prompt

L'état de la cybersécurité au Québec : Pratiques, incidents, et résilience des entreprises

Analyse des données de l'Enquête canadienne sur la cybersécurité et le cybercrime (ECCC de 2021 et 2023) de Statistique Canada

Benoît Dupont & Jessica Roy
IMC2 – Université de Montréal

Juin 2026

Avec la participation financière de
Québec

Table des matières

Introduction 1

Méthodologie 3

Chapitre 1. Évolution de la posture de cybersécurité des entreprises québécoises entre 2021 et 2023 5

Portrait des cyberattaques subies 5

Panorama de l'évolution des pratiques de cybersécurité 7

Expertise en cybersécurité disponible à l'interne 7

Mesures techniques et activités de gestion des risques 10

Relations avec les partenaires externes et réponses aux cyberattaques 16

Chapitre 2. Mise en perspective de la posture de cybersécurité québécoise dans le contexte canadien 20

Victimologie comparée 20

Mesures et pratiques de cybersécurité 22

Employés spécialisés en cybersécurité et recrutement 22

Sensibilisation de l'ensemble des employés : le Québec en retrait 25

Fréquence et régularité des mises à jour à la haute direction : deux profils distincts 25

Auto-évaluation du niveau de préparation et risque de sur-confiance 26

Gestion des risques et mesures internes 27

Collaboration et pratiques partenariales 30

Chapitre 3. Pratiques de cybersécurité et cyber-résilience : une analyse multivariée 33

Profil de l'échantillon et distribution des variables 33

Déterminants de la victimisation : ce qui protège réellement les organisations 35

Déterminants des coûts de rétablissement : la gouvernance comme variable protectrice 37

Déterminants des arrêts de service : les limites de la prédictibilité 41

Synthèse : la cybersécurité comme investissement en capital humain 44

INTRODUCTION

Les connaissances sur l'état de la cybersécurité dans les entreprises des pays développés dépendent généralement de sondages produits par les vendeurs de solutions techniques et de services-conseils qui profitent de la visibilité offerte aux résultats de ces études dans les médias pour augmenter leur notoriété auprès de clients potentiels. Certains de ces sondages sont reconduits annuellement et sont attendus avec impatience par l'industrie, à l'image de l'étude du Ponemon Institute et d'IBM sur le coût des brèches de données, qui permet d'étalonner les impacts financiers, les causes et l'efficacité des mesures d'atténuation à l'échelle mondiale.[1] Si certains de ces sondages sont devenus des références incontournables en matière de cybersécurité, la majorité d'entre eux souffrent de faiblesses méthodologiques qui limitent leur utilité : les échantillons à partir desquels les données sont recueillies sont de tailles très limitées et jamais représentatifs, les taux de réponse sont faibles et introduisent des biais de sélection, et la nature des questions découle plus souvent des objectifs commerciaux de l'entreprise qui commandite ces études que d'un souci de mesurer de manière rigoureuse l'exposition des organisations aux risques cyber et la maturité de leurs pratiques de sécurité.[2]

Les études menées par les agences gouvernementales de statistique publique peuvent compenser ces faiblesses, mais rares sont les pays qui disposent des ressources suffisantes pour établir un programme national de collecte des données en cybersécurité, notamment en raison des coûts induits et de l'expertise technique nécessaire. Par chance, notre pays dispose d'un tel programme à travers l'Enquête canadienne sur la cybersécurité et le cybercrime (ECCC) de Statistique Canada, financée depuis 2018 par Sécurité publique Canada. Par la taille généreuse de son échantillon (plus de 10 000 entreprises à chaque vague), sa régularité (l'enquête est administrée tous les deux ans), l'obligation pour les entreprises de participer à l'enquête en vertu de lois fédérales (ce qui garantit des taux de réponse de plus de 70%), et la relative stabilité de son questionnaire d'une vague à l'autre, cette enquête est probablement l'une des plus représentatives des pratiques de cybersécurité des entreprises et des enjeux auxquels elles font face à l'échelle mondiale.

Bien que chaque vague fasse l'objet d'un rapport détaillé de la part de Statistique Canada, les résultats restent souvent présentés à très haut niveau et exploitent rarement le plein potentiel de la richesse des données recueillies.[3] Par ailleurs, les résultats publiés concernent uniquement l'ensemble du Canada, alors que des variations importantes peuvent survenir d'une province à l'autre, à la faveur de l'adoption de cadres règlementaires particuliers venant redéfinir les obligations et incitatifs des organisations en matière de cybersécurité. C'est par exemple ce qui s'est produit au Québec en 2021 avec l'adoption de la Loi 25 modernisant les lois sur la protection des renseignements personnels et venant notamment renforcer les exigences à l'égard des entreprises lors des incidents de confidentialité qui résultent souvent

[1] Ponemon Institute (2025), *Cost of a data breach report 2025 The AI oversight gap*, IBM, Armonk.

[2] Côté, A.-M., Bérubé, M., et Dupont, B. (2016), Statistiques et menaces numériques, Comment les organisations de sécurité quantifient la cybercriminalité, *Réseaux*, vol 3-4, no. 197-198, pp. 203-224.

[3] Voir par exemple Statistique Canada (2024), L'incidence du cybercrime sur les entreprises canadiennes, 2023, *Le Quotidien,* 21 octobre; ou Statistique Canada (2020), About one-fifth of Canadian businesses were impacted by cyber security incidents in 2019, *The Daily*, 20 octobre.

de cyberattaques. Cette loi est entrée en vigueur graduellement entre septembre 2022 et septembre 2024, forçant les entreprises de la province à se conformer à des obligations plus strictes en matière de gouvernance, de transparence et de cybersécurité.

C'est de la convergence entre la disponibilité de données d'une rare qualité au Canada, d'une part, et le souci de mieux comprendre les particularités de la posture de cybersécurité des entreprises québécoises dans un contexte législatif en évolution, d'autre part, que découle ce rapport. Grâce au programme d'accès sécurisé aux données de Statistique Canada, nous avons pu travailler sur les fichiers de microdonnées confidentielles de l'ECCC afin d'extraire le sous-groupe d'entreprises établies au Québec. Cela nous a permis de procéder à des analyses comparatives plus poussées que celles disponibles dans les documents publics de Statistique Canada. Cette démarche visait plus spécifiquement à atteindre trois objectifs :

1. Dresser un portrait dynamique de la posture de cybersécurité des entreprises québécoises entre 2021 et 2023 et identifier quels changements la Loi 25 avait pu provoquer pendant ces deux premières années de mise en application;
2. Comparer l'exposition aux cyber-risques et les pratiques de cybersécurité des entreprises québécoises avec celles de leurs homologues du reste du Canada, afin de mettre en lumière d'éventuelles spécificités et des défis nécessitant une attention particulière;
3. Essayer d'utiliser ces données extrêmement détaillées afin d'identifier les mesures ou les pratiques de cybersécurité qui permettent d'améliorer la cyber-résilience des entreprises québécoises en les mettant à l'abri des cyberattaques et en réduisant leurs délais et leurs coûts de rétablissement.

Ces trois objectifs sont successivement abordés dans les trois chapitres qui constituent ce rapport, après une section méthodologique qui précise la nature des données utilisées et leur traitement.

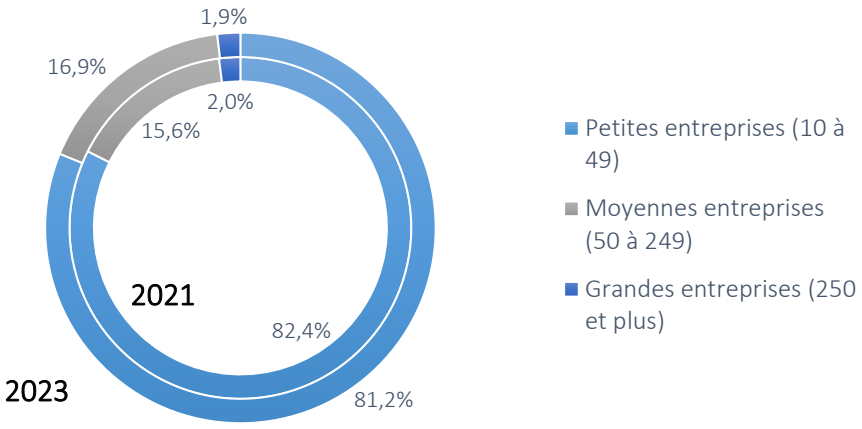
Les constats de cette étude sont nombreux et concernent des volets très diversifiés de la cybersécurité en entreprise, mais les principaux peuvent être résumés comme suit : entre 2021 et 2023, les entreprises québécoises ont absorbé un doublement des coûts d'incidents et ont appliqué les exigences nouvelles de la Loi 25 en renforçant leur gouvernance via une implication systématique de la haute direction, des politiques formelles, ou un recours plus fréquent aux experts externes. Toutefois, aucun de ces dispositifs n'a démontré d'effet mesurable sur leur cybersécurité. Par ailleurs, les analyses multivariées sont sans ambiguïté : la seule variable qui réduit de façon constante la victimisation, les coûts de rétablissement et les arrêts de service est la présence d'employés spécialisés en cybersécurité. Malheureusement, c'est précisément la ressource qui stagne au Québec. La cyber-résilience québécoise repose ainsi sur une tension encore non résolue : la nécessité de renforcer la conformité formelle aux exigences législatives tout en augmentant les investissements dans un capital humain spécialisé à la disponibilité limitée.

MÉTHODOLOGIE

Cette étude s'appuie sur les deux vagues les plus récentes de l'Enquête canadienne sur la cybersécurité et le cybercrime (ECCC), conduite par Statistique Canada pour le compte de Sécurité publique Canada.[4] Réalisée par questionnaire électronique auprès d'entreprises canadiennes comptant dix employés et plus, l'ECCC mesure l'incidence des cyber-risques auxquels font face les entreprises ainsi que les pratiques mises en place pour prévenir les incidents et en atténuer les conséquences. La population-cible est constituée des entreprises inscrites au Registre des entreprises de Statistique Canada, couvrant la quasi-totalité des secteurs définis selon le Système de classification des industries de l'Amérique du Nord (SCIAN 2022). L'échantillon est stratifié par industrie et par taille d'entreprise : petites (10 à 49 employés), moyennes (50 à 249) et grandes (250 et plus). La vague de 2023, dont la collecte s'est déroulée de janvier à mars 2024 pour une période de référence correspondant à l'année civile 2023, a été diffusée officiellement le 21 octobre 2024. Elle comprend environ 12 000 entreprises à l'échelle canadienne, dont quelque 2 800 au Québec, pour un taux de réponse de 71 %. Des poids d'enquête par calage sont associés aux données afin de produire des estimations représentatives de la population cible. La comparabilité entre les vagues de 2021 et de 2023 est assurée par l'harmonisation des strates d'échantillonnage et des procédures d'imputation, ce qui permet d'attribuer les évolutions documentées à des changements substantiels plutôt qu'à des artefacts de conception. La combinaison d'un échantillon d'une telle taille, d'un taux de réponse aussi élevé et de mesures méthodologiques aussi rigoureuses, font de ce sondage l'un des plus fiables et des plus représentatifs au monde sur les questions de cybersécurité en entreprise.

La composition de l'échantillon selon la taille des entreprises est représentative de l'économie québécoise et les infimes différences observées résultent de la pondération appliquée lors de l'extraction des données.

Figure 1 : Taille des entreprises de l'échantillon



[4] Adapté de Statistique Canada, Enquête canadienne sur la cybersécurité et le cybercrime, 2021 et 2023. Cela ne constitue pas une approbation de ce produit par Statistique Canada.

L'analyse est structurée en trois sections. La première compare les pratiques déclarées par les entreprises québécoises et leur évolution entre 2021 et 2023 à l'aide de tableaux de contingence et de tests de Mann-Whitney pour les variables continues. La deuxième effectue une comparaison similaire entre le Québec et le reste du Canada pour 2023. La troisième section présente des analyses multivariées afin d'évaluer l'effet des mesures et pratiques de gestion des risques sur l'exposition aux cyber-attaques et les capacités de rétablissement (rapidité de retour à la normale et coûts induits). Ces calculs s'appuient sur trois modèles de régression logistique binaire pour les variables dichotomiques (résultats exprimés en rapports de cotes) et deux modèles linéaires généralisés avec distribution Gamma pour les variables continues (résultats exprimés en rapports de moyennes), choisis en raison de la distribution asymétrique de ces dernières.

Les analyses descriptives des sections 1 et 2 utilisent les poids d'enquête. Les analyses multivariées de la section 3, réalisées à partir des données non pondérées, sont à interpréter comme des associations observées au sein de l'échantillon plutôt que comme des estimations généralisables à l'ensemble de la population.

Les analyses statistiques permettent de déterminer si une différence entre deux groupes (comme entre les entreprises québécoises de 2021 et de 2023) est réelle ou simplement due au hasard. Mais elles ne disent pas, en elles-mêmes, si cette différence est importante. Dans une enquête portant sur des dizaines de milliers d'entreprises, même un écart infime peut être déclaré statistiquement significatif simplement parce que l'échantillon est très grand. Pour distinguer ce qui est statistiquement détectable de ce qui est substantiellement significatif, les résultats présentés dans ce rapport sont accompagnés d'une mesure indiquant l'intensité de l'association observée, c'est-à-dire à quel point deux variables évoluent ensemble de façon prononcée. Ces niveaux d'intensité sont établis à partir du eta carré (η^2), une mesure couramment utilisée en sciences sociales pour quantifier la force des associations statistiques entre variables catégorielles. Cette mesure varie entre 0 et 1 : plus elle est proche de 1, plus la relation est marquée. Proche de 0, elle indique que les deux variables sont pratiquement indépendantes l'une de l'autre. Afin de faciliter la lecture, les valeurs obtenues sont systématiquement traduites en six niveaux d'intensité, présentés dans le tableau ci-dessous : négligeable, faible, modeste, modérée, forte et très forte. Ce sont ces qualificatifs qui apparaissent tout au long du rapport pour caractériser l'ampleur des évolutions et des différences documentées.

Force des relations statistiques (η^2)
Négligeable : $\eta^2 < 0{,}05$
Faible : $0{,}05 \leq \eta^2 < 0{,}10$
Modeste : $0{,}10 \leq \eta^2 < 0{,}20$
Modérée : $0{,}20 \leq \eta^2 < 0{,}30$
Forte : $0{,}30 \leq \eta^2 < 0{,}45$

CHAPITRE 1. ÉVOLUTION DE LA POSTURE DE CYBERSÉCURITÉ DES ENTREPRISES QUÉBÉCOISES ENTRE 2021 ET 2023

Entre 2021 et 2023, les entreprises québécoises ont évolué dans un environnement numérique doublement reconfiguré par l'intensification des menaces à visée financière, d'une part, et par la mise en œuvre progressive de la Loi 25, d'autre part. Ce double contexte de menaces qui s'intensifient et d'un cadre légal qui se raffermit constitue le prisme au travers duquel on doit lire les données présentées dans les sections suivantes. Les changements documentés au Québec entre les deux vagues de l'ECCC de Statistique Canada doivent en effet distinguer ce qui relève d'une adaptation réactive aux menaces mondiales de ce qui traduit une mise en conformité réglementaire sous la pression d'exigences locales, ces deux logiques opérant simultanément.

Portrait des cyberattaques subies

La proportion d'entreprises québécoises victimes d'au moins un cyberincident au cours de l'année est restée remarquablement stable entre 2021 et 2023, passant de 16,4 % à 15,5 %, ce qui suggère un certain équilibre entre l'expansion des menaces et la montée en maturité progressive des défenses organisationnelles. Cette stabilité de surface dissimule cependant une transformation profonde des types d'incidents auxquels sont exposées les entreprises. Le changement le plus marqué est l'explosion des attaques à finalité financière: la proportion d'entreprises victimes ciblées pour un vol d'argent ou le paiement d'une rançon est passée de 19,8 % en 2021 à 39,9 % en 2023, soit une hausse de 20,1 points, représentant l'augmentation la plus forte documentée parmi les menaces recensées. Les cybercriminels monétisent donc leurs attaques avec une intensité croissante. À l'inverse, les intrusions informatiques dans les zones d'accès non autorisé ou privilégié reculent significativement, faisant passer les entreprises victimes de 22,6 % à 11,2 %. Cette réduction reflète vraisemblablement les progrès accomplis en matière de gestion des accès et des identités, ces mesures ayant connu la hausse la plus marquée dans l'éventail des mesures techniques adoptées par les entreprises entre les deux vagues de l'enquête. On notera également une légère diminution des incidents visant à voler des renseignements personnels ou financiers (-2,3 points, de 27,5% à 25,2%). Si cet écart reste statistiquement modeste, il n'en est pas moins cohérent avec les effets attendus de la Loi 25 sur la prévention de ce type de violation, contre lequel les entreprises avaient désormais une raison légale de déployer des mesures de protection plus agressives. Les autres différences présentées dans le Tableau 1 ci-dessous sont négligeables et peuvent être attribuées à la pondération de l'échantillon.

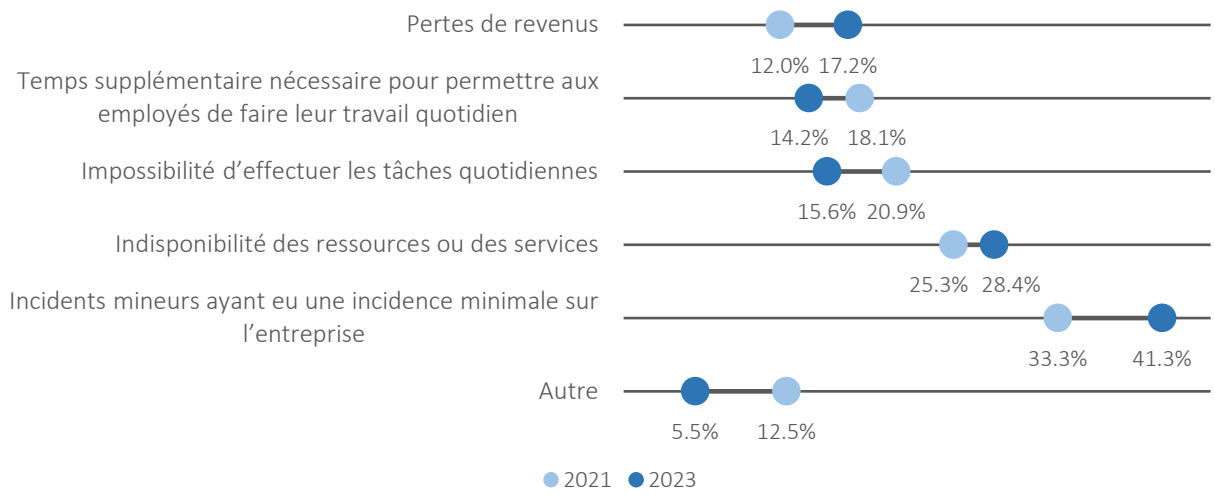
Tableau 1 : Évolution des types d'incidents de cybersécurité ayant touché les entreprises québécoises entre 2021 et 2023

Augmentation	Diminution
• Voler de l'argent ou demander une rançon (+20,1 points)	• Accéder à des zones d'accès non autorisé ou privilégié (-11,4 points)

• Perturber ou défigurer la présence Web (+2,1 points)	• Autres (-3,3 points) • Voler des renseignements personnels ou financiers (-2,3 points) • Sans motif connu (-1.8 points)

Les conséquences subies par les entreprises victimes de cyberattaques présentées à la Figure 2 dessinent un tableau contrasté entre 2021 et 2023. Deux types de perturbations opérationnelles régressent de façon notable: la proportion d'entreprises contraintes de consacrer du temps supplémentaire pour permettre à leurs employés d'accomplir leurs tâches quotidiennes diminue de 18,1 % à 14,2 %, et celle des entreprises confrontées à une impossibilité pour leurs employés d'effectuer ces tâches recule de 20,9 % à 15,6 %. Ces baisses impliquent que les entreprises québécoises absorbent plus efficacement les incidents sur le plan opérationnel. De plus, lorsque les entreprises ont dû faire face à des problèmes au niveau de la disponibilité de leurs ressources ou de leurs services, le temps d'arrêt de leurs activités était, en moyenne, significativement plus court en 2023 qu'en 2021. Par ailleurs, les pertes de revenus progressent de 12,0 % à 17,2 %, et les incidents qualifiés de mineurs avec une incidence minimale sur l'entreprise augmentent de 33,3 % à 41,3 %. La stabilité de l'indisponibilité des ressources (25,3 % à 28,4 %, différence statistiquement négligeable), de la perte de fournisseurs ou de clients, et des atteintes à la réputation complète ce portrait. Les cyberattaques de 2023 pèsent davantage sur les finances que sur les relations et les opérations, ce qui peut être interprété comme un signe de cyber-résilience accrue des entreprises québécoises.

Figure 2 : Conséquences des incidents de cybersécurité sur l'entreprise



Cette stabilité des effets post-incidents s'accompagne toutefois d'une réalité économique préoccupante. Si la proportion d'entreprises qui ont dû assumer des frais de rétablissement ne diffère pas significativement entre les deux vagues, les coûts de celles qui ont été exposées ont plus que doublé en

moyenne. De manière agrégée, les coûts totaux de rétablissement au Québec passent de 122,5 millions de dollars en 2021 à 315 millions en 2023, soit une multiplication par 2,5 en deux ans. Cette tendance n'est pas spécifiquement québécoise: à l'échelle canadienne, les coûts totaux progressent de 600 millions à 1,2 milliard de dollars sur la même période, confirmant que la monétisation croissante des cybermenaces constitue une dynamique structurelle. La Loi 25 a pu également contribuer à ce gonflement des coûts post-incident: la notification obligatoire aux personnes concernées et à la Commission d'accès à l'information (CAI), la mobilisation de services juridiques, et les mesures d'atténuation imposées par le cadre réglementaire alourdissent les coûts de rétablissement. La mesure précise de cet effet reste difficile à isoler dans les données disponibles, mais il serait imprudent d'en ignorer l'éventualité.

Tableau 2 : Évolution des coûts agrégés de rétablissement post-incident encourus par les entreprises québécoises et canadiennes entre 2021 et 2023

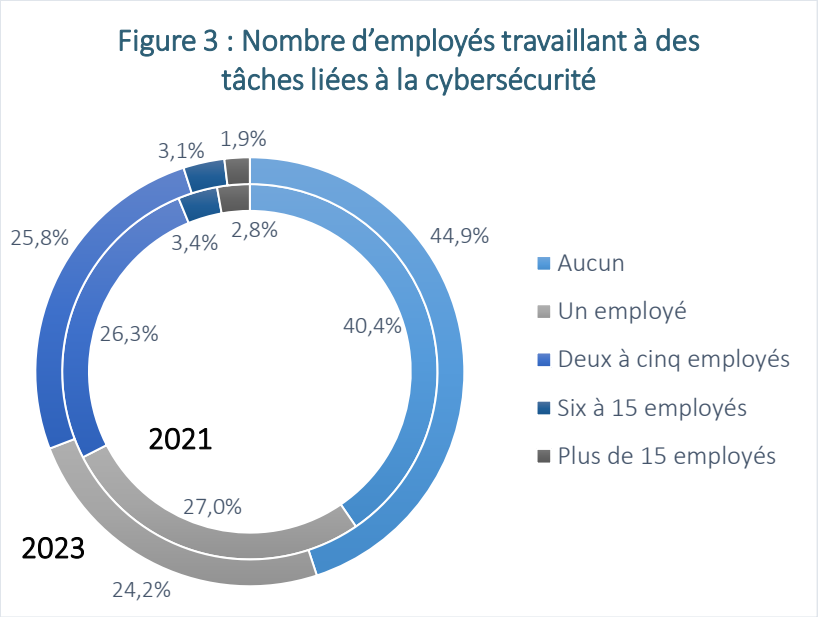
	2021	2023
Canada	600 M$	1,2 Mds$
Québec	122,5 M$	315 M$

Panorama de l'évolution des pratiques de cybersécurité

Alors que la section précédente documente l'évolution de l'exposition des entreprises québécoises aux cybermenaces, celle-ci s'intéresse à l'autre versant de l'équation : la façon dont ces organisations ont fait évoluer leur posture défensive entre 2021 et 2023. L'enjeu est ici de distinguer ce qui relève d'une adaptation naturelle aux menaces, comme investir davantage parce que les incidents coûtent plus cher, de ce qui reflète une mise en conformité réglementaire impulsée par la Loi 25. Ces deux logiques ne s'excluent évidemment pas : elles coexistent et se renforcent mutuellement. Mais les analyser séparément conditionne l'interprétation que l'on peut faire de la pérennité des changements observés: une adaptation dictée par la conformité peut se stabiliser ou même régresser une fois les obligations satisfaites, alors qu'une transformation plus profonde de la culture organisationnelle s'inscrit dans la durée. Trois catégories principales de mesures sont examinées : la nature de l'expertise professionnelle disponible au sein de chaque organisation, la fréquence de déploiement des mesures de contrôle et des procédures de gestion des risques, ainsi que la nature des interactions avec les partenaires externes.

Expertise en cybersécurité disponible à l'interne

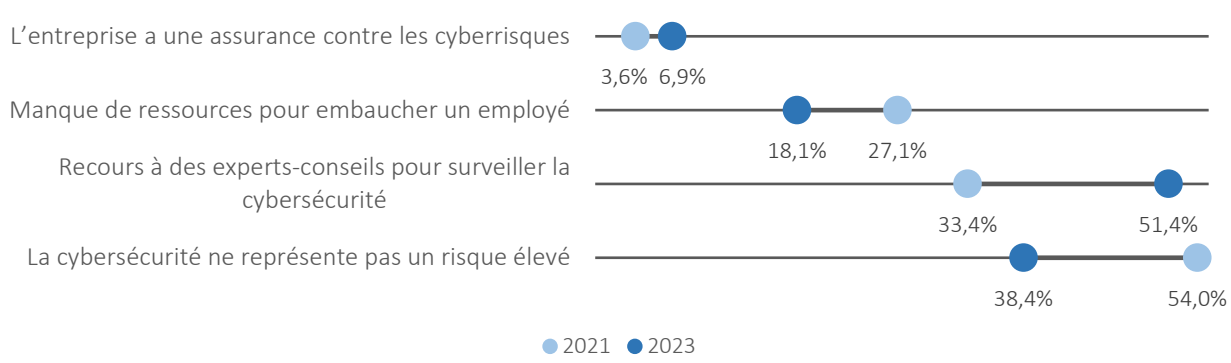
La structure des ressources humaines dédiées à la cybersécurité révèle une tension persistante entre une prise de conscience croissante des enjeux et une capacité organisationnelle qui tarde à se mettre à niveau. Le premier constat est à ce titre frappant : en 2023, un plus grand nombre d'entreprises québécoises (44,9 %, contre 40,4 % en 2021) déclare n'avoir aucun employé dédié à des tâches liées à la cybersécurité (figure 3). Cela signifie donc qu'une fraction importante de l'écosystème entrepreneurial québécois continue de faire face aux cybermenaces sans aucune ressource interne spécialisée.



Les entreprises dans cette situation justifient leur choix principalement de trois manières (figure 4). D'abord, plus du tiers d'entre elles estime que la cybersécurité ne constitue pas pour elles un risque suffisamment élevé pour justifier un tel investissement. Si cette perception semble déconnectée de la réalité statistique, il est encourageant de constater que cette posture insouciante a toutefois reculé de 15,6 points entre 2021 et 2023. En deuxième lieu, on observe une augmentation à peu près équivalente des entreprises qui justifient leur absence de recrutement interne par le recours à des prestataires externes de services-conseils en cybersécurité, ce qui constitue l'une des évolutions les plus substantielles de cette section. En troisième lieu, la proportion d'entreprises qui déclarent qu'elles manquent de ressources pour embaucher un employé reste élevée, à 18,1%. Toutefois, cette justification a diminué de neuf points en deux ans. La souscription d'une police d'assurance contre les cyberrisques demeure en dessous du seuil des 10%, même si elle augmente sensiblement de 6,3 points en deux ans, traduisant un effet d'aléa moral (*moral hazard*) par lequel les assurés altèrent leurs comportements face au risque lorsqu'ils se sentent couverts face aux pertes possibles.[5]

[5] Shavell, S. (1979), On moral hazard and insurance, In: Dionne, G., et Harrington, S.E. (dirs.), *Foundations of Insurance Economics*, Springer, Dordrecht, pp. 280-301.

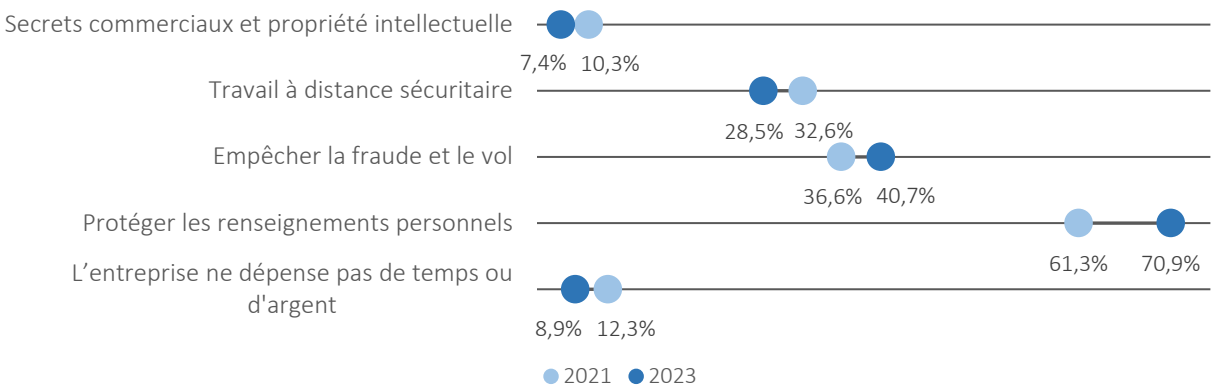
Figure 4 : Raisons de ne pas recruter d'employés specialisés en cybersécurité



Si le recrutement de spécialistes semble stagner, les efforts de formation à l'ensemble des employés progressent de 11,8 % en 2021 à 19,1 % en 2023. Si on ramène cette hausse de 7,3 points à la base de départ, elle représente une augmentation relative de 62 % du nombre d'entreprises ayant contribué à renforcer les compétences de l'ensemble de leur main d'œuvre face aux cyberrisques. Ce résultat découle probablement en partie des obligations introduites par la Loi 25, dont des dispositions exigent explicitement la mise en place et la documentation d'activités de formation et de sensibilisation du personnel à la protection des renseignements personnels.

Le lien entre exigence légale et comportement déclaré est encore plus lisible dans l'évolution des motivations invoquées pour justifier les dépenses en cybersécurité : la proportion d'entreprises citant la protection des renseignements personnels des employés, des fournisseurs, des clients ou des partenaires comme raison principale de leurs investissements passe de 61,3 % à 70,9 % entre les deux vagues (figure 5). Cette hausse de 9,6 points est l'un des indicateurs les plus directement imputables à la Loi 25 dans l'ensemble des résultats analysés : elle traduit la mise en place progressive des obligations légales en matière de protection de la vie privée dans les investissements de cybersécurité des organisations québécoises. La prudence interprétative reste toutefois de mise dans la mesure où aucune question ne portait spécifiquement sur la Loi 25 dans le questionnaire de Statistique Canada. Pour ce qui est de garantir un travail à distance sécuritaire; de protéger la réputation de l'entreprise; d'éviter les temps d'arrêt et les pannes informatiques; d'empêcher la fraude et le vol; ou de garantir la continuité des activités, les différences entre 2021 et 2023 sont négligeables. Les entreprises québécoises qui investissent en réaction à la suite d'un incident de cybersécurité ont aussi vu une augmentation négligeable en 2023.

Figure 5 : Principales raisons expliquant les dépenses en temps ou en argent pour la cybersécurité et la formation

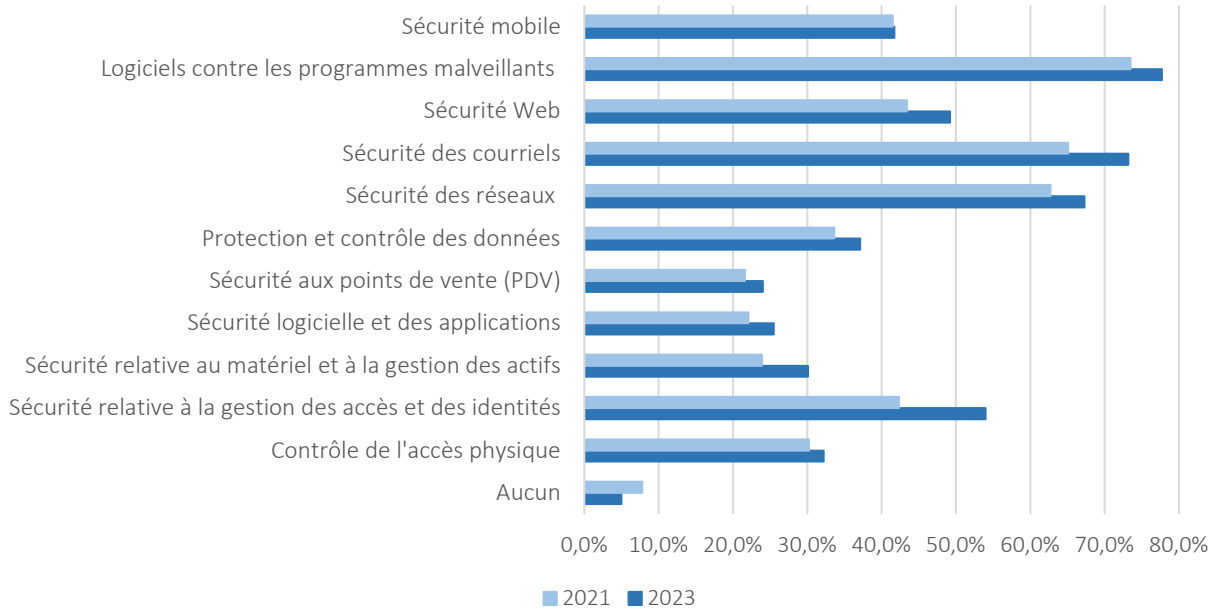


Mesures techniques et activités de gestion des risques

Les pratiques analysées dans cette section relèvent de deux logiques distinctes : les mesures techniques comme les pare-feux, les dispositifs de chiffrement, les technologies de gestion des identités et des accès, ou l'application de correctifs logiciels constituent la couche défensive déployée au niveau des systèmes et des réseaux. Elles opèrent de façon largement automatisée et forment le premier rempart contre les cyberattaques. Les activités de gestion des risques, qu'il s'agisse d'évaluations formelles, de politiques écrites, du degré d'implication de la haute direction, ou de l'élaboration des plans de continuité des activités et des plans de relève reflètent quant à elles une logique organisationnelle et décisionnelle. Elles ne protègent pas directement les systèmes, mais elles structurent le cadre dans lequel les décisions de sécurité sont prises, les responsabilités assignées et les ressources allouées.

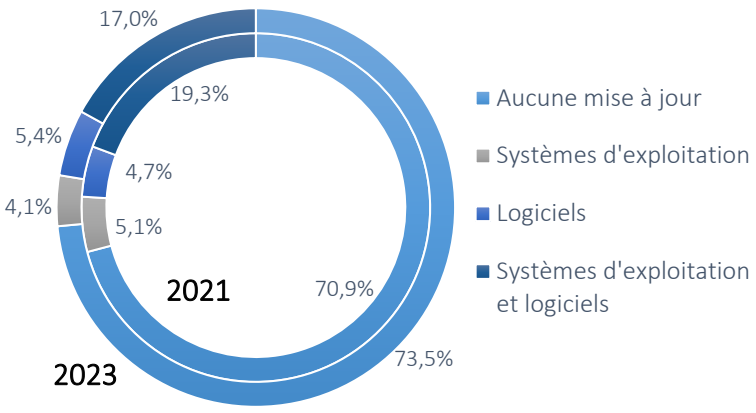
Si l'on se penche d'abord sur les mesures techniques de cybersécurité mises en œuvre (figure 6), le portrait révèle une stabilité entre 2021 et 2023, la quasi-totalité des différences observées étant statistiquement négligeables. Seule la gestion des identités et des accès enregistre une progression modeste, résultat qui semble cohérent avec la baisse documentée des incidents d'intrusion en zones non autorisées. Par conséquent, malgré l'intensification des menaces et le déplacement vers des attaques à finalité financière documentés plus haut, l'arsenal technique des entreprises québécoises est resté pratiquement inchangé sur la période de référence.

Figure 6 : Les mesures de cybersécurité actuellement en place dans les entreprises québécoises



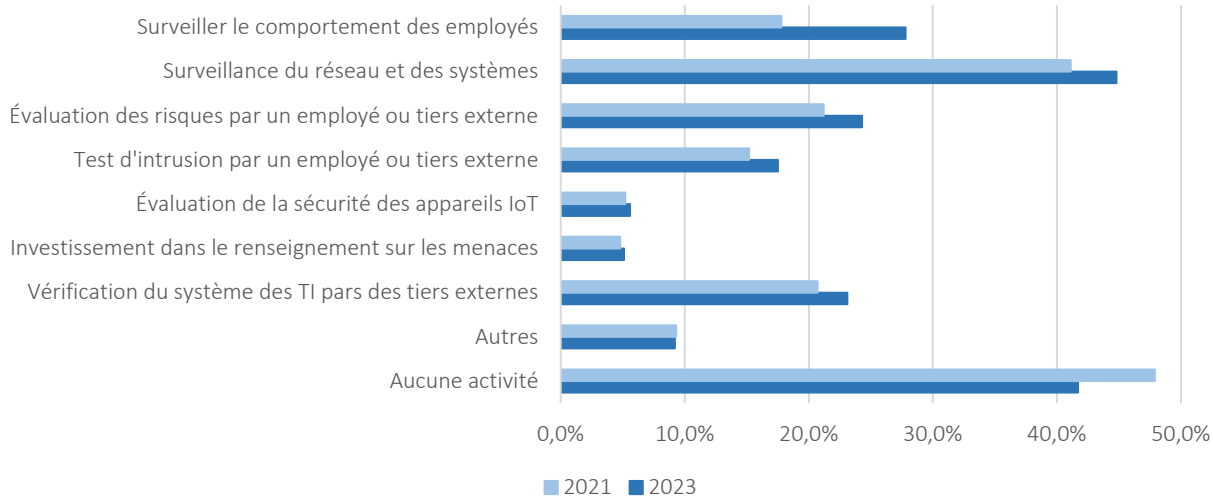
L'application de correctifs et de mises à jour de sécurité mensuelles constitue l'une des pratiques de cyber-résilience les plus élémentaires recommandées par toutes les autorités en cybersécurité. Le constat est pourtant sévère : plus de 73 % des entreprises québécoises déclarent n'appliquer aucun correctif ni aucune mise à jour de sécurité sur une base mensuelle, ce chiffre étant resté stable entre 2021 et 2023 (figure 7). Ni l'intensification des menaces, ni la mise en œuvre de la Loi 25, ni la professionnalisation observable sur d'autres dimensions de la gouvernance qui seront présentées plus loin n'ont permis d'améliorer ce résultat. C'est là l'une des vulnérabilités les plus tenaces dans la posture de cybersécurité des entreprises québécoises.

Figure 7 : Mise(s) à jour mensuelle(s)



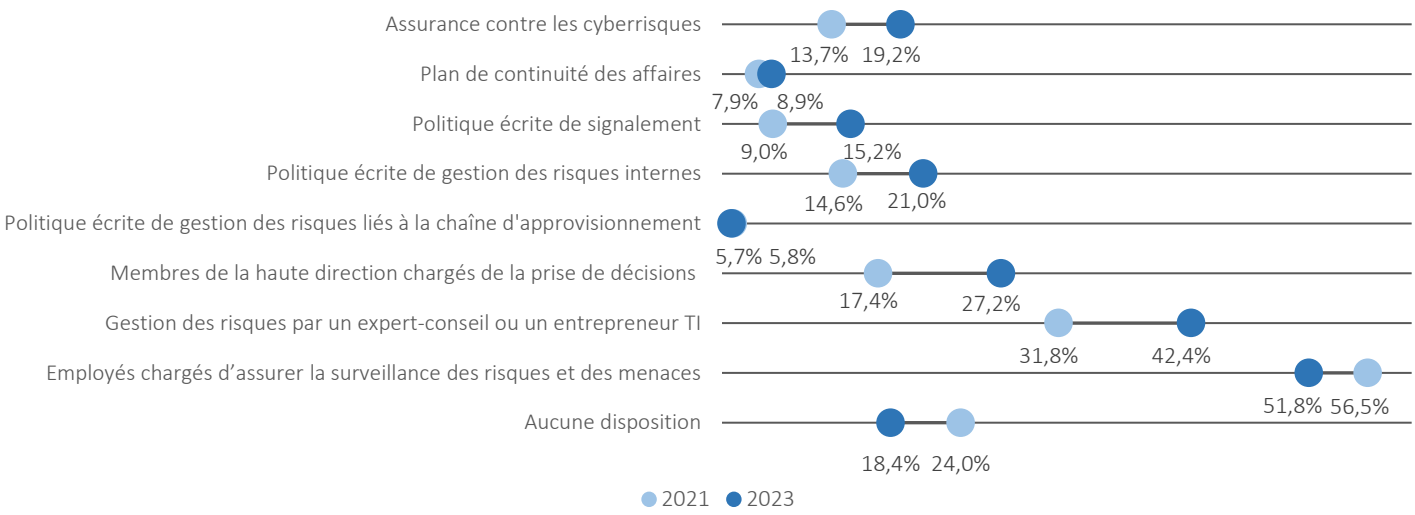
En ce qui concerne les activités menées pour identifier les risques de cybersécurité (figure 8), tous les types d'activités ont vu une augmentation en 2023. En revanche, cette augmentation est négligeable pour toutes les catégories, à l'exception de la surveillance du comportement des employés qui a connu une augmentation modérée (+10 points), probablement en raison d'une prise de conscience du risque associé à l'existence de menaces internes. Il est cependant inquiétant de constater qu'environ quatre entreprises québécoises sur dix ne mènent *aucune* activité pour identifier les risques auxquels leurs systèmes sont exposés. Ce chiffre, stable entre 2021 et 2023, est difficile à minimiser. Il signifie qu'une fraction substantielle du tissu entrepreneurial québécois opère au quotidien sans cartographie de ses vulnérabilités, dans un environnement où les coûts des incidents ont pourtant plus que doublé sur la même période.

Figure 8 : Les activités menées par l'entreprise pour identifier les risques à la cybersécurité



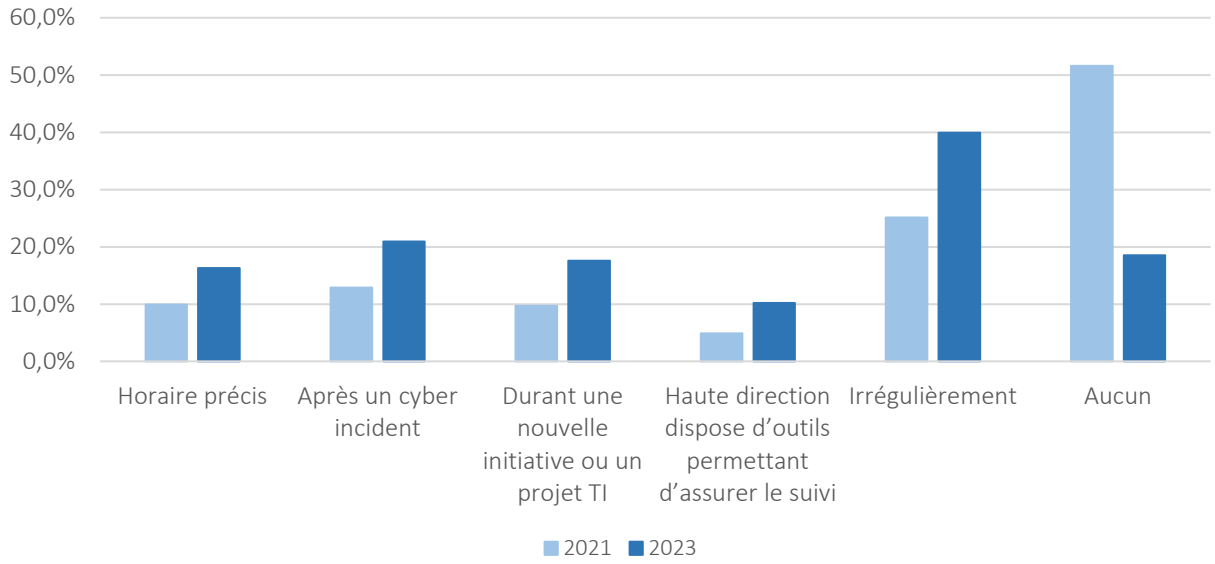
De manière plus encourageante, les dispositions formelles de gestion des risques ont progressé sur la majorité des dimensions mesurées par l'enquête (figure 9), ce qui semble traduire dans les faits les exigences de gouvernance introduites par la Loi 25, qui impose la mise en place de politiques écrites, de procédures de signalement interne et de mécanismes de surveillance. Les évolutions positives concernent notamment l'implication de la haute direction dans les décisions relatives aux risques cybernétiques (+9,8 points) et le recours à des experts-conseils externes (+10,6 points), deux dimensions qui seront analysées de manière plus approfondie dans les pages qui suivent. Il faut toutefois souligner deux points de fragilité persistants. D'une part, les plans de continuité des activités et la surveillance des risques internes demeurent stables ou reculent entre les deux vagues, ce qui génère des lacunes structurelles que les incitatifs de la Loi 25 n'ont pas suffi à combler. D'autre part, les politiques écrites de gestion des risques liés à la chaîne d'approvisionnement restent pratiquement inexistantes (5,8 % en 2021 et 5,7 % en 2023), ce qui constitue un angle mort alarmant à l'heure où les attaques indirectes via les fournisseurs et prestataires représentent un vecteur croissant de compromission des systèmes d'information.

Figure 9 : Dispositions de gestion des risques actuellement appliquées



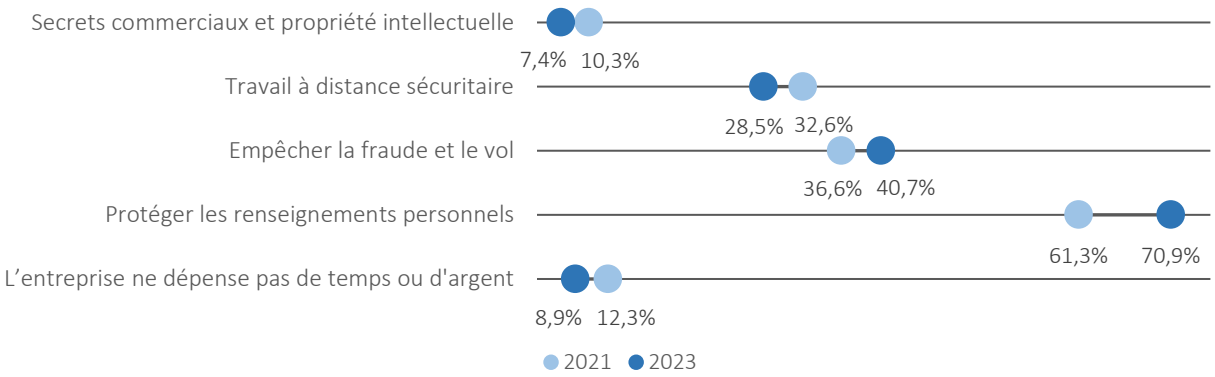
C'est dans l'implication accrue des instances dirigeantes dans la gouvernance de la cybersécurité que la transformation entre 2021 et 2023 est la plus spectaculaire et la plus significative statistiquement. La proportion d'entreprises québécoises dont la haute direction ne reçoit *aucune* mise à jour sur la cybersécurité chute de 51,6 % à 18,5 % entre les deux vagues : une réduction de 33 points qui constitue la relation la plus forte de l'ensemble de l'analyse (figure 10). En deux ans, le statut de la cybersécurité est passé de dossier technique délégué aux équipes TI à celui de préoccupation centrale relevant de la responsabilité des plus hautes instances décisionnelles des entreprises québécoises. Ce changement majeur n'est pas le fruit du hasard. La Loi 25 attribue explicitement la responsabilité de la protection des renseignements personnels à la personne ayant la plus haute autorité au sein de l'organisation, créant de ce fait une incitation institutionnelle puissante à faire remonter les informations relevant de la cybersécurité vers les instances dirigeantes.

Figure 10 : Fréquence à laquelle la haute direction reçoit des mises à jour sur la cybersécurité



Les effets de la Loi 25 ne se limitent pas à la structure de l'imputabilité en cybersécurité. Ils influencent également les motivations qui justifient les décisions d'investissement en cybersécurité. Si la loi a poussé les entreprises à rendre davantage de comptes à leur haute direction, elle a aussi renforcé le statut de la protection des renseignements personnels comme principale raison pour laquelle elles consentent à y consacrer du temps et de l'argent, loin devant la prévention de la fraude et du vol (figure 11).

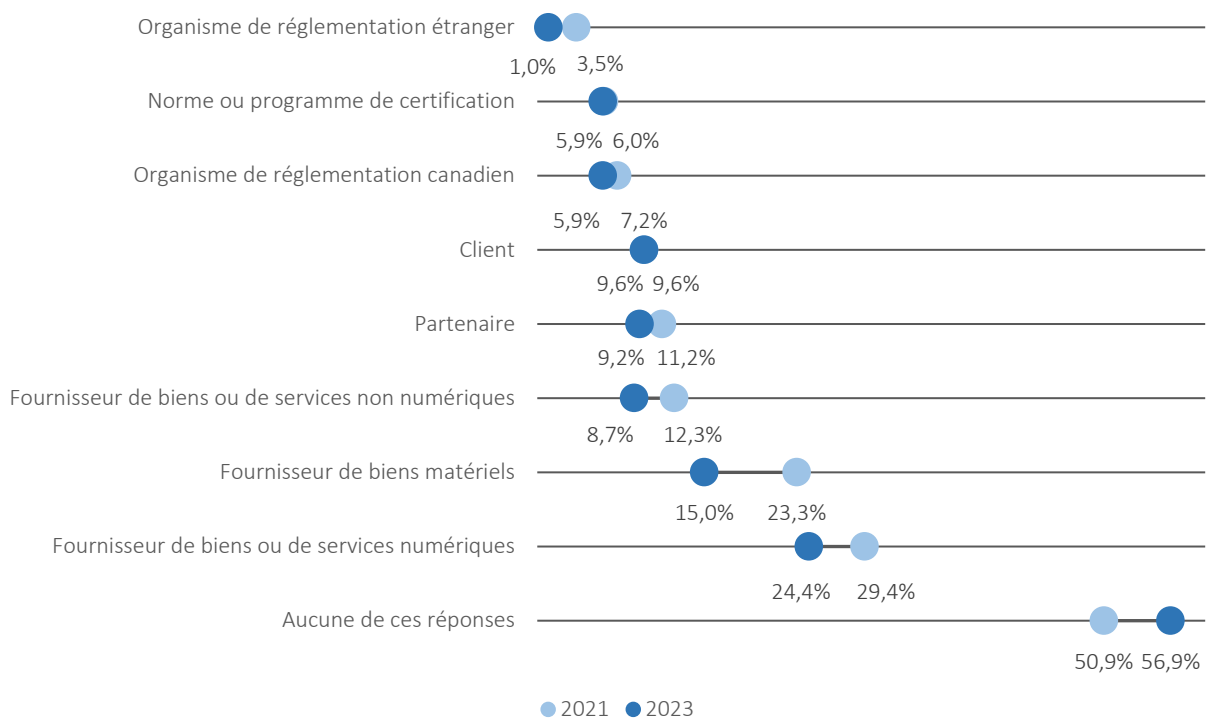
Figure 11 : Principales raisons expliquant les dépenses en temps ou en argent pour la cybersécurité et la formation



Les transformations documentées jusqu'ici en matière de renforcement du *reporting* à la haute direction et de l'évolution des motivations déclarées pour les dépenses en cybersécurité renvoient essentiellement à des dynamiques internes liées à la pression réglementaire de la Loi 25. Mais la posture de cybersécurité d'une entreprise ne se construit pas uniquement de l'intérieur. Fournisseurs, clients, organismes de

certification et autorités réglementaires constituent autant de vecteurs de pression externe susceptibles d'imposer ou d'encourager la mise en place de mesures et d'activités de gestion des risques que les organisations n'auraient pas nécessairement adoptées de leur propre initiative. C'est ce que documente la figure 12, qui révèle qu'il n'y a aucune différence entre 2021 et 2023 pour ce qui est des demandes faites par les clients (9,6% pour les deux vagues) et aucune différence significative au niveau des demandes faites par un organisme de réglementation canadien (6,0% en 2021 et 5,9% en 2023). Il n'y a que des différences statistiquement négligeables pour la mise en place des mesures exigées par les normes ou programmes de certification (7,2% en 2021 et 5,9% en 2023) et les partenaires (11,2% en 2021 et 9,2% en 2023). Pour les autres catégories de tiers externes, il y a eu une diminution faible ou modeste des demandes de mise en place de mesures de cybersécurité parmi les entreprises québécoises.

Figure 12 : Tiers externes, normes de cybersécurité ou programmes de certification ayant exigé la mise en place de mesures de cybersécurité



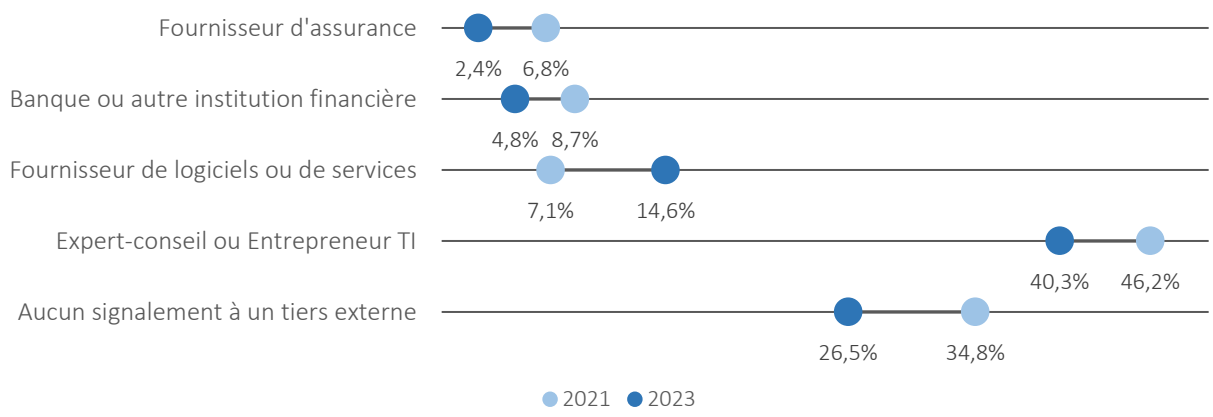
Ce léger recul des exigences formulées par les tiers externes peut s'interpréter de deux façons : soit les entreprises québécoises ont suffisamment amélioré leur posture pour que ces demandes deviennent redondantes, soit la conformité minimale attendue est désormais intégrée par toutes les organisations (notamment, suite à un renforcement de l'encadrement réglementaire) et ne nécessite plus d'être rappelée. La nature des données analysées ici ne permet malheureusement pas de trancher cette question.

Relations avec les partenaires externes et réponses aux cyberattaques

Les sections précédentes ont documenté une transformation substantielle de la posture de cybersécurité interne des entreprises québécoises entre 2021 et 2023 : gouvernance renforcée et motivations d'investissement recentrées sur la protection des données personnelles. Mais la cyber-résilience ne se construit pas uniquement en autarcie organisationnelle. Elle suppose également une capacité à mobiliser des ressources externes telles que les forces de l'ordre, les assureurs, les autorités réglementaires, les communautés de partage du renseignement, etc., et à contribuer par le signalement des incidents à renforcer la capacité collective de répondre aux cybermenaces. C'est précisément dans ce domaine que la Loi 25 était censée produire ses effets les plus structurants : en imposant aux organisations québécoises des obligations formelles de notification des atteintes à la vie privée à la Commission d'accès à l'information et aux personnes concernées, elle visait à réduire la tentation du règlement silencieux et à institutionnaliser une culture de transparence. Les résultats présentés dans cette section invitent à mesurer l'écart entre cette ambition législative et les comportements effectivement observés en 2023. Ils examinent successivement les comportements de consultation adoptés par les entreprises québécoises en réponse à des cyberattaques, les pratiques de signalement à des tiers externes et les raisons invoquées pour y renoncer. Ces résultats invitent à une lecture critique : là où les sections précédentes révélaient une maturité organisationnelle en progression, la section sur les relations avec les partenaires externes révèle une dynamique inverse, caractérisée par un repli mesuré mais constant vers la gestion interne et discrète des incidents, dont les implications pour la cyber-résilience méritent d'être prises au sérieux.

En premier lieu, pour les entreprises faisant face à une cyberattaque, la figure 13 sur le signalement aux tiers externes (hors police) indique un net repli. Les signalements aux fournisseurs d'assurance sont en déclin marqué, malgré une adoption croissante des polices d'assurance cyber sur la même période. Cet écart laisse penser que les entreprises compartimentent leur relation avec les assureurs, souscrivant une couverture sans nécessairement enclencher les procédures de déclaration, ce qui pourrait traduire une désillusion à l'égard de cet outil de gestion des risques ou un recours parcimonieux à ses bénéfices. Le signalement aux ministères et organismes de réglementation canadiens, quant à lui, demeure à des niveaux très bas. Ce résultat contraste avec les obligations de notification introduites par la Loi 25, mais ce résultat pourrait s'expliquer par la formulation de la question qui implique une portée nationale.

Figure 13 : Tiers externes auxquels l'entreprise a signalé un incident, excluant la police



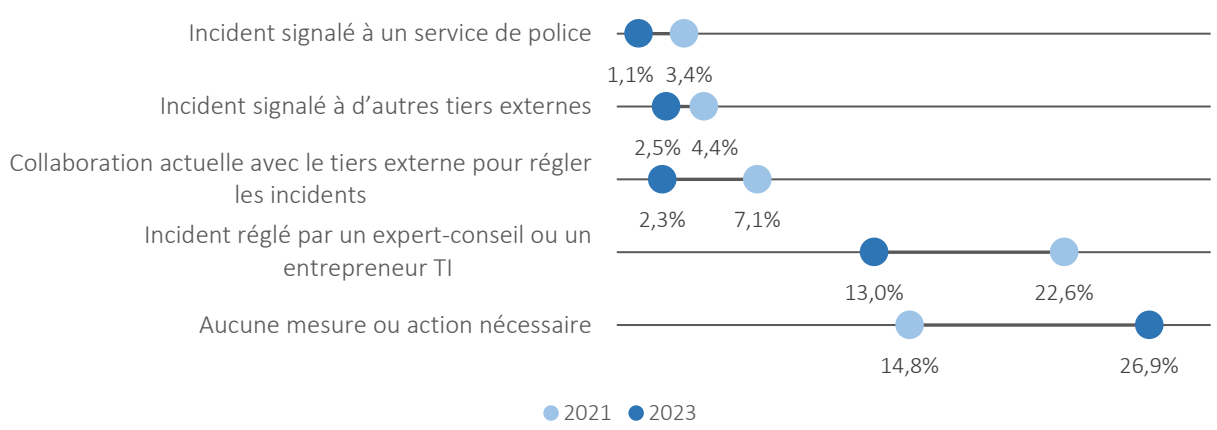
La dynamique de reflux des signalements aux partenaires externes est principalement attribuable à l'absence de volonté de consacrer davantage de temps ou d'argent à un incident mettant déjà les ressources de l'entreprise sous pression. Ce motif de non-signalement passe de 6,6 % en 2021 à 37,9 % en 2023 (tableau 3). Simultanément, la proportion d'entreprises estimant qu'il n'y a « aucun avantage ou obligation à signaler » progresse de 14,3 % à 22,4 % (+8,1 points). Ces deux indicateurs convergent vers un même constat : les entreprises québécoises se replient de façon accélérée sur le règlement interne des incidents, et considèrent de moins en moins le signalement externe à leurs partenaires comme une démarche utile ou obligatoire. Ce constat est d'autant moins rassurant qu'il semble aller à rebours des objectifs de la Loi 25, qui visait précisément à institutionnaliser les obligations de signalement (à la Commission d'accès à l'information notamment), et à réduire la tentation du règlement opaque. Les données de 2023 suggèrent qu'à mi-chemin du déploiement de la loi, cet effet normatif ne s'est pas encore matérialisé dans les comportements déclarés. Les entreprises absorbent les coûts croissants des incidents sans pour autant s'engager davantage dans des démarches de mutualisation des renseignements et de partage des leçons apprises.

Tableau 3 : Raisons de ne pas signaler certains ou tous les incidents à un tiers externe

Augmentation	Diminution
• Aucune volonté de consacrer plus de temps ou d'argent (+31,3 points) • Aucun avantage ou obligation à signaler (+8,1 points) • Incidents signalés à un service de police uniquement (+2,2 points) • N'y a pas pensé (+1,7 points)	• Incident mineur avec répercussion minimale (-34,5 points) • Protéger la réputation de l'entreprise (-1,8 points) • Manque de preuves (-0,9 points)

Au désengagement croissant dans le signalement de leurs propres incidents, s'ajoute un comportement similaire à l'égard des incidents signalés par des partenaires externes. La proportion d'entreprises ne prenant aucune disposition en réponse à un incident rapporté par un fournisseur ou un partenaire augmente de 14,8 % à 26,9 % entre 2021 et 2023 (figure 14). À l'inverse, les démarches de résolution collaborative avec des tiers externes et le recours à des experts-conseils diminuent modestement. Ce mouvement de repli est cohérent avec la hausse du non-signalement observée plus haut. Les entreprises québécoises semblent ainsi développer une posture de gestion interne et discrète des incidents, qu'il s'agisse des leurs ou de ceux qui leur sont signalés par des tiers. Ce faisant, elles affaiblissent les dynamiques de coopération et de partage de l'information qui constituent le fondement d'une cyber-résilience collective.[6]

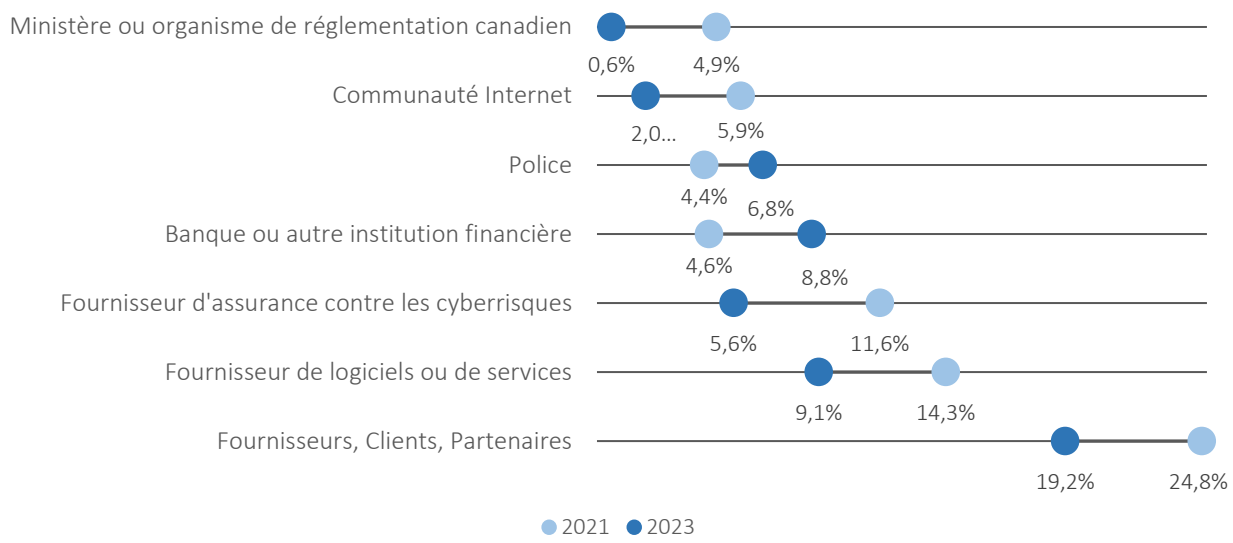
Figure 14 : Réponses de l'entreprise au(x) incident(s) signalés par des partenaires externes



Une fois l'incident détecté et en cours de résolution, les tendances de consultation des partenaires externes correspondent au déplacement des menaces documenté dans la première section (figure 15). La hausse des consultations de la police et des institutions financières (deux groupes de partenaires dont les entreprises sollicitent davantage l'assistance en 2023 qu'en 2021) reflète directement la montée en puissance des cyberattaques à visée financière : vol d'argent et rançongiciels appellent des interlocuteurs spécialisés dans le domaine économique et pénal. À l'inverse, le recours aux assureurs recule de façon notable, de 11,6 % à 5,6 %. Le résultat le plus troublant, cependant, est l'effondrement de la consultation des ministères et organismes de réglementation canadiens en réponse à un cyberincident : de 4,9 % en 2021 à 0,6 % en 2023, soit une diminution relative de 88 %. Dans un contexte où la Loi 25 visait précisément à accroître la transparence des organisations québécoises vis-à-vis des autorités de protection des données, ce recul constitue un paradoxe inquiétant.

[6] Dupont, B., Shearing, C., Bernier, M., et Leukfeldt, R. (2023), The tensions of cyber-resilience: From sensemaking to practice, *Computers & Security*, vol. 132, pp. 1-17.

Figure 15 : Tiers externes consultés pour obtenir des renseignements ou des conseils après un incident



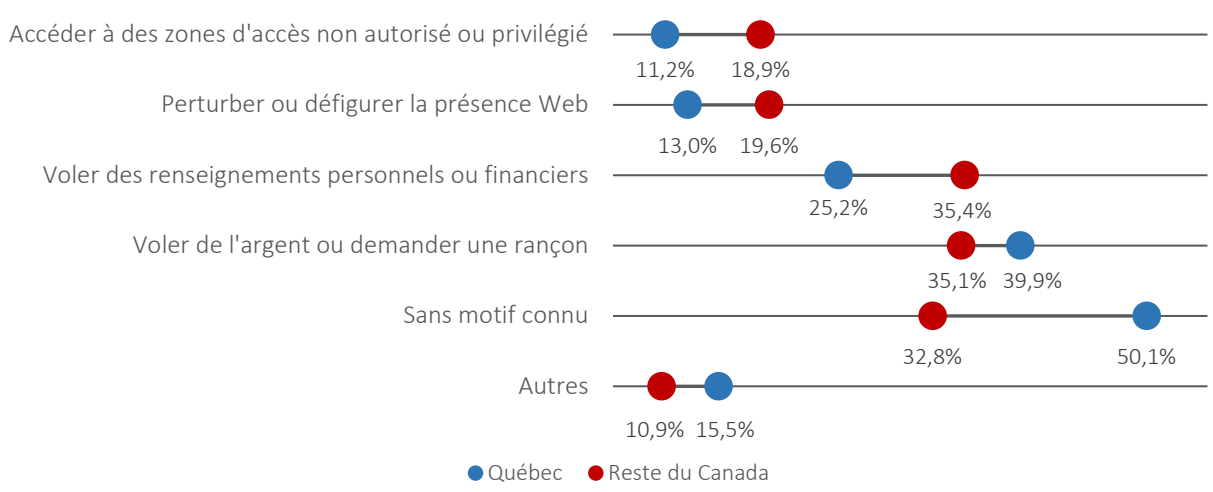
CHAPITRE 2. MISE EN PERSPECTIVE DE LA POSTURE DE CYBERSÉCURITÉ QUÉBÉCOISE DANS LE CONTEXTE CANADIEN

La comparaison des pratiques et des expériences des entreprises québécoises avec celles du reste du Canada pour la vague 2023 de l'enquête révèle un tableau nuancé : un taux de victimisation et des coûts de rétablissement globalement comparables à travers tout le pays, mais des profils d'incidents, des modes de gouvernance et des comportements de signalement qui divergent de façon mesurable. Ces écarts reflètent des réalités organisationnelles, culturelles et réglementaires distinctes, au premier rang desquelles figure la mise en œuvre de la Loi 25, dont les effets se font ressentir dans plusieurs dimensions de la posture de cybersécurité québécoise, parfois de façon attendue, d'autres fois de façon contre-intuitive.

Victimologie comparée

La différence d'exposition à des cyberattaques entre les entreprises québécoises et celles du reste du Canada est négligeable. En effet, 15,5% des entreprises québécoises ont été victimes d'un incident en 2023 contre 16,3% pour les entreprises du reste du Canada. La répartition des types d'incidents révèle néanmoins des profils de victimisation distincts entre le Québec et le reste du Canada (figure 16). Le résultat le plus frappant concerne les incidents « sans motif connu », déclarés par 50,1 % des entreprises québécoises victimes contre 32,8 % dans le reste du Canada. Cet écart de 17 points constitue la relation la plus forte de ce chapitre comparatif sur les incidents. Deux lectures non exclusives pourraient expliquer cette surreprésentation québécoise. La première est une explication par le déficit de capacités d'analyse internes : les entreprises québécoises disposeraient de moins d'outils ou d'expertise pour attribuer et caractériser les incidents qu'elles subissent. La seconde, plus structurelle, serait que les entreprises québécoises subiraient proportionnellement davantage d'attaques opportunistes ou peu sophistiquées, qui sont par définition moins faciles à classer dans une catégorie précise. Ces deux hypothèses devraient faire l'objet de recherches plus approfondies. À l'inverse, les entreprises du reste du Canada sont davantage ciblées par des incidents visant le vol de renseignements personnels ou financiers (35,4 % contre 25,2 % au Québec) et par des intrusions en zones d'accès non autorisé ou privilégié (18,9 % contre 11,2 %), des types d'attaques qui exigent généralement un niveau de sophistication supérieur et une connaissance préalable de l'architecture des systèmes ciblés. Pour finir, la proportion d'incidents visant à voler de l'argent ou demander une rançon est comparable entre les deux sous-échantillons et constitue l'une des formes d'incidents les plus fréquents.

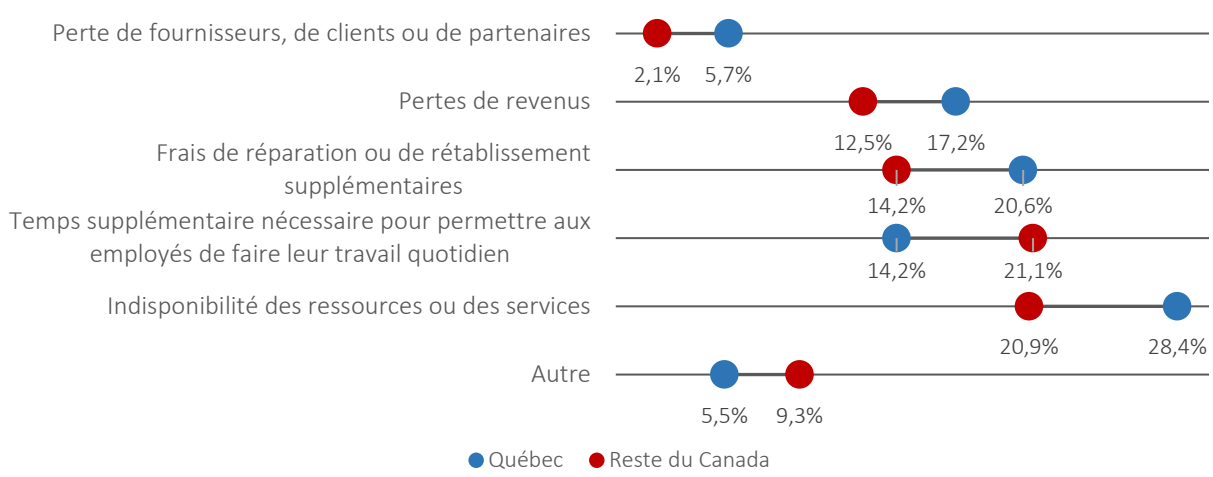
Figure 16 : Types d'incidents de cybersécurité ayant touché l'entreprise



En matière de coûts de rétablissement, la comparaison Québec/reste du Canada livre un résultat qui mérite notre attention : malgré des comportements de signalement distincts (les entreprises du reste du Canada étant proportionnellement plus nombreuses à ne contacter aucun tiers externe, tandis que les entreprises québécoises, lorsqu'elles renoncent au signalement, invoquent bien plus souvent le désir de garder l'incident en interne—8,4 % contre 1,8 %), les coûts totaux engagés pour se remettre des incidents de cybersécurité ne sont pas significativement différents entre les deux sous-groupes. Une proportion légèrement plus élevée d'entreprises québécoises déclare avoir eu des frais de rétablissement, mais le niveau moyen de ces coûts est comparable de part et d'autre. Ce résultat signifie que les stratégies différentes de gestion des incidents n'engendrent ni économies ni surcoûts mesurables. La dimension économique ne saurait donc suffire à justifier un changement de comportement vers un signalement plus systématique, et c'est plutôt l'argument collectif de la contribution au partage des renseignements sur les menaces qui doit être mobilisé. Pour ce qui est des autres conséquences, à l'exception des différences statistiquement faibles présentées dans la figure 17, elles s'avèrent soit non significatives soit statistiquement négligeables.[7]

[7] Non significatives : Atteinte à la réputation de l'entreprise et manipulation ou vol de données. Négligeables : Impossibilité pour les employés d'effectuer leurs tâches quotidiennes; incidents mineurs ayant eu une incidence minimale sur l'entreprise; vol ou atteinte à l'intégrité des logiciels ou du matériel et obligation d'informer les parties externes de toute atteinte à la sécurité.

Figure 17 : Conséquences des incidents de cybersécurité sur l'entreprise

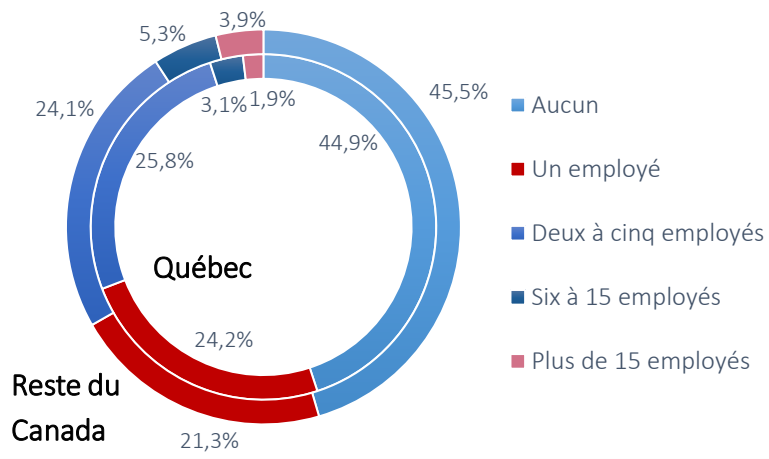


Mesures et pratiques de cybersécurité

Employés spécialisés en cybersécurité et recrutement

Les différences concernant le nombre d'employés travaillant en cybersécurité sont toutes négligeables. Comme on peut le remarquer dans la figure 18, près de la moitié des entreprises dans le reste du Canada indiquent n'avoir aucun employé dédié aux tâches liées à la cybersécurité, dans le prolongement de ce qui a été constaté au Québec dans la section précédente.

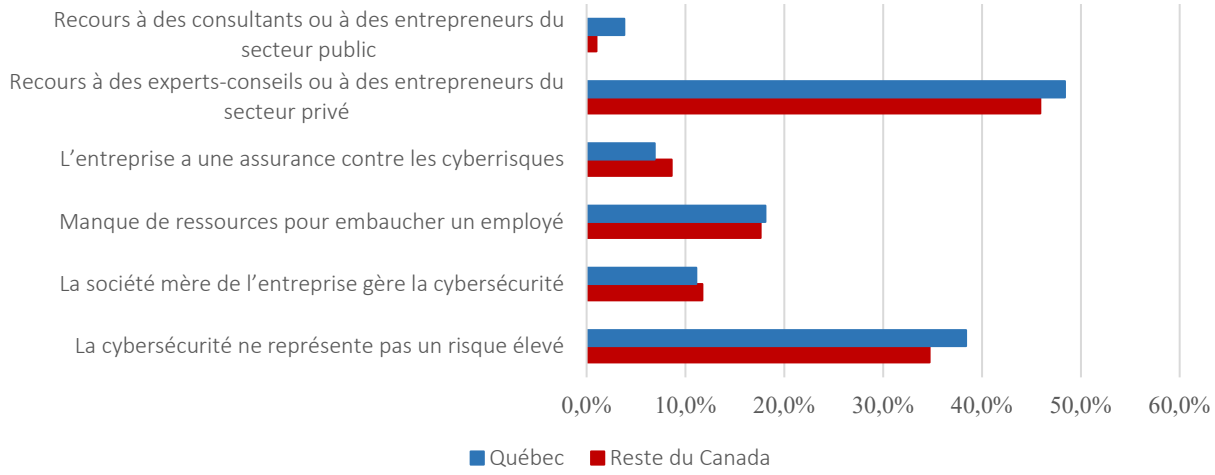
Figure 18 : Nombre d'employés travaillant à des tâches liées à la cybersécurité



prompt

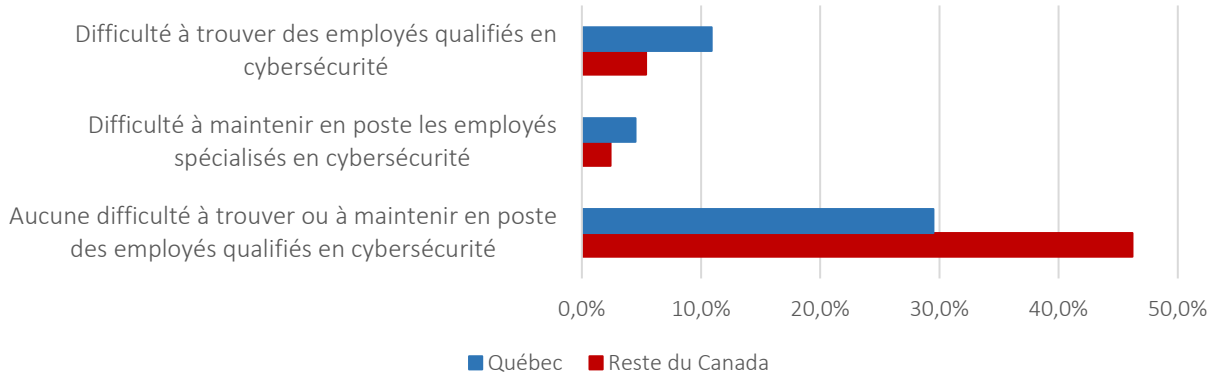
Les raisons offertes pour expliquer cette situation sont également similaires à travers tout le Canada (figure 19). Toutes les différences sont statistiquement négligeables à l'exception du recours à des consultants ou à des entrepreneurs du secteur public (qui est toutefois une pratique relativement peu répandue).

Figure 19 : Raisons de ne pas disposer d'employés specialisés en cybersécurité



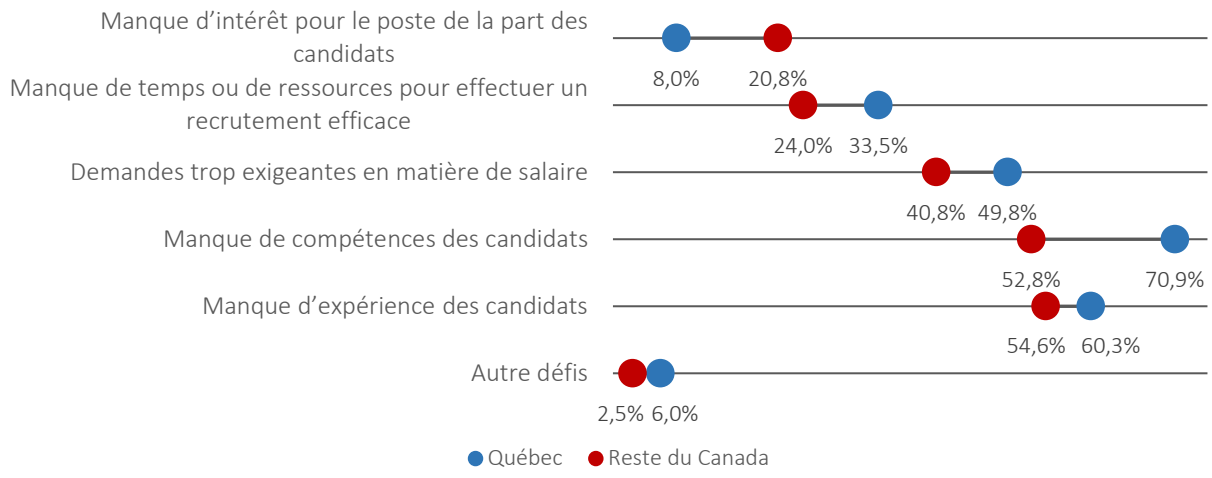
Les difficultés en matière de ressources humaines spécialisées constituent l'une des spécificités québécoises les plus prononcées de cette comparaison avec le reste du Canada (même si la force de la relation reste modeste). Alors que près de la moitié des entreprises du reste du Canada déclarent n'éprouver aucune difficulté à trouver ou maintenir en poste des employés qualifiés en cybersécurité, cette proportion n'atteint pas 30 % au Québec (29,5 %) (figure 20). Cet écart d'une vingtaine de points reflète un marché de l'emploi plus tendu dans la province. Ce déficit de main-d'œuvre qualifiée est cohérent avec la progression plus forte observée au Québec du recours aux experts-conseils et entrepreneurs externes pour la gestion des risques cybernétiques : face aux difficultés à recruter et à retenir les compétences en interne, les organisations québécoises se tournent davantage vers l'impartition. La Loi 25 amplifie vraisemblablement cette dynamique en imposant des exigences de gouvernance que les entreprises ne peuvent satisfaire sans expertise externe spécialisée.

Figure 20 : Difficultés rencontrées pour trouver ou maintenir en poste des employés spécialisés



La figure 21 révèle que le problème québécois n'est pas simplement quantitatif mais qualitativement distinct de celui du reste du Canada. Le manque de compétences des candidats est de loin le défi le plus fréquemment cité par les entreprises québécoises (70,9 % d'entre elles le nomment, contre 52,8 % dans le reste du Canada), avec un écart de 18 points qui constitue la différence la plus marquée sur cette question. Les exigences salariales jugées trop élevées (49,8 % contre 40,8 %) et le manque de temps ou de ressources pour effectuer un recrutement efficace (33,5 % contre 24,0 %) accentuent ce portrait d'un marché de l'emploi sous tension. À l'inverse, le manque d'intérêt des candidats pour le poste est bien moins fréquemment évoqué au Québec que dans le reste du Canada (8,0 % contre 20,8 %), ce qui pourrait signifier que les candidats québécois ne sont pas absents du marché, mais qu'ils n'y arrivent pas avec les compétences attendues par les employeurs.

Figure 21 : Défis rencontrés au moment d'embaucher des employés spécialisés en cybersécurité



prompt

Sensibilisation de l'ensemble des employés : le Québec en retrait

L'une des principales différences entre le Québec et le reste du Canada ne porte pas sur la victimisation ni sur les mesures techniques déployées, mais sur la diffusion interne de la culture de sécurité. En 2023, 58,4 % des entreprises canadiennes hors Québec déclarent avoir communiqué des pratiques exemplaires ou des renseignements généraux sur les cyberrisques à tous leurs employés, contre seulement 46,9 % des entreprises québécoises. Cet écart statistiquement significatif de 11,5 points implique que plus d'une entreprise québécoise sur deux ne diffuse pas encore cette sensibilisation de façon universelle à l'ensemble de son personnel.

Ce résultat est important à plusieurs égards. Il laisse d'abord penser que le Québec concentre peut-être davantage ses efforts sur les équipes techniques et les instances dirigeantes—ce qui serait cohérent avec la forte progression du *reporting* à la haute direction documentée dans la vague 2023, au détriment d'une culture de vigilance collective. Il contraste par ailleurs avec l'impression de relative préparation que les entreprises québécoises expriment : se sentir mieux préparé que les autres, tout en formant moins systématiquement son personnel, esquisse un décalage entre la perception et la pratique qui mérite d'être approfondi. Enfin, dans le contexte de la Loi 25, dont les obligations de formation et de sensibilisation visaient précisément à élargir la diffusion des bonnes pratiques au sein des organisations, cet écart souligne que la mise en conformité reste inégalement distribuée à l'intérieur même du tissu entrepreneurial québécois.

Fréquence et régularité des mises à jour à la haute direction : deux profils distincts

La comparaison des fréquences de mise à jour de la haute direction révèle deux approches de gouvernance fondamentalement différentes, dont la compréhension requiert de dépasser le simple constat de plus ou moins grande régularité (figures 22 et 23). Les entreprises du reste du Canada privilégient des rituels institutionnalisés : 32,5 % font des mises à jour mensuelles (contre 21,2 % au Québec) et 28,6 % des mises à jour trimestrielles (contre 13,7 % au Québec). Ces cadences planifiées s'inscrivent dans les routines organisationnelles. Les entreprises québécoises présentent un profil inverse : surreprésentation du *reporting* quotidien (13,5 % contre 4,9 %) et des horaires ad hoc ou « autre » (20,8 % contre 8,2 %). Ces résultats suggèrent une gouvernance davantage réactive : les dirigeants québécois sont plus fréquemment sollicités, mais selon des rythmes moins formalisés. La Loi 25 est sans doute un facteur explicatif de cette mobilisation accrue. En attribuant à la personne ayant la plus haute autorité la responsabilité de la protection des renseignements personnels, elle crée une demande de suivi soutenu de la part des dirigeants. Mais elle n'explique pas à elle seule l'irrégularité de ces mises à jour. Il serait certainement pertinent de se pencher sur ces variations des pratiques.

Figure 22 : Fréquence à laquelle la haute direction reçoit des mises à jour sur la cybersécurité

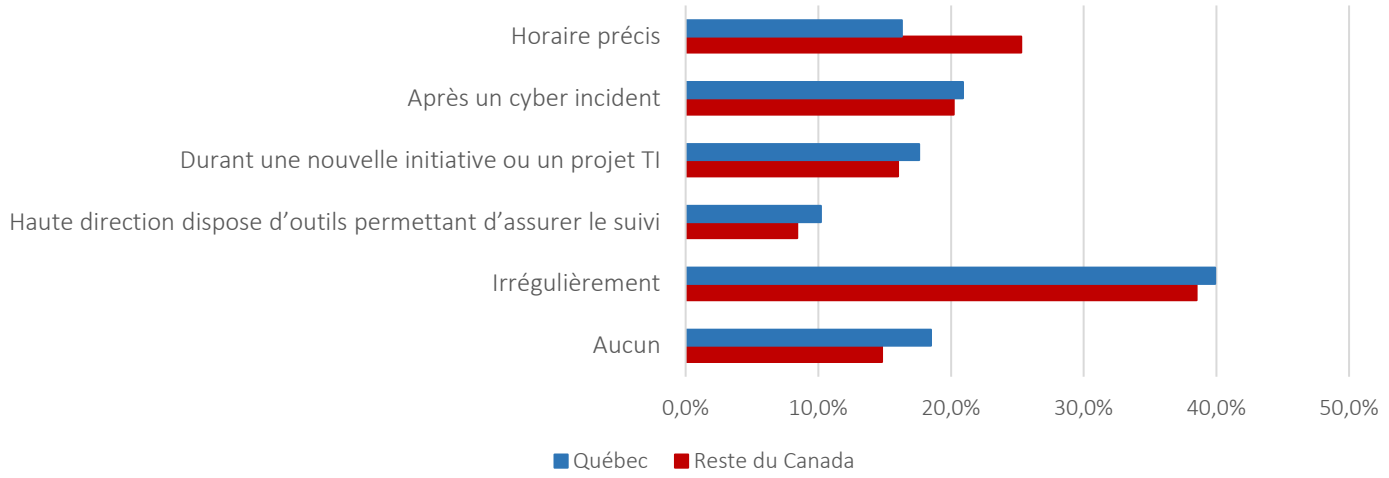
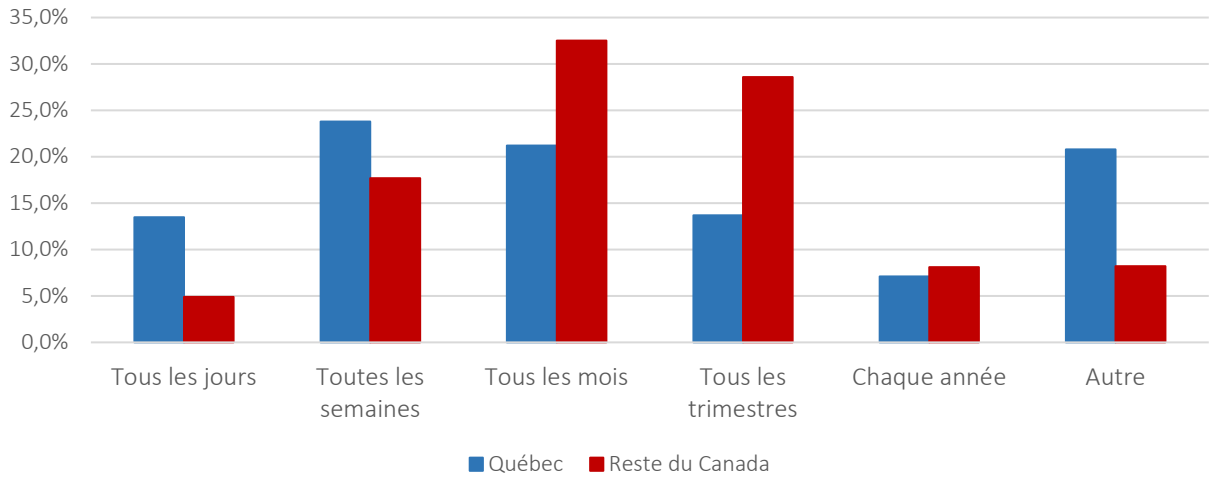


Figure 23 : Détails de la catégorie "Horaire précis"



Auto-évaluation du niveau de préparation et risque de sur-confiance

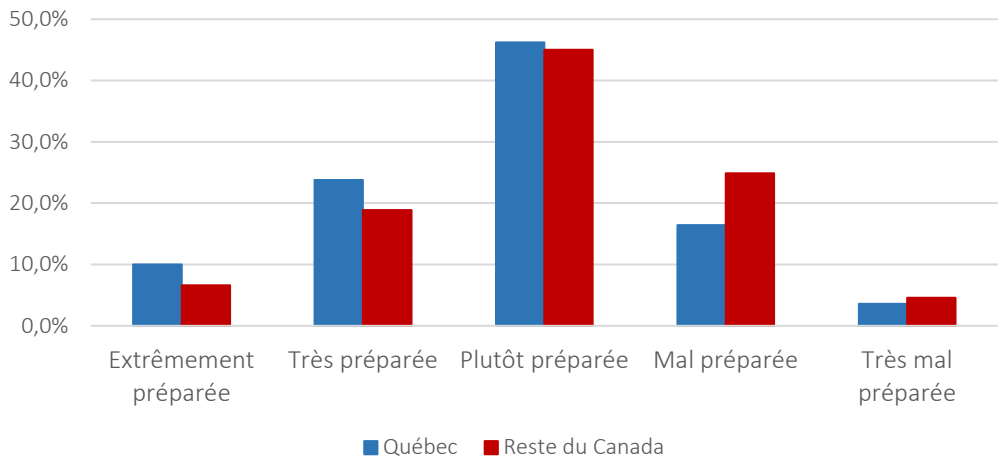
La figure 24 invite à confronter la perception que les entreprises québécoises ont de leur propre préparation avec les indicateurs objectifs de pratiques documentés précédemment dans ce rapport. Les entreprises québécoises se déclarent en effet mieux préparées pour faire face aux cybermenaces que leurs homologues du reste du Canada.

Pourtant, aucun des indicateurs de pratiques examinés dans cette section ne corrobore cette confiance : les entreprises québécoises communiquent moins largement les pratiques de sécurité à l'ensemble de leurs employés, ont plus de difficultés à recruter des employés spécialisés en cybersécurité, et déploient

des mesures techniques et des pratiques de gestion des risques relativement similaires à celles du reste du pays, sans avantage mesurable. L'implication de la haute direction semble bien plus intensive, mais il est peu probable que celle-ci affecte de manière notable les capacités opérationnelles de détection et de réponse aux incidents dans le contexte général examiné ici.

Cette dissociation entre la confiance déclarée et les pratiques observées est un phénomène bien documenté dans la littérature sur la culture de sécurité organisationnelle qui n'est pas sans conséquences : une organisation qui surestime sa préparation est moins susceptible d'investir dans les dimensions où elle est réellement vulnérable, et moins réactive face aux signaux d'alerte qui précèdent les incidents.[8] Le paradoxe québécois de la préparation perçue constitue en ce sens l'un des résultats les plus préoccupants de ce portrait comparatif.

Figure 24 : Auto-évaluation du niveau de préparation face aux cybermenaces



Gestion des risques et mesures internes

Sur l'ensemble des autres dimensions examinées dans cette section (mesures techniques déployées au niveau des systèmes et des réseaux—figure 25, activités d'identification et pratiques de gestion des risques—figures 26 et 27), les entreprises québécoises et celles du reste du Canada présentent des profils largement convergents. Quelques écarts ponctuels subsistent, notamment dans les motivations déclarées pour les dépenses en cybersécurité, où la protection des renseignements personnels et la lutte contre la fraude sont plus souvent citées au Québec (figure 28), probablement du fait des obligations de la Loi 25, ainsi que dans certaines mesures techniques où le Québec se situe légèrement en deçà du reste du pays. Toutefois, ces différences restent d'intensité faible et ne traduisent pas de divergences structurelles comparables à celles documentées dans les sous-sections précédentes. Cette convergence est en soi informative : elle indique que les spécificités québécoises identifiées dans ce rapport comme le retard sur

[8] Dupont, B. (2019), The cyber-resilience of financial institutions: Significance and applicability, *Journal of Cybersecurity*, vol. 5, no. 1, pp. 1-17.

la sensibilisation universelle du personnel, la gouvernance réactive, ou les difficultés de recrutement plus prononcées ne reflètent pas un écart généralisé sur l'ensemble des pratiques, mais constituent des points de fragilité ciblés dans une posture qui, sur la majorité des dimensions mesurables, s'aligne sur celle du reste du Canada.

Figure 25 : Les mesures de cybersécurité actuellement en place dans l'entreprise

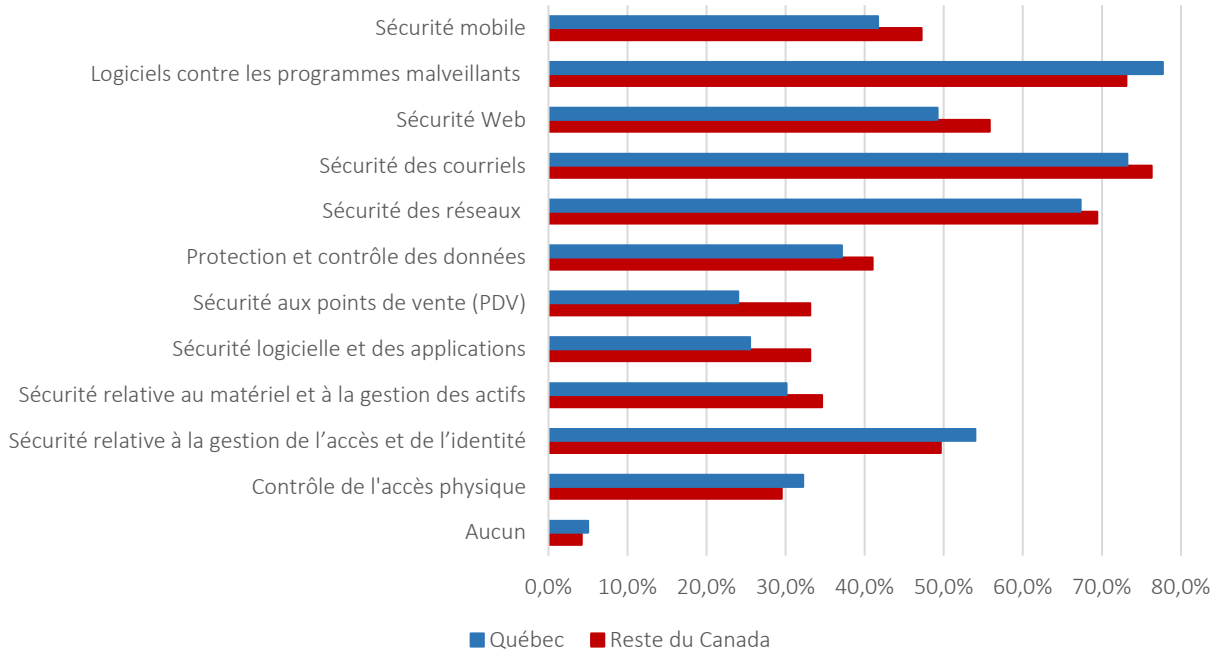


Figure 26 : Les activités menées par l'entreprise pour identifier les risques à la cybersécurité

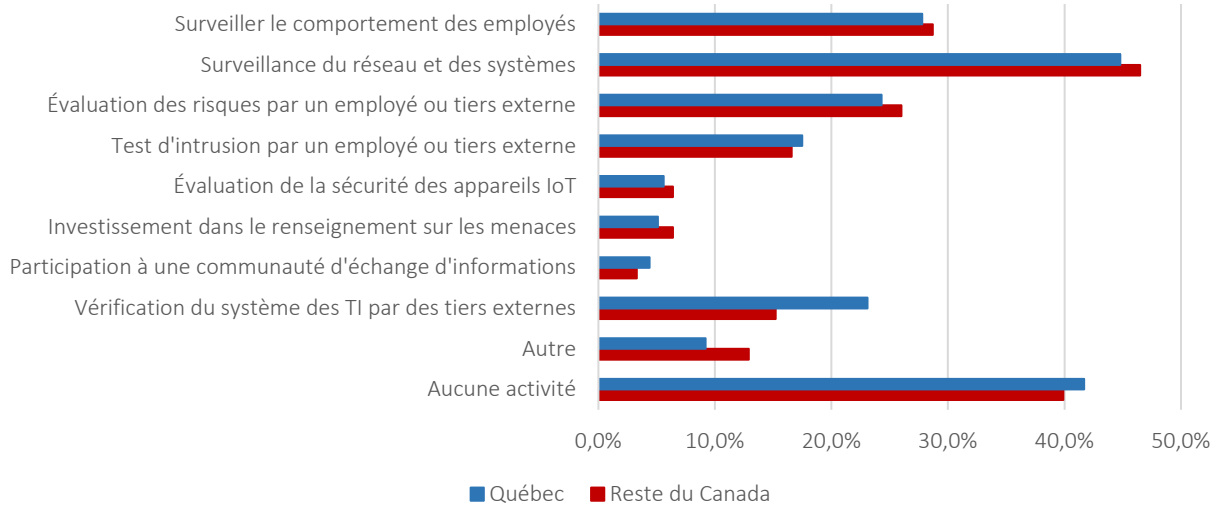


Figure 27 : Dispositions de gestion des risques actuellement appliquées

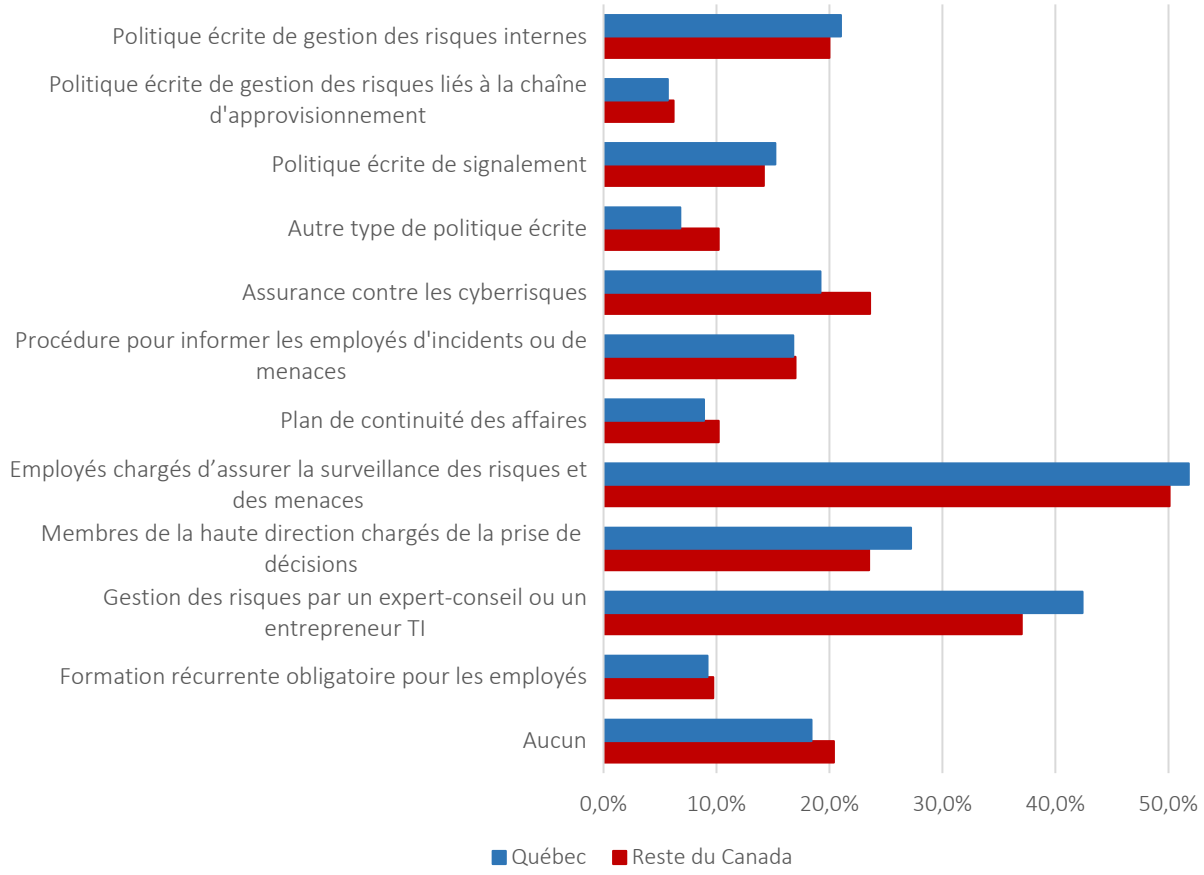
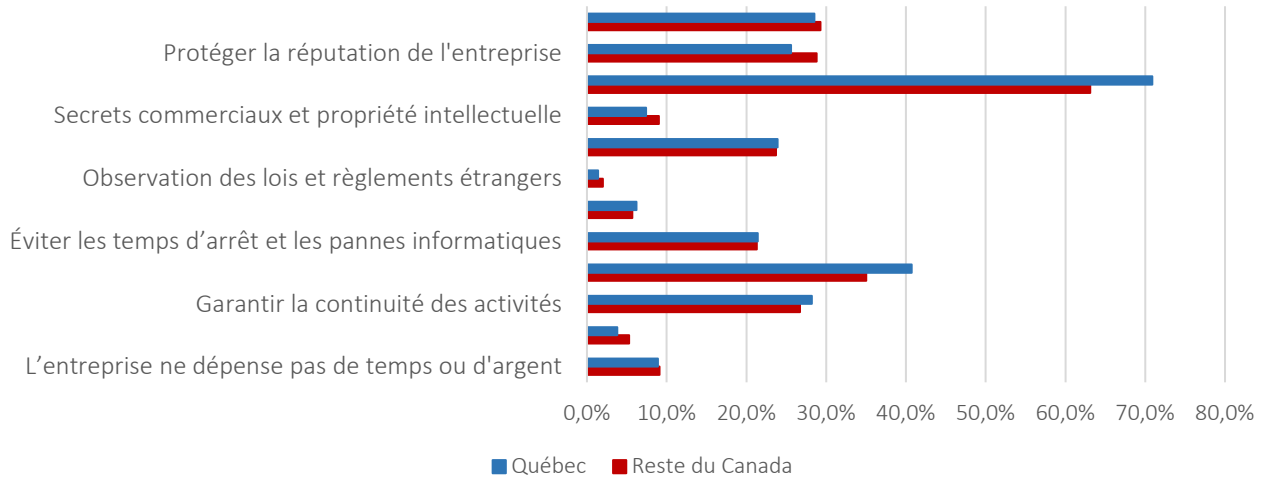


Figure 28 : Principales raisons expliquant les dépenses en temps ou en argent pour la cybersécurité et la formation



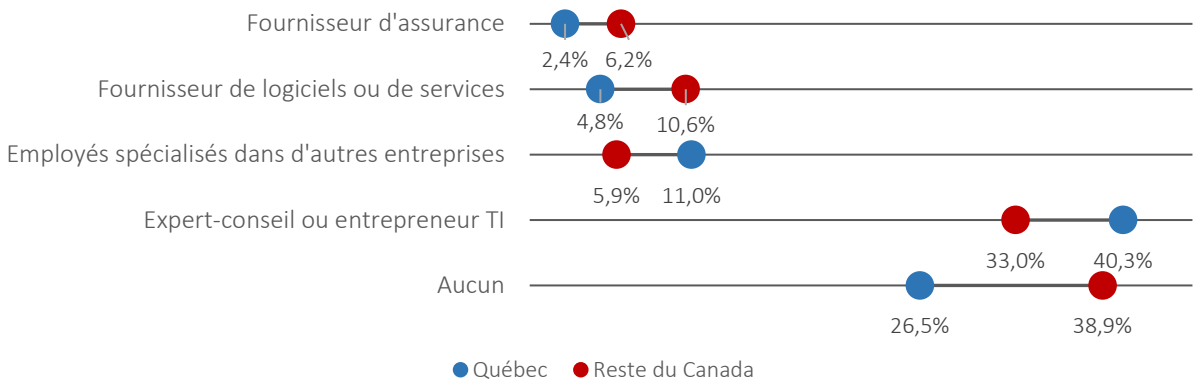
prompt

Collaboration et pratiques partenariales

La comparaison des pratiques de collaboration afin de gérer les répercussions d'une cyberattaque révèle un contraste québécois face au reste du Canada.

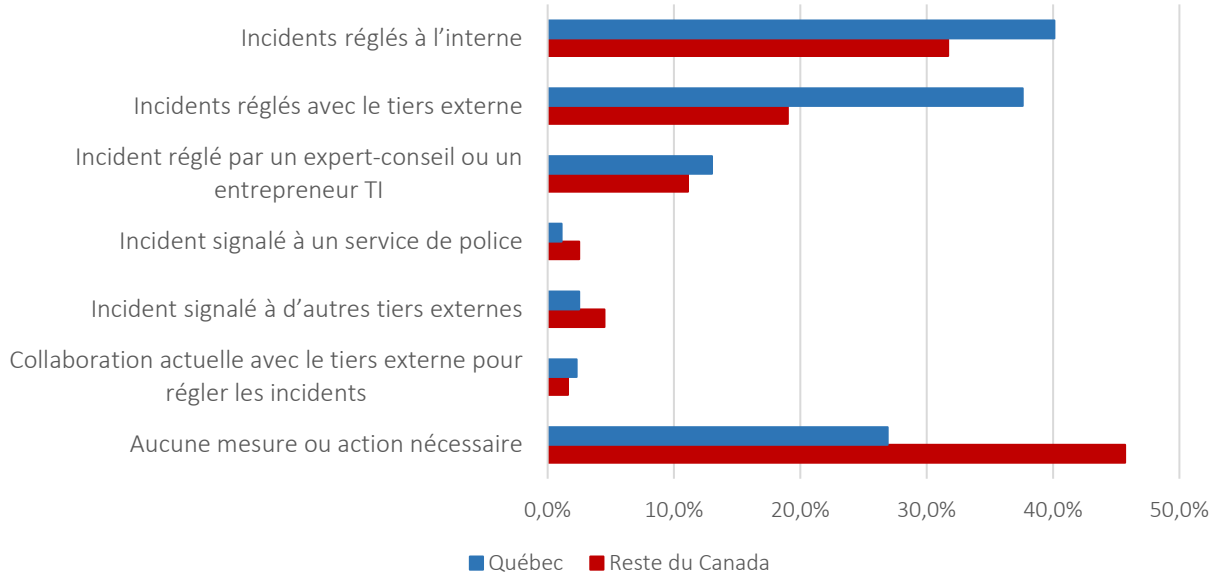
Lorsque les entreprises québécoises sont frappées par une cyberattaque, elles sont proportionnellement plus nombreuses que leurs homologues canadiennes à signaler l'incident à au moins un partenaire externe hors police (26,5 % d'entre elles ne contactent personne, contre 38,9 % dans le reste du Canada) (figure 29). La nature de ce signalement est par ailleurs ciblée : les entreprises québécoises se tournent prioritairement vers leurs experts-conseils ou entrepreneurs TI (40,3 % contre 33,0 %) et vers des employés spécialisés d'autres entreprises (11,0 % contre 5,9 %), tandis que le reste du Canada recourt davantage aux fournisseurs de logiciels ou de services (10,6 % contre 4,8 %) et aux fournisseurs d'assurance (6,2 % contre 2,4 %).

Figure 29 : Tiers externes auxquels l'entreprise a signalé un incident, excluant la police



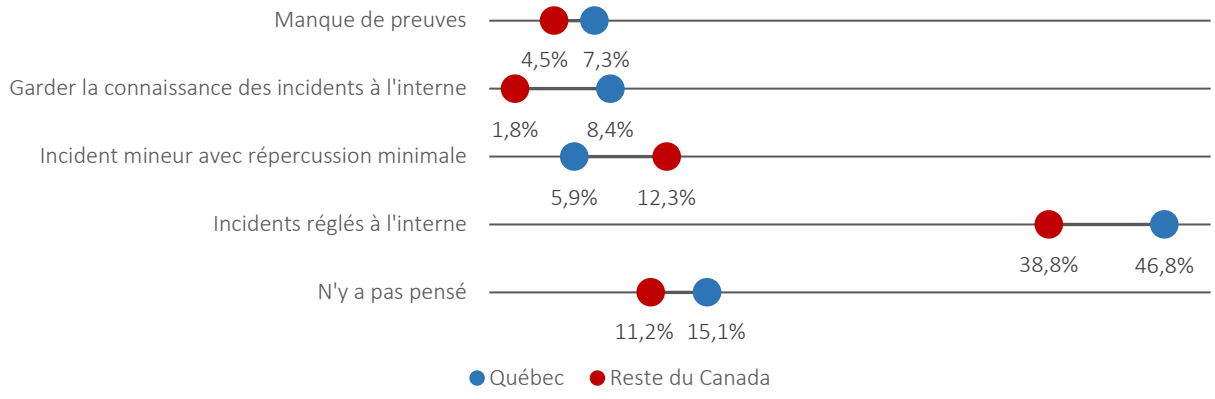
Pour ce qui concerne la réaction des entreprises face aux incidents signalés par des partenaires externes, les entreprises québécoises sont, de la même manière, nettement plus enclines à engager une démarche de résolution collaborative avec le partenaire concerné (figure 30) : 37,6 % contre 19,0 % dans le reste du Canada. De plus, les entreprises canadiennes hors Québec sont presque deux fois plus nombreuses à ne prendre aucune mesure en réponse à ces signalements (45,7 % contre 26,9 %). Le Québec se distingue donc par un engagement partenarial plus élevé en cas de cyber-crise, mais qui semble s'exercer dans un espace bilatéral et privé plutôt qu'à travers les canaux institutionnels.

Figure 30 : Façon dont l'entreprise a réagi au(x) incident(s) des tiers externes



Cette orientation se précise dans les raisons invoquées pour ne pas signaler les incidents à des tiers externes : les entreprises québécoises sont près de cinq fois plus nombreuses que leurs homologues canadiennes à citer explicitement le désir de garder la connaissance de l'incident en interne (8,4 % contre 1,8 %) (figure 31). Cet écart, d'intensité modeste, traduit néanmoins une disposition cohérente avec le comportement observé ci-dessus : les entreprises québécoises privilégient la gestion bilatérale et discrète des incidents avec des partenaires de confiance, ce qui peut nuire à la transparence institutionnelle que la Loi 25 visait précisément à encourager.

Figure 31 : Raisons de ne pas signaler certains ou tous les incidents à un tiers externe



prompt

La majorité des autres résultats sur les pratiques de consultation des pairs et de signalement ne présentent pas de différences significatives entre les deux sous-groupes et ne sont pas développées ici.

Au terme de cette mise en perspective, la posture québécoise de cybersécurité apparaît moins comme un retard généralisé que comme une configuration singulière, marquée par un écart notable entre mobilisation institutionnelle, capacités opérationnelles et perception de préparation. Les entreprises québécoises ne sont pas davantage exposées aux cyberattaques que celles du reste du Canada, et les coûts de rétablissement qu'elles assument demeurent comparables. Toutefois, elles se distinguent par une plus forte proportion d'incidents sans motif connu, par des difficultés plus prononcées à recruter des compétences spécialisées, par une diffusion moins systématique des pratiques de sensibilisation à l'ensemble du personnel, et par une gouvernance de la cybersécurité plus intensive mais moins routinisée. La Loi 25 semble avoir contribué à renforcer l'attention portée à la protection des renseignements personnels et à impliquer plus directement la haute direction, mais cela ne se traduit pas encore clairement par des retombées mesurables sur les performances techniques, la culture organisationnelle ou les capacités collectives de réponse. Le principal enjeu n'est donc pas seulement d'accroître la conformité à un nouveau dispositif législatif, mais de transformer cette conformité en un moteur d'apprentissages organisationnels durables et une source de cyber-résilience.

CHAPITRE 3. PRATIQUES DE CYBERSÉCURITÉ ET CYBER-RÉSILIENCE : UNE ANALYSE MULTIVARIÉE

Les sections précédentes ont brossé un tableau descriptif et comparatif de l'évolution de la posture de cybersécurité des entreprises québécoises entre 2021 et 2023, puis de leurs spécificités par rapport au reste du Canada. Elles ont mis en évidence une série de transformations notables comme le renforcement de la gouvernance à la haute direction, le recentrage des motivations d'investissement sur la protection des renseignements personnels, et certaines fragilités persistantes comme le faible taux de correction mensuelle des vulnérabilités ou l'absence de cartographie des risques dans près de quatre entreprises sur dix. Ces constats soulèvent une question que les analyses descriptives seules ne permettent pas de trancher : dans quelle mesure les pratiques de gestion des risques adoptées par les entreprises québécoises ont-elles un effet mesurable sur leur exposition aux cyberattaques et sur leur capacité à en absorber les conséquences et à s'en rétablir dans les meilleurs délais ?

C'est précisément à cette question que répond la présente section, en mobilisant les cinq modèles de régression mentionnés dans la méthodologie : trois régressions logistiques binaires pour les résultats dichotomiques (victimisation, survenue de coûts de rétablissement, survenue d'un arrêt de service), et deux modèles linéaires généralisés avec distribution Gamma pour les variables continues (montant des coûts de rétablissement, durée des arrêts de service). Les statistiques descriptives présentées en ouverture de cette section mobilisent les données pondérées de l'ECCC afin de brosser un portrait représentatif de la population cible des entreprises québécoises. Les modèles de régression qui suivent reposent quant à eux sur les microdonnées non pondérées, conformément aux exigences de confidentialité de Statistique Canada associées à l'accès aux fichiers de microdonnées à grande diffusion. Cette distinction n'affecte pas la validité interne des coefficients estimés (la pondération n'est pas requise pour l'estimation des associations entre variables), mais elle implique que les résultats des modèles doivent être interprétés comme des associations observées au sein de l'échantillon plutôt que comme des estimations généralisables à l'ensemble des entreprises québécoises. Ces modèles permettent de distinguer ce qui protège réellement les organisations de ce qui ne constitue qu'une apparence de préparation.

Profil de l'échantillon et distribution des variables

Avant de présenter les résultats des modèles de régression, il convient de décrire le profil de l'échantillon sur lequel ils reposent (tableau 4). La structure par taille d'entreprise est représentative de l'économie québécoise : les petites entreprises (10 à 49 employés) constituent 81,2 % de l'échantillon pondéré (n = 44 724), les moyennes 16,9 % (n = 9 333), et les grandes 1,9 % (n = 1 019), pour un total de 55 075 entreprises. Cette répartition reflète fidèlement le tissu entrepreneurial québécois, à dominante de PME, et constitue le contexte structurel dans lequel les résultats qui suivent doivent être interprétés.

Sur la question des ressources humaines dédiées à la cybersécurité (variable centrale dans les analyses multivariées), le tableau confirme le constat déjà formulé dans les chapitres précédents : 44,9 % des entreprises n'ont aucun employé affecté à ces tâches, tandis que 24,2 % en comptent un seul et 25,8 %

entre deux et cinq. Les équipes plus étoffées demeurent l'exception, ne concernant que 5 % des entreprises.

L'adoption des mesures de gestion des risques révèle des disparités considérables selon les pratiques. La surveillance du comportement des employés (27,8 %), l'implication de la haute direction (27,2 %) et l'évaluation formelle des risques (24,3 %) sont les mesures les plus répandues, tandis que la participation à une communauté d'échange d'informations sur la cybersécurité (4,4 %), la formation obligatoire (9,2 %) et le plan de continuité des affaires (8,9 %) restent très minoritaires. Ce rappel des statistiques descriptives démontre que la diffusion des pratiques de cybersécurité est loin d'être homogène et que les modèles qui suivent cherchent précisément à identifier quelles mesures, parmi cet éventail, ont un impact mesurable sur les résultats de sécurité.

Les variables continues dépendantes présentent des distributions fortement asymétriques, ce qui justifie le recours aux modèles GLM Gamma. Parmi les entreprises ayant subi un incident et déclaré des coûts de rétablissement (n = 4 399), la médiane s'établit à 6 500 $, mais la moyenne atteint 34 000 $ avec un écart-type de 91 700 $ et un maximum de 712 000 $. Ce schéma classique—une majorité d'entreprises absorbant des coûts modestes, et une minorité subissant des pertes très élevées—est cohérent avec la distribution agrégée documentée dans le premier chapitre du rapport, où les coûts totaux ont plus que doublé malgré une relative stabilité du taux de victimisation. La durée des arrêts de service présente une asymétrie similaire : médiane de 12 heures, mais moyenne de 23,98 heures (É.t. = 28,41), avec des valeurs pouvant atteindre 170 heures.

Tableau 4 : Statistiques descriptives, Québec 2023 (données pondérées)

	n	%		
Taille de l'entreprise				
Petite (10–49 employés)	44 724	81,2		
Moyenne (50–249 employés)	9 333	16,9		
Grande (250 et plus)	1 019	1,9		
Total	55 075	100,0		
Employés dédiés à la cybersécurité				
Aucun	23 311	44,9		
Un employé	12 536	24,2		
Deux à cinq employés	13 379	25,8		
Six à 15 employés	1 629	3,1		
Plus de 15 employés	1 005	1,9		
Total	51 861	100,0		
Mesures de gestion des risques				

Politique écrite de gestion des risques	11 941	21,7		
Assurance contre les cyberrisques	10 583	19,2		
Procédures d'information des employés	9 242	16,8		
Plan de continuité des affaires	4 893	8,9		
Implication de la haute direction	14 985	27,2		
Formation obligatoire en cybersécurité	5 075	9,2		
Surveillance des menaces internes	15 320	27,8		
Évaluation formelle des risques	13 400	24,3		
Tests d'intrusion	9 627	17,5		
Participation à une communauté d'échange	2 430	4,4		
Vérification des systèmes TI par un tiers	12 732	23,1		
Variables dépendantes				
Victime d'un cyberincident	8 520	15,5		
Coûts de rétablissement (parmi les victimes)	4 410	51,8		
Arrêt de service (parmi les victimes)	3 379	39,7		
Variables continues (parmi les entreprises touchées)				
	n	**Médiane ($)**	**Moyenne ($)**	**É.t.**
Coûts de rétablissement	4 399	6 500	34 000	91 700
Durée des arrêts de service (heures)	3 373	12,00	23,98	28,41

Note : Les coûts de rétablissement sont arrondis au millier le plus proche pour des raisons de confidentialité des microdonnées.

Déterminants de la victimisation : ce qui protège réellement les organisations

Les résultats du premier modèle de régression logistique (tableau 5) offrent une perspective analytique que les données descriptives ne permettaient pas d'atteindre : ils permettent d'isoler, toutes choses égales par ailleurs, l'effet propre des pratiques de gestion des risques sur la probabilité d'être victime d'un cyberincident. Le bilan est à la fois rassurant sur certains points et inquiétant sur d'autres.

Le résultat le plus robuste de l'ensemble de l'analyse concerne les ressources humaines dédiées à la cybersécurité. Dans le modèle de contrôle, une entreprise disposant d'un seul employé affecté à ces tâches a 3,85 fois moins de chances d'être victimisée qu'une entreprise sans aucun employé dédié (RC = 0,26; $p < 0,001$). Cette protection demeure significative et substantielle dans le modèle explicatif (RC = 0,38; $p < 0,001$). Cette relation forte et stable rappelle que la cybersécurité, avant d'être une question de

technologies ou de politiques, est d'abord une question de compétences humaines. Elle entre en résonance directe avec le constat formulé dans la section comparative : les entreprises québécoises éprouvent davantage de difficultés que leurs homologues canadiennes à recruter des professionnels qualifiés en cybersécurité, et cette pénurie de main-d'œuvre spécialisée pourrait constituer l'un des facteurs explicatifs de la plus forte proportion d'incidents « sans motif connu » au Québec.

La relation entre la taille de l'entreprise et la victimisation est plus nuancée. Si les entreprises de taille moyenne présentent une probabilité significativement plus faible d'être victimes que les petites entreprises (RC = 0,59; p = 0,004 dans le modèle explicatif), cet avantage ne se retrouve pas chez les grandes entreprises, dont le coefficient est non significatif. Ce résultat suggère que les moyennes entreprises ont atteint un seuil critique de ressources et d'organisation qui améliore leur posture de sécurité, mais que les grandes entreprises, exposées à des menaces plus sophistiquées et à des surfaces d'attaque plus étendues, ne bénéficient pas du même effet protecteur relatif.

Parmi les variables explicatives proprement dites, deux résultats contre-intuitifs méritent une attention particulière. Les entreprises qui procèdent à une surveillance du comportement de leurs employés (pour détecter les menaces internes) ont 1,39 fois plus de chances d'être victimes d'un incident que celles qui ne le font pas (RC = 1,39; p = 0,011). De même, les entreprises qui ont effectué des évaluations formelles des risques présentent une probabilité accrue de victimisation (RC = 1,34; p = 0,037). Ces deux associations positives ne doivent pas être interprétées comme une preuve que ces mesures augmentent le risque. Elles reflètent plutôt un phénomène bien documenté de biais de sélection inverse : les organisations les plus exposées aux menaces, qui opèrent dans les environnements les plus risqués ou qui ont été récemment victimes d'une cyberattaque sont précisément celles qui investissent dans des mesures de surveillance et de détection avancées. La causalité est inverse : c'est l'exposition au risque qui motive l'adoption de ces pratiques, et non l'inverse. Toutes les autres variables explicatives (politiques écrites, assurance, plans de continuité, formation, etc.) sont non significatives, ce qui indique que ces mesures, prises isolément, ne réduisent pas de façon mesurable la probabilité d'être ciblé par une attaque.

Ce résultat a une implication pratique directe : dans la perspective de la Loi 25, qui a principalement stimulé la mise en place de dispositions formelles de gouvernance (politiques écrites, implication de la haute direction, procédures de signalement), les données suggèrent que ces mesures, bien que nécessaires à la conformité réglementaire, ne se traduisent pas en elles-mêmes par une protection accrue contre la victimisation. La variable qui importe le plus (le capital humain spécialisé) est précisément celle sur laquelle les entreprises québécoises rencontrent le plus de défis.

Tableau 5 : Régression logistique—Déterminants de la probabilité d'être victime d'un cyberincident, Québec 2023

	Modèle contrôle			Modèle explicatif		
	RC	IC (95 %)	Sig.	RC	IC (95 %)	Sig.
Variables contrôles						
Taille de l'entreprise						
Petite (réf.)	—	—	—	—	—	—

Moyenne	0,48	0,34–0,66	***	0,59	0,41–0,84	**
Grande	0,75	0,54–1,05		0,82	0,59–1,16	
Employés en cybersécurité						
Aucun (réf.)	—	—	—	—	—	—
Un employé	0,26	0,16–0,44	***	0,38	0,22–0,67	***
Deux à cinq employés	0,40	0,24–0,67	***	0,53	0,31–0,93	*
Six à 15 employés	0,58	0,36–0,95	*	0,71	0,42–1,19	
Plus de 15 employés	0,45	0,23–0,86	*	0,47	0,24–0,92	*
Variables explicatives						
Politique de gestion des risques				0,86	0,65–1,14	
Assurance				0,93	0,72–1,21	
Procédures d'information des employés				1,24	0,93–1,65	
Plan de continuité des affaires				1,02	0,73–1,41	
Implication de la haute direction				1,11	0,85–1,44	
Formation obligatoire				0,81	0,59–1,13	
Surveillance des menaces internes				1,39	1,08–1,80	*
Évaluation formelle des risques				1,34	1,02–1,76	*
Tests d'intrusion				1,16	0,87–1,55	
Échange d'informations				1,28	0,89–1,85	
Vérification des systèmes TI				1,02	0,79–1,31	
χ^2	97,040 ***			128,591 ***		
R^2 de Nagelkerke	0,072			0,094		
Test de Hosmer-Lemeshow	4,415 (p = 0,621)			12,711 (p = 0,079)		

Note : RC = rapport de cotes. Seuils de signification : * p < 0,05; ** p < 0,01; *** p < 0,001. N = 2 055. Données non pondérées.

Déterminants des coûts de rétablissement : la gouvernance comme variable protectrice

Si les résultats du tableau 5 portaient sur la probabilité d'être victime d'un incident, les deux modèles suivants s'intéressent aux conséquences financières de ces incidents pour les entreprises qui en sont victimes. Cette distinction analytique est centrale : elle permet de dissocier les facteurs qui réduisent l'exposition au risque de ceux qui influencent la capacité de rétablissement. Il s'agit de deux dimensions de la cyber-résilience qui, comme le montrent les données, obéissent à des logiques partiellement différentes.

Le premier constat est lui-même un résultat substantiel : les variables incluses dans les modèles de régression logistique ne permettent pas de prédire si un incident engendrera des coûts pour l'entreprise (tableau 6—modèles non significatifs, $\chi^2 = 5,772$ et 19,160). Cette absence de prédictibilité semble refléter la nature aléatoire et imprévisible de la distribution des coûts post-incident, où des facteurs n'ayant pu être mesurés par le questionnaire administré durant l'enquête (comme la nature précise de l'attaque, la capacité et les stratégies de négociation avec les attaquants, le soutien offert par les assureurs, la vitesse

de détection, etc.) jouent un rôle déterminant. C'est là une limite méthodologique qui doit être reconnue : les données de l'ECCC permettent de documenter l'ampleur du phénomène mais non de l'anticiper au niveau de l'entreprise individuelle.

Une exception notable doit toutefois être mentionnée : dans le modèle explicatif, les entreprises dont la haute direction est impliquée dans les décisions de cybersécurité ont une probabilité significativement plus faible de subir des coûts de rétablissement (RC = 0,56; p = 0,016). Ce résultat constitue l'une des rares preuves empiriques, dans l'ensemble de l'analyse, d'un lien direct entre une disposition organisationnelle et une réduction des conséquences financières des incidents. Il semble apporter un argument quantitatif à l'interprétation formulée plus haut : la forte hausse du *reporting* à la haute direction documentée entre 2021 et 2023 sous l'impulsion partielle de la Loi 25 n'est pas un simple signal de conformité à portée purement symbolique. Elle semble associée à une meilleure capacité d'absorption lorsqu'un incident survient.

Tableau 6 : Régression logistique—Déterminants de la probabilité de subir des coûts de rétablissement suite à un cyberincident, Québec 2023

	Modèle contrôle			Modèle explicatif		
	RC	IC (95 %)	Sig.	RC	IC (95 %)	Sig.
Variables contrôles						
Taille de l'entreprise						
Petite (réf.)	—	—	—	—	—	—
Moyenne	1,51	0,86–2,68		1,43	0,77–2,65	
Grande	1,30	0,75–2,25		1,14	0,65–2,03	
Employés en cybersécurité						
Aucun (réf.)	—	—	—	—	—	—
Un employé	0,50	0,22–1,15		0,37	0,14–0,98	*
Deux à cinq employés	0,55	0,25–1,26		0,43	0,17–1,10	
Six à 15 employés	0,60	0,28–1,26		0,52	0,23–1,20	
Plus de 15 employés	0,35	0,11–1,08		0,33	0,11–1,05	
Variables explicatives						
Politique de gestion des risques				0,62	0,38–1,01	
Assurance				0,87	0,55–1,37	

Procédures d'information des employés				1,05	0,65–1,69	
Plan de continuité des affaires				1,19	0,70–2,03	
Implication de la haute direction				0,56	0,35–0,90	*
Formation obligatoire				0,86	0,50–1,50	
Surveillance des menaces internes				0,94	0,61–1,44	
Évaluation formelle des risques				1,26	0,77–2,06	
Tests d'intrusion				1,04	0,63–1,72	
Échange d'informations				1,28	0,69–2,35	
Vérification des systèmes TI				1,34	0,87–2,08	
χ^2	5,772 (n.s.)			19,160 (n.s.)		
R^2 de Nagelkerke	0,018			0,058		
Test de Hosmer-Lemeshow	1,862 (p = 0,762)			5,205 (p = 0,636)		

Note : RC = rapport de cotes. Seuils de signification : * p < 0,05; ** p < 0,01; *** p < 0,001. n.s. = non significatif. N = 432. Données non pondérées.

Le GLM Gamma sur le montant des coûts de rétablissement (ableau 7) livre un portrait plus contrasté. Le modèle global est significatif (χ^2 = 75,804; p < 0,001), confirmant que certains prédicteurs ont un effet mesurable sur l'ampleur des dépenses de rétablissement—même si une part importante de la variance reste inexpliquée, comme en témoignent les rapports déviance/degrés de liberté (3,05) et χ^2 de Pearson/degrés de liberté (2,67) qui s'avèrent très élevés.

La taille de l'entreprise constitue le prédicteur le plus puissant : les moyennes entreprises supportent en moyenne 97 % de coûts supplémentaires par rapport aux petites (rapport de moyenne = 1,97; p < 0,001), et les grandes entreprises des coûts cinq fois plus élevés (rapport de moyenne = 5,04; p < 0,001). Ce gradient taille-coût s'explique aisément par l'exposition plus large des grandes organisations, tant en termes de volume de données et de systèmes compromis que de complexité des opérations de rétablissement. Combiné avec le constat que les grandes entreprises ne présentent pas de moindre probabilité de victimisation (tableau 5), ce résultat dessine un profil de risque logique : les organisations les plus grandes sont aussi celles qui, lorsqu'elles sont touchées, assument les coûts les plus lourds.

La présence d'employés dédiés à la cybersécurité réduit également de façon significative les coûts : par rapport aux entreprises sans spécialistes, celles qui en comptent un voient leurs dépenses de

rétablissement diminuer de 56 % (rapport de moyenne = 0,44; p = 0,020), et celles qui en comptent deux à cinq de 67 % (rapport de moyenne = 0,33; p < 0,001). Ce résultat complémentaire renforce le tableau déjà brossé par le ableau 5 : le capital humain spécialisé en cybersécurité agit à double titre. Il réduit la probabilité d'être victime d'un incident et, lorsque l'incident survient quand-même, il diminue substantiellement son coût financier.

Un dernier résultat mérite d'être souligné, même s'il doit être interprété avec la même prudence que les associations contre-intuitives observées dans le tableau 5 : les entreprises qui ont réalisé une évaluation formelle des risques encourent en moyenne des coûts de rétablissement deux fois plus élevés que celles qui ne l'ont pas fait (rapport de moyenne = 2,02; p = 0,013). À l'instar de l'association entre surveillance des menaces internes et victimisation, les organisations qui procèdent à des évaluations formelles des risques sont précisément celles qui opèrent dans des environnements où les risques sont objectivement plus élevés et où les incidents, quand ils surviennent, tendent à être plus coûteux. Ce n'est pas l'évaluation des risques qui génère des coûts plus élevés, mais la conscience accrue du risque qui motive cette évaluation.

Tableau 7 : GLM Gamma—Déterminants des coûts de rétablissement suite à un cyberincident, Québec 2023

	Rapport de moyenne	IC (95 %)	Sig.
Variables contrôles			
Taille de l'entreprise			
Petite (réf.)	—	—	—
Moyenne	1,97	1,16–3,37	***
Grande	5,04	2,41–10,53	***
Employés en cybersécurité			
Aucun (réf.)	—	—	—
Un employé	0,44	0,22–0,88	*
Deux à cinq employés	0,33	0,18–0,64	***
Six à 15 employés	0,30	0,07–1,33	
Plus de 15 employés	0,52	0,16–1,73	
Variables explicatives			
Politique de gestion des risques	1,46	0,77–2,76	
Assurance	0,70	0,43–1,14	

Procédures d'information des employés	1,72	0,97–3,05	
Plan de continuité des affaires	0,63	0,32–1,22	
Implication de la haute direction	0,91	0,46–1,69	
Formation obligatoire	1,19	0,61–2,32	
Surveillance des menaces internes	1,08	0,67–1,73	
Évaluation formelle des risques	2,02	1,16–3,54	*
Tests d'intrusion	0,98	0,53–1,80	
Échange d'informations	1,66	0,82–3,37	
Vérification des systèmes TI	1,16	0,72–1,88	
Déviance	551,446		
χ^2 de Pearson	483,293		
Rapport de vraisemblance (χ^2)	75,804 ***		
Degrés de liberté résiduels	181		

Note : Rapport de moyenne = Exp(B). Seuils de signification : * p < 0,05; ** p < 0,01; *** p < 0,001. N = 199. Données non pondérées.

Déterminants des arrêts de service : les limites de la prédictibilité

Les deux derniers modèles s'intéressent à la dimension opérationnelle de l'impact des cyberincidents : l'existence d'un arrêt de service et sa durée. Le portrait qui en ressort est plus sévère.

Les régressions logistiques sur la probabilité d'un arrêt de service (tableau 8) ne sont pas significatives (χ^2 = 11,440 et 19,035), à l'exception d'un résultat isolé : dans le modèle de contrôle, les entreprises disposant d'un seul employé dédié à la cybersécurité présentent une probabilité d'arrêt de service significativement plus faible (RC = 0,29; p = 0,004), un effet qui demeure dans le modèle explicatif (RC = 0,25; p = 0,006). Une seule variable explicative atteint le seuil de signification : la mise en place de procédures d'information des employés est associée à une probabilité réduite d'arrêt de service (RC = 0,59; p = 0,037). Ce dernier résultat, bien qu'isolé, est cohérent avec une logique de préparation collective : informer les employés des procédures à suivre en cas d'incident permet vraisemblablement d'accélérer les processus de confinement et de réponse, limitant ainsi les interruptions opérationnelles. Sur l'ensemble des autres dimensions, les variables incluses n'ont pas de pouvoir prédictif mesurable quant à la survenue d'un arrêt de service.

Tableau 8 : Régression logistique—Déterminants de la probabilité d'un arrêt de service suite à un cyberincident, Québec 2023

	Modèle contrôle			Modèle explicatif		
	RC	IC (95 %)	Sig.	RC	IC (95 %)	Sig.
Variables contrôles						
Taille de l'entreprise						
Petite (réf.)	—	—	—	—	—	—
Moyenne	1,04	0,59–1,85		0,96	0,52–1,79	
Grande	0,87	0,50–1,50		0,84	0,47–1,50	
Employés en cybersécurité						
Aucun (réf.)	—	—	—	—	—	—
Un employé	0,29	0,12–0,67	**	0,25	0,09–0,68	**
Deux à cinq employés	0,59	0,26–1,33		0,55	0,22–1,39	
Six à 15 employés	0,55	0,26–1,16		0,57	0,25–1,29	
Plus de 15 employés	0,55	0,19–1,64		0,53	0,18–1,59	
Variables explicatives						
Politique de gestion des risques				0,83	0,50–1,38	
Assurance				0,80	0,51–1,28	
Procédures d'information des employés				0,59	0,36–0,97	*
Plan de continuité des affaires				1,17	0,69–2,00	
Implication de la haute direction				1,17	0,73–1,89	
Formation obligatoire				1,11	0,63–1,93	
Surveillance des menaces internes				1,02	0,66–1,59	
Évaluation formelle des risques				0,96	0,58–1,58	
Tests d'intrusion				1,01	0,60–1,71	
Échange d'informations				1,23	0,67–2,27	

Vérification des systèmes TI				1,01	0,65–1,58	
χ^2	11,440 (n.s.)			7,595 (n.s.)		
R^2 de Nagelkerke	0,035			0,058		
Test de Hosmer et Lemeshow	8,024			11,578		

Note : RC = rapport de cotes. Seuils de signification : * p < 0,05; ** p < 0,01; *** p < 0,001. n.s. = non significatif. N = 432. Données non pondérées.

Le modèle GLM Gamma sur la durée des arrêts de service (tableau 9) n'est pas davantage significatif dans son ensemble (χ^2 = 26,338; n.s.), même si un coefficient isolé y atteint le seuil de signification—un résultat à considérer comme exploratoire. Les entreprises qui ont procédé à une vérification complète de leurs systèmes TI par un tiers externe présentent des arrêts de service en moyenne 72 % plus longs que celles qui ne l'ont pas fait (rapport de moyenne = 1,72; p = 0,005). Ce résultat, à première vue contre-intuitif, s'inscrit dans la même logique de biais de sélection déjà rencontrée : les organisations dont les systèmes sont suffisamment complexes ou sensibles pour justifier une vérification externe indépendante sont précisément celles dont les arrêts de service, lorsqu'ils surviennent, tendent à être plus longs. L'absence générale de prédictibilité de la durée des arrêts renforce l'idée que cette variable est davantage déterminée par la nature de l'attaque et l'architecture spécifique des systèmes que par les mesures de gestion des risques génériques mesurées dans l'enquête.

Tableau 9 : GLM Gamma—Déterminants de la durée des arrêts de service suite à un cyberincident, Québec 2023

	Rapport de moyenne	IC (95 %)	Sig.
Variables contrôles			
Taille de l'entreprise			
Petite (réf.)	—	—	—
Moyenne	1,12	0,69–1,82	
Grande	1,13	0,67–1,92	
Employés en cybersécurité			
Aucun (réf.)	—	—	—
Un employé	0,86	0,50–1,50	
Deux à cinq employés	1,01	0,60–1,70	
Six à 15 employés	0,78	0,33–1,84	

Plus de 15 employés	0,84	0,38–1,84	
Variables explicatives			
Politique de gestion des risques	1,15	0,77–1,71	
Assurance	0,98	0,67–1,42	
Procédures d'information des employés	1,04	0,70–1,55	
Plan de continuité des affaires	1,38	0,87–2,18	
Implication de la haute direction	0,77	0,51–1,18	
Formation obligatoire	1,35	0,85–2,14	
Surveillance des menaces internes	0,72	0,51–1,03	
Évaluation formelle des risques	1,11	0,70–1,77	
Tests d'intrusion	0,62	0,38–1,00	
Échange d'informations	0,73	0,44–1,22	
Vérification des systèmes TI	1,72	1,17–2,52	**
Déviance	199,878		
χ^2 de Pearson	191,925		
Degrés de liberté résiduels	149		
Rapport de vraisemblance (χ^2)	26,338 (n.s.)		

Note : Rapport de moyenne = Exp(B). Seuils de signification : * p < 0,05; ** p < 0,01; *** p < 0,001. n.s. = non significatif. n = 167. Données non pondérées.

SYNTHÈSE : LA CYBERSÉCURITÉ COMME INVESTISSEMENT EN CAPITAL HUMAIN

Pris dans leur ensemble, les cinq modèles présentés dans cette section dessinent une image plus nuancée, et à certains égards moins optimiste, que celle que les seules analyses descriptives ont laissé entrevoir. Trois constats transversaux peuvent être dressés.

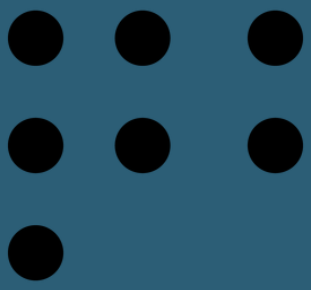
Le premier constat est que la cybersécurité est avant tout une question de capital humain. La variable la plus robuste, la plus stable et la plus cohérente à travers tous les modèles est la présence d'employés dédiés à la cybersécurité. Cette variable réduit la probabilité de victimisation, diminue les coûts de rétablissement et, dans une certaine mesure, limite les arrêts de service. Aucune autre variable ne présente un profil de prédiction aussi constant. Ce résultat entre en résonance directe avec l'un des angles morts les plus préoccupants documentés dans les sections précédentes : la quasi-stagnation du

recrutement spécialisé au Québec et les difficultés spécifiques du marché de l'emploi local dans ce domaine. La pénurie de main-d'œuvre en cybersécurité n'est pas seulement un enjeu de gouvernance ou de conformité réglementaire : c'est, selon ces modèles, la principale vulnérabilité structurelle des entreprises québécoises face aux cybermenaces.

Le deuxième constat indique que les mesures de gouvernance formelle ont des effets limités et circonscrits sur les résultats de sécurité. Les politiques écrites, les plans de continuité, les assurances et les programmes de formation, dont la prévalence a souvent augmenté entre 2021 et 2023 (en partie sous l'impulsion de la Loi 25), ne présentent dans aucun des modèles de pouvoir prédictif significatif sur la victimisation ou les coûts. Les deux seules exceptions notables sont l'implication de la haute direction et les procédures d'information des employés, associées à une probabilité réduite de coûts de rétablissement. Ce résultat doit être accueilli avec prudence : il ne signifie pas que ces mesures sont sans valeur, mais que leur effet ne se mesure pas directement dans les données de l'ECCC, soit parce qu'elles agissent sur des dimensions non captées par l'enquête, soit parce que leur déploiement est encore trop récent ou que leur implantation est trop qualitativement inégale pour produire des effets observables à l'échelle de l'échantillon.

Le troisième et dernier constat invite à interpréter ces résultats avec précaution : plusieurs associations contre-intuitives (comme la surveillance des menaces internes et les évaluations formelles des risques associées à une victimisation accrue, ou l'évaluation des risques associée à des coûts de rétablissement plus élevés) illustrent les pièges de la causalité inversée dans les études observationnelles sur la cybersécurité. Ces résultats incitent à la vigilance méthodologique : les entreprises les plus exposées/attaquées sont aussi celles qui investissent le plus dans la détection et l'évaluation des risques dans une fenêtre temporelle déterminée, de sorte que les corrélations observées dans des données recueillies ponctuellement (plutôt que de manière longitudinale) tendent à refléter des réponses adaptatives à des environnements où les menaces s'intensifient plutôt que des effets iatrogènes de ces pratiques.

Au terme de cette analyse multivariée, la posture de cybersécurité québécoise apparaît déséquilibrée : avec des investissements croissants dans des mesures de conformité et de gouvernance formelle dont les effets sur les résultats de sécurité restent difficiles à démontrer empiriquement, et un sous-investissement relatif dans la dimension qui importe le plus : les compétences humaines spécialisées. Combler cet écart constitue à la fois le principal défi et la principale opportunité de renforcement de la cyber-résilience pour les entreprises québécoises dans les années à venir.



Prompt
1200 McGill College Ave suite 1650, Montreal,
Quebec H3B 4G7

promptinnov.com

Avec la participation financière de

prompt

Québec