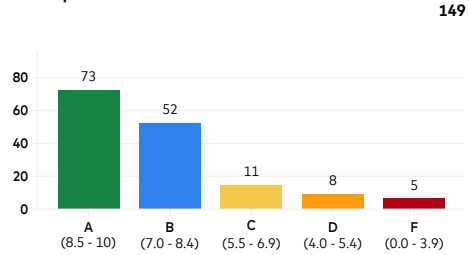


Commerce de détail

Sommaire de performance du portefeuille
Note moyenne

B
8.2 /10

Nombre total d'entreprises
149

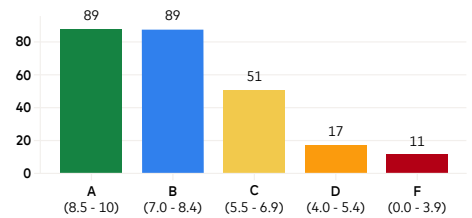


Secteur scientifique et technique

Sommaire de performance du portefeuille
Note moyenne

B
7.6 /10

Nombre total d'entreprises
257

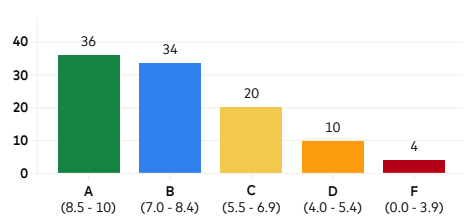


Transport

Sommaire de performance du portefeuille
Note moyenne

B
7.5 /10

Nombre total d'entreprises
104

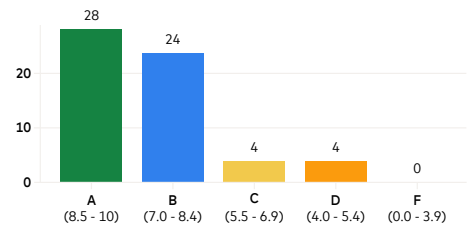


Services publics

Sommaire de performance du portefeuille
Note moyenne

B
8.2 /10

Nombre total d'entreprises
60

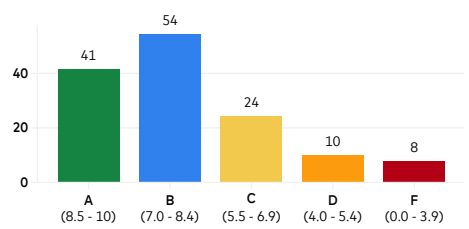


Commerce de gros

Sommaire de performance du portefeuille
Note moyenne

B
7.4 /10

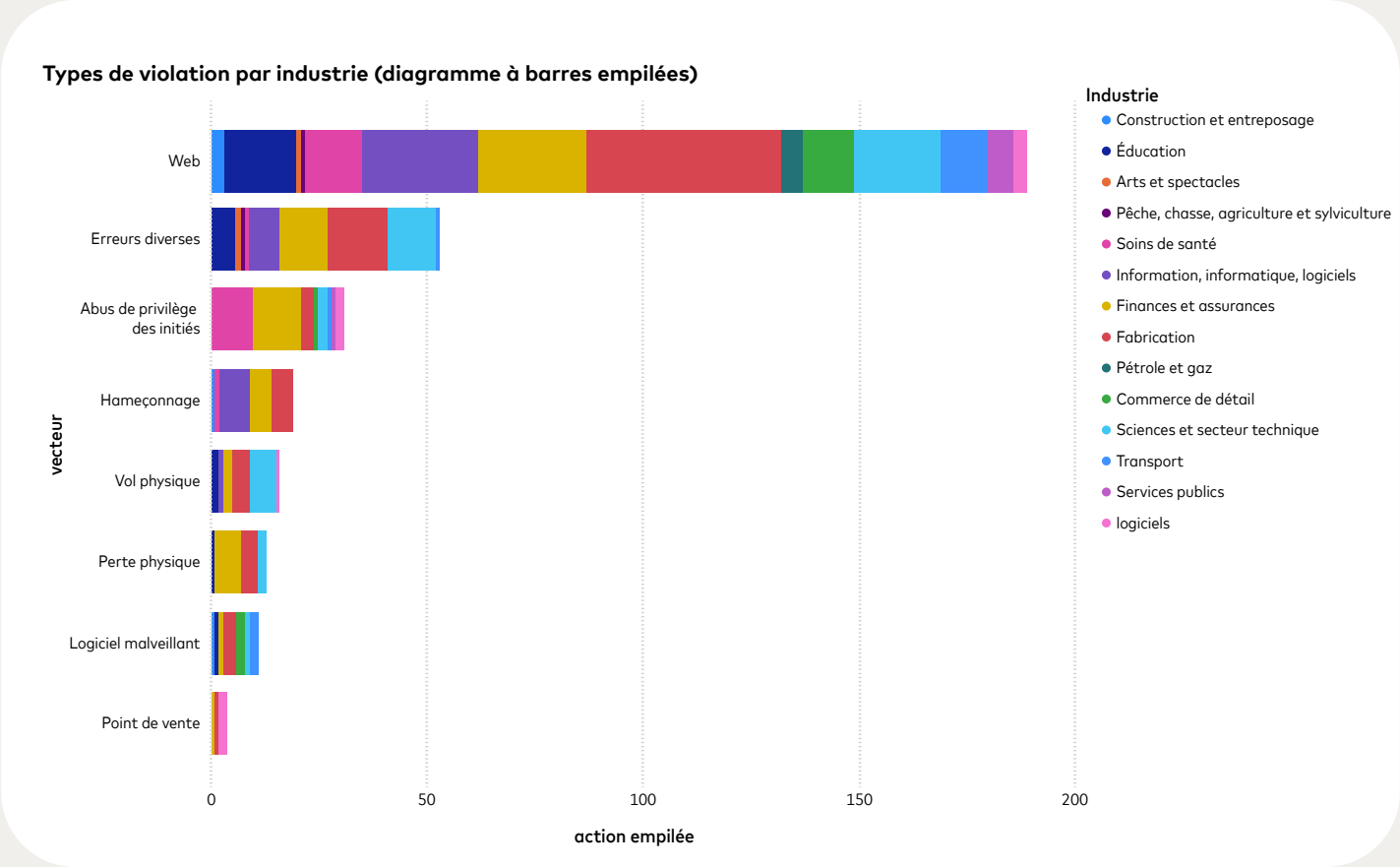
Nombre total d'entreprises
137



Observation 3:
Tous les secteurs d'activité au Canada font face à un grand nombre d'attaques sur le Web

Comme illustré ci-dessous, tous les secteurs d'activité font face à un grand nombre d'attaques sur le Web comparativement à d'autres types de violations comme l'abus de privilèges par les initiés, l'hameçonnage et le vol physique. Les attaques sur le Web ont été incluses après un processus d'examen approfondi de sept sources externes par la plateforme RiskRecon.

Figure 3: Types de violations dans les différents secteurs d'activité au Canada



Observation 4:
Certains secteurs d'activités comme l'industrie manufacturière, la sécurité de l'information et l'éducation font face à un plus grand nombre de cyberproblèmes de niveau de risque moyen ou élevé

Pour mieux comprendre ce qui peut être à l'origine de la faible cote de cybersécurité d'un secteur, nous avons décomposé les problèmes par gravité dans l'ensemble des secteurs d'activité. La gravité d'un problème dans RiskRecon est fortement influencée par plusieurs types d'intrants qui contribuent à la note de cybersécurité:

- Préoccupations en matière de correctifs de logiciels
- Services à risque (ports ouverts)
- Appareils IdO publiquement accessibles
- Systèmes essentiels non chiffrés

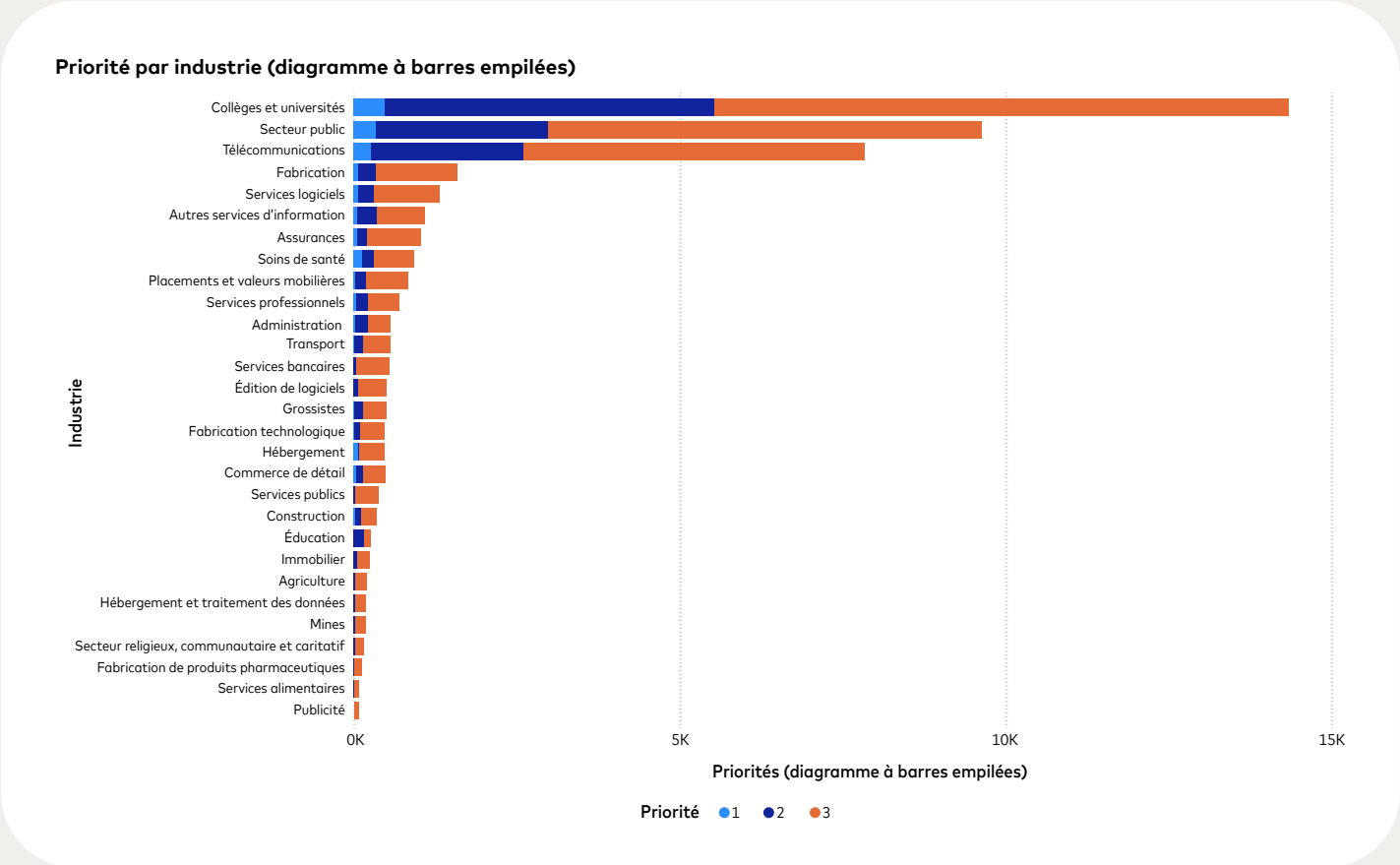
Selon la méthodologie expliquée dans cette section, RiskRecon a fourni une ventilation des organisations par secteur d'activité afin de mettre davantage de l'avant les domaines de préoccupation spécifiques susceptibles d'intéresser les parties responsables appropriées au Canada. La section suivante présente un aperçu de la cyberhygiène et des résultats de toutes les organisations recensées au Canada. Le tableau ci-dessous résume la concentration des problèmes à haut risque dans chaque secteur, classés par ordre de gravité (la priorité 1 est élevée, la priorité 2 est moyenne et la priorité 3 est faible). Bien que la cote moyenne globale soit positive (B/7,5), plusieurs organisations présentent un nombre élevé de problèmes de priorité 1, 2 et 3, qui présentent un risque le plus élevé.

En analysant le graphique ci-dessus, on constate que les collèges et les universités ont le plus grand nombre de problèmes de priorité 1, 2 et 3 combinés. Ce fait est dû au modèle collectif normal d'échange de renseignements de ce secteur.

De plus, bien que le secteur public et des télécommunications soient confrontés à des problèmes de priorité 1, la résolution de plusieurs problèmes de priorité 3 pourrait permettre d'obtenir une meilleure cote en réglant ainsi des problèmes plus faciles à résoudre.

Enfin, les secteurs de l'industrie manufacturière, de l'information et scientifiques et techniques sont ceux qui font face au plus grand nombre de problèmes, ce qui laisse supposer des lacunes dans les méthodes de lutte contre les risques de cybersécurité. Une analyse approfondie des facteurs à l'origine du nombre de problèmes est fournie ci-dessous; aux fins du présent rapport, nous nous sommes concentrés sur les problèmes les plus graves (priorité 1). Il est également important de noter que le nombre de problèmes dans un secteur peut être dû à la présence d'un plus grand nombre d'entreprises dans celui-ci.

Figure 4: Nombre de problèmes par priorité de risque dans les secteurs d'activité au Canada



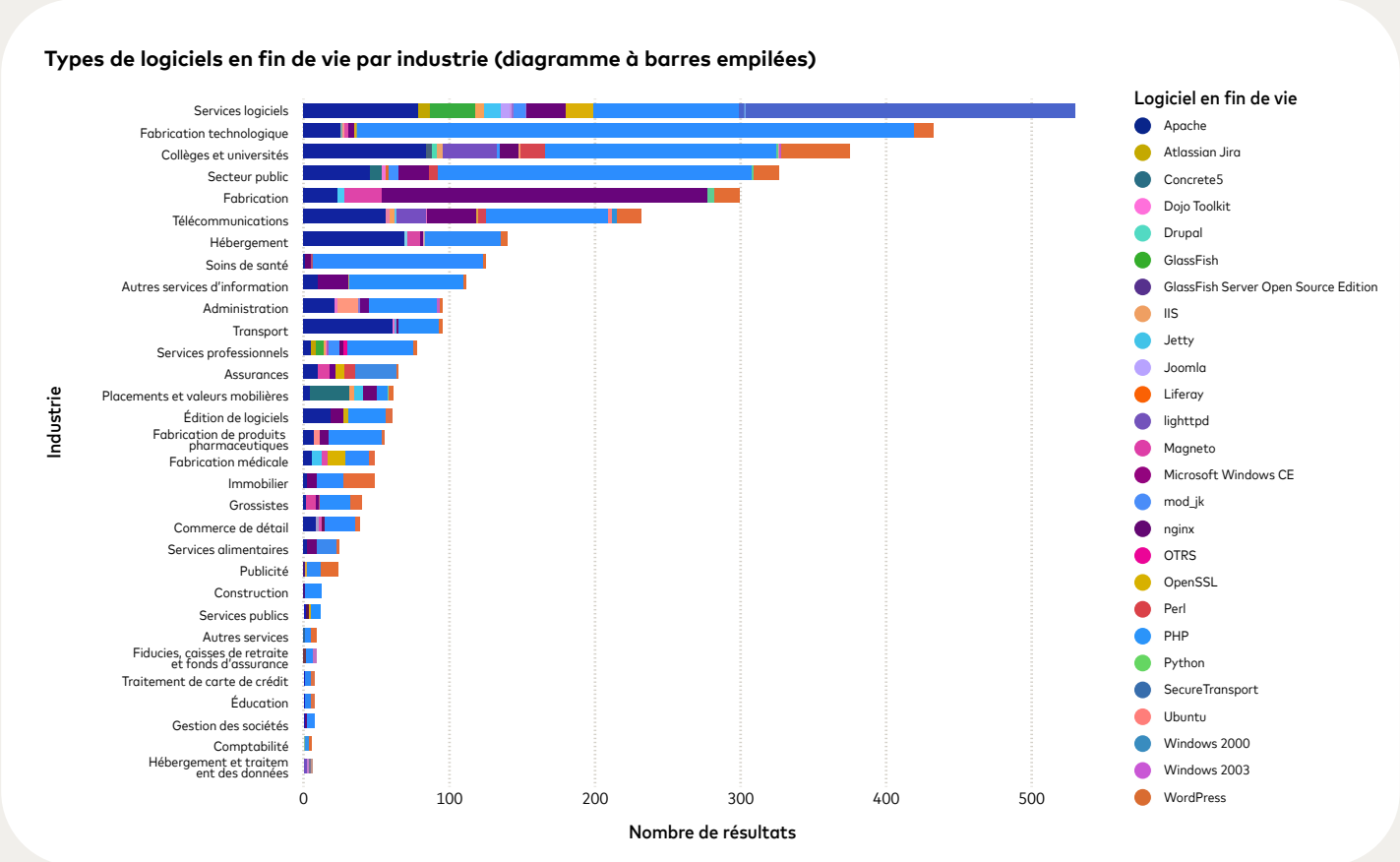
Observation 5:

Le secteur des services logiciels est confronté à des risques importants de fuite de données en raison de l'utilisation de logiciels non pris en charge ou en fin de vie

L'application de correctifs logiciels et, notamment, la présence de logiciels non pris en charge ou en fin de vie (logiciels dont l'éditeur ne fournit plus de correctifs ou de protection contre les vulnérabilités, le cas échéant) est un indicateur important de risque de violations de données ou d'attaques par rançongiciel.

Le tableau ci-dessous résume le type et la concentration des logiciels en fin de vie observés dans les entreprises analysées. Comme on peut le voir ci-dessous, les services logiciels sont très sensibles aux violations dues à des logiciels en fin de vie. La majorité des versions de logiciels en fin de vie détectées sont des versions de PHP (un serveur d'application) et d'Apache (un serveur Web) qui sont particulièrement susceptibles de présenter de graves vulnérabilités.

Figure 5: Types de logiciels en fin de vie et non pris en charge dans les différents secteurs d'activité au Canada



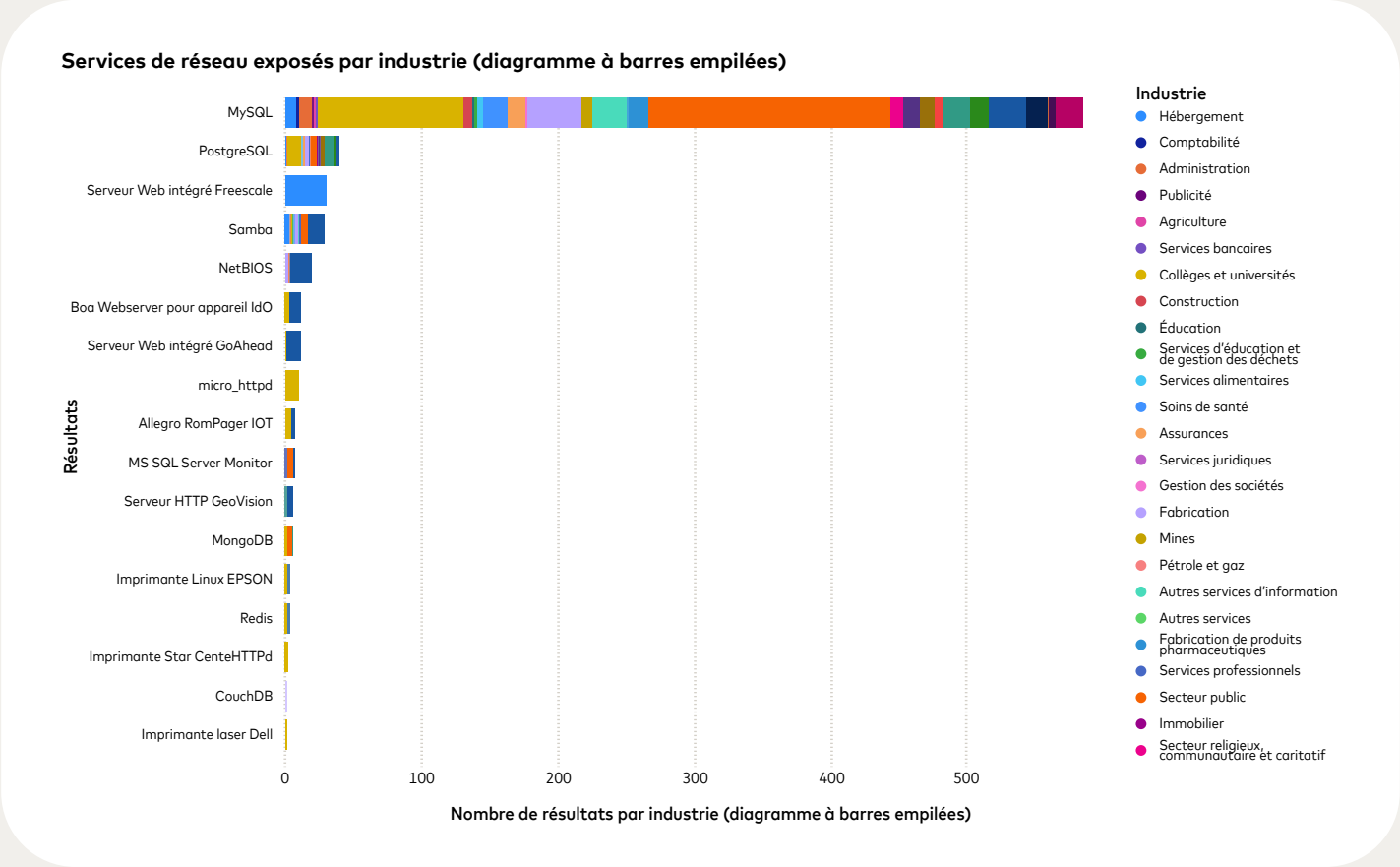
Observation 6:
Le secteur public et le secteur de l'enseignement et des télécommunications présentent un plus grand nombre de services réseau à risque

Le domaine de sécurité de filtrage de réseau de RiskRecon fournit des informations sur les organisations et leurs systèmes connectés à l'Internet, y compris sur les situations où elles n'emploient pas un filtrage approprié. Un tel filtrage inapproprié est démontré par la présence de ports ouverts ou à risque (services à risque) ou la présence d'appareils à capacités d'Internet des objets (IdO) accessibles. Ces lacunes forment des points d'entrée potentiels pour les acteurs malveillants, et il est recommandé de filtrer et de protéger ces points d'entrée de manière appropriée.

RiskRecon emploie une combinaison d'observations directes et de sources de données commerciales pour identifier les systèmes dans lesquels des services ou des appareils sont exposés à l'Internet public. Comme illustré ci-dessous, la majorité des problèmes sont liés au service de serveur MySQL, qui peut exposer des données non publiques ou permettre à un pirate de contrôler le système identifié. Il est clair que le secteur public, les établissements d'enseignement supérieur et les universités et les secteurs des télécommunications présentent les services réseau les plus à risque, ce qui offre aux acteurs malveillants une occasion importante de pénétrer dans les systèmes.

Il est important de noter que le nombre plus élevé de ports ouverts et d'appareils IdO accessibles dans le secteur de l'éducation peut être dû à des facteurs propres à ce secteur. Notamment, la plupart des établissements d'enseignement supérieur et des universités font partie d'une infrastructure de réseau où les services de réseau peuvent être à risque en raison des activités des étudiants ou du transfert de données entre les établissements.

Figure 6: Services de réseaux exposés par secteur d'activité



À propos de RiskRecon

RiskRecon, une société de Mastercard, est une plateforme de gestion des risques de cybersécurité qui fournit des évaluations automatisées et basées sur des données des risques de cybersécurité de tiers. Elle permet aux organisations d'évaluer et de contrôler en continu le niveau de sécurité de tiers, de partenaires et d'autres organisations externes pour ainsi aider les entreprises à atténuer les cybermenaces dans un environnement de plus en plus interconnecté.

Les analyses de RiskRecon fournissent des évaluations des cyberrisques pour chaque organisation analysée et décomposent l'évaluation globale en neuf domaines de sécurité évalués, eux-mêmes décomposés en 36 sous-domaines spécifiquement évalués (appelés critères de sécurité), et ces analyses sont étayées par des conclusions détaillées, une hiérarchisation des problèmes et des capacités d'analyse approfondies.

CE QUE RISKRECON FAIT:

Exploration en profondeur des bases de données d'enregistrement de domaines

Exploration en profondeur des bases de données d'enregistrement de réseaux

Analyse de l'adresse IP du DNS Internet par rapport aux journaux de résolution de noms d'hôte

Requêtes DNS

Navigation sommaire sur les sites Web en respectant les instructions du fichier robots.txt

Analyse du code, du contenu et des configurations accessibles au public

Suivi et analyse des flux de réputation d'adresses IP commerciales et de code source libre

Recherche sur Internet d'informations pertinentes comme des indicateurs de perte de données

Analyse de données de balayage des ports Internet provenant d'un fournisseur commercial

CE QUE RISKRECON NE FAIT PAS:

Modification des paramètres

Injection de code

Exécution de scripts intersites

Exécution d'injections SQL

Tentative de contournement d'authentification

Tests de dépassement de mémoire tampon

Remplissage de champs de formulaire

Déchiffrage de données de connexion

Exploitation de vulnérabilité

Tentative de contournement des contrôles de sécurité

Personnes-ressources principales

Vous désirez en savoir plus?

Vous désirez en savoir plus? Veuillez communiquer avec Chetan Bhogal pour découvrir la valeur ajoutée que RiskRecon peut offrir à votre organisation.