Devolutions

PORTRAIT DE LA SÉCURITÉ INFORMATIQUE

CHEZ LES PME QUÉBÉCOISES

2024/2025

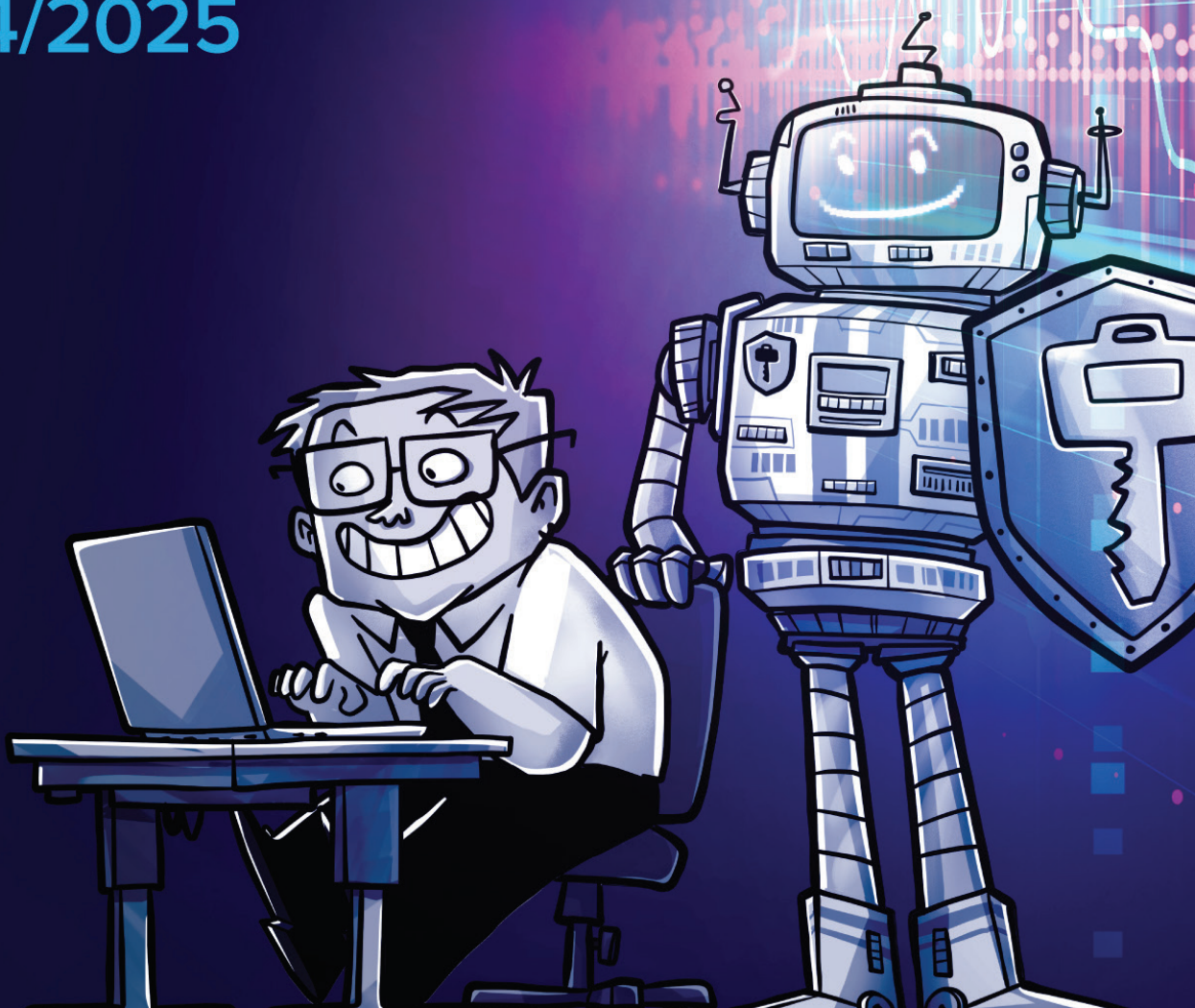


Table des matières

50% des PME québécoises ont été victimes d'au moins une cyberattaque en 2024.

Et pourtant, trop peu sont réellement prêtes à y faire face.

Ce chiffre illustre une réalité désormais bien établie : les petites et moyennes entreprises ne sont plus épargnées par les cybermenaces — elles en sont des cibles de choix.

Face à ce contexte, les organisations québécoises se montrent globalement confiantes. La majorité affirme avoir les ressources pour répondre à un incident majeur, et plusieurs indiquent vouloir augmenter leur budget en cybersécurité. Pourtant, les résultats de ce sondage révèlent un **décalage persistant entre les intentions affichées et les pratiques concrètes.**

Par exemple, la gestion des accès privilégiés repose encore largement sur des processus manuels, les formations formelles sont absentes dans un tiers des organisations, et peu de plans structurés sont en place pour répondre aux menaces internes, malgré une prise de conscience croissante.

Comparé aux résultats obtenus à l'international, **le Québec affiche un certain retard** dans plusieurs domaines clés de la cybersécurité. Ce rapport présente un état des lieux détaillé de ces écarts, en mettant en lumière **six constats majeurs.** L'objectif est clair : offrir aux PME québécoises des points de repère concrets pour évaluer leur posture actuelle, identifier leurs zones de vulnérabilité et orienter leurs priorités pour l'année à venir.

Les résultats du sondage 2024-2025 mettent en évidence **six constats clés** sur l'état de la cybersécurité dans les PME québécoises. Ces points révèlent des tendances fortes, des angles morts persistants et des occasions d'amélioration concrètes pour les mois à venir :

Chaque constat sera développé dans les pages suivantes. Nous proposerons des pistes d'action claires, des recommandations concrètes et des moyens réalistes d'améliorer la posture de cybersécurité des PME, étape par étape.

Pourquoi ce retard au Québec?

Un contexte législatif encore jeune (avec l'entrée en vigueur progressive de la Loi 25), des ressources limitées, une sensibilisation inégale et parfois une perception que les menaces concernent surtout les grandes organisations. Mais ce portrait évolue.

Notre ambition?

Offrir un point de repère utile pour s'évaluer, amorcer des changements, et bâtir une cybersécurité plus forte — à son rythme, mais avec détermination.

1. **Confiance élevée, mais posture encore limitée**

   Les PME québécoises se disent prêtes, mais peu disposent d'une posture de cybersécurité avancée.

2. **La gestion des accès privilégiés reste largement manuelle**

   Les processus critiques s'appuient encore trop souvent sur des méthodes non automatisées.

3. **L'intelligence artificielle séduit, mais son adoption tarde**

   Malgré l'intérêt, l'IA est peu intégrée dans les pratiques actuelles.

4. **Les budgets augmentent… mais restent modestes**

   Les intentions sont là, mais l'investissement réel demeure en deçà des besoins.

5. **Les menaces internes sont reconnues, mais peu traitées**

   La majorité des organisations n'a toujours pas de plan solide pour y répondre.

6. **La formation en cybersécurité reste inégale**

   Une part importante des PME ne propose toujours pas de formation formelle à ses employés.

1 Confiance élevée, mais posture encore limitée

71% des répondants se disent plutôt ou très confiants en leur capacité à répondre à un incident de cybersécurité majeur.

Pourtant, seulement 13% estiment que leur posture est réellement avancée.

Ce décalage soulève une question essentielle : **sur quoi repose cette confiance?** Est-elle fondée sur une évaluation réaliste des capacités en place, ou reflète-t-elle une perception optimiste, déconnectée des pratiques concrètes?

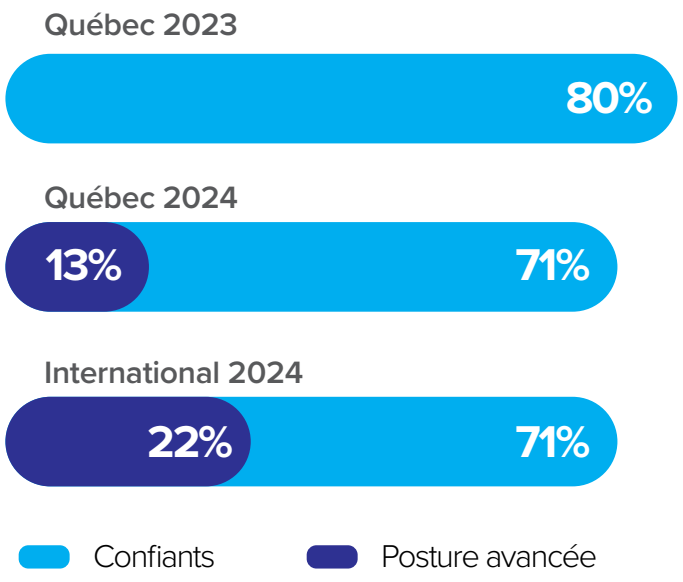
Les données révèlent un **écart préoccupant entre le sentiment de préparation et le niveau de maturité opérationnelle.** Un écart qui peut donner l'impression qu'on est prêt… jusqu'à ce qu'un incident vienne en révéler les limites.

Ce niveau de confiance est similaire à celui observé à l'international (71%) et en légère baisse par rapport à l'an dernier, où 80% des répondants québécois se déclaraient confiants.

À noter également que si les dirigeants québécois affichent un niveau de confiance élevé (78%), seulement 11% d'entre eux estiment disposer d'une posture avancée. À l'international, cette proportion grimpe à 28%.

Ce décalage plus marqué au Québec montre que la perception de préparation au sommet des organisations reste encore trop déconnectée de la réalité opérationnelle.

Confiance perçue vs posture avancée déclarée



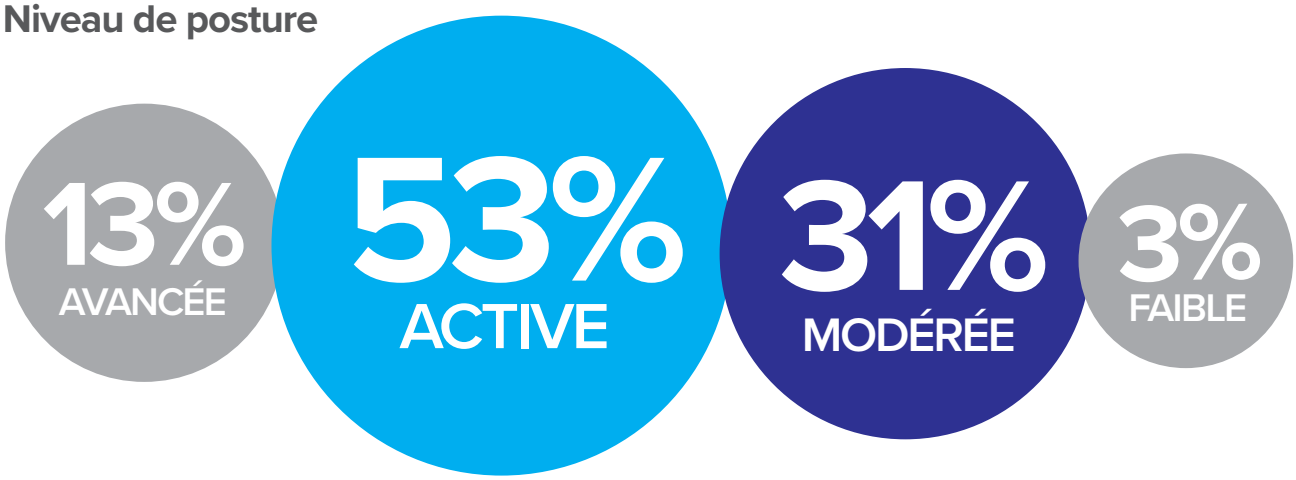
Ces résultats révèlent un écart important entre la perception de préparation et la maturité opérationnelle réelle, particulièrement marqué chez les PME québécoises. La baisse apparente n'est pas tant le signe d'une détérioration que celui d'une **meilleure prise de conscience** des exigences élevées associées à une cybersécurité pleinement mature. Ces résultats appellent une analyse plus fine de ce que cela signifie pour les PME québécoises.

CE QUE CELA RÉVÈLE

Ce nouvel indicateur permet de poser un regard plus lucide sur la réalité opérationnelle des PME. La confiance demeure forte, mais les données suggèrent **une prise de conscience plus réaliste** de ce que représente une posture véritablement avancée : capacité de détection rapide, plan de réponse formalisé, gestion continue des risques, veille technologique, etc.

Confiance ≠ préparation complète
Cette prise de conscience est une étape essentielle, mais elle devra s'accompagner d'actions concrètes pour porter ses fruits.

Niveau de posture

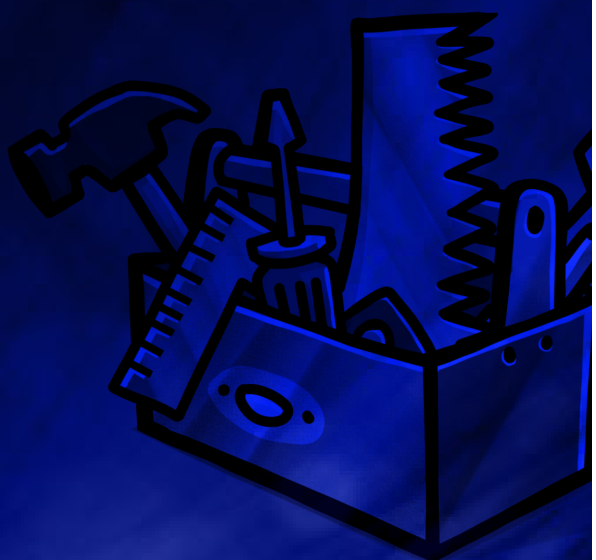


Lorsqu'on examine plus en détail la posture de cybersécurité déclarée par les PME québécoises, **la majorité se situe dans une zone intermédiaire**. Ce portrait illustre que si l'adoption de mesures de cybersécurité progresse, **la véritable maturité proactive reste encore marginale**, soulignant la nécessité d'accélérer l'évolution vers des pratiques plus robustes.

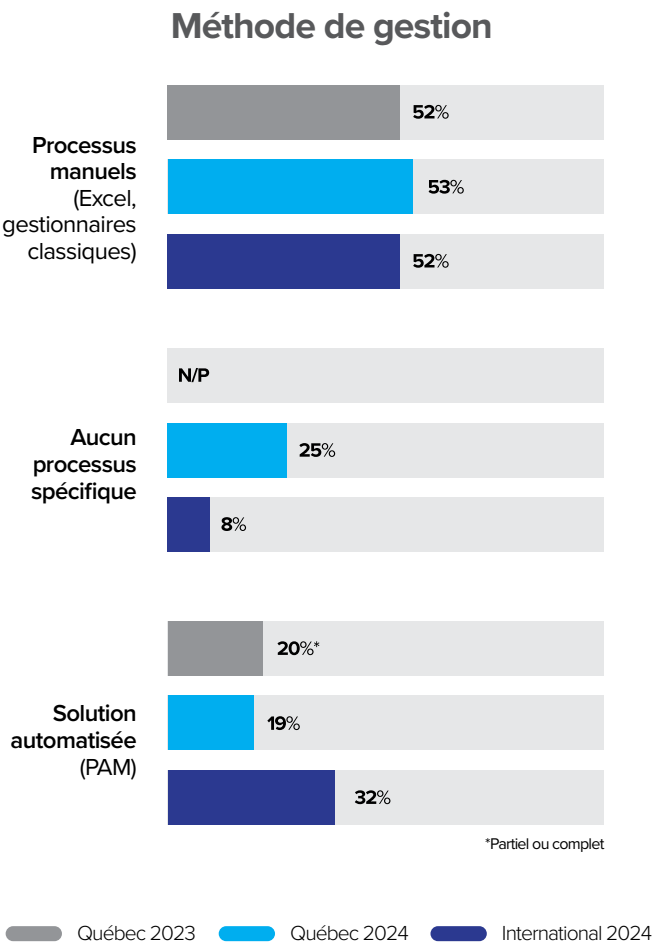
La cybersécurité ne repose pas sur un sentiment de sécurité, mais sur des processus éprouvés et une vigilance continue. Le Québec affiche une mobilisation encourageante, mais la véritable maturité reste marginale. C'est en structurant les bases que les organisations pourront réellement progresser.

Patrick Pilotte, chef de la sécurité de l'information, Devolutions

2 La gestion des accès privilégiés reste largement manuelle



53% des organisations utilisent encore des processus manuels (tableurs, gestionnaires de mots de passe classiques), et **25%** n'ont aucun processus défini.



La gestion des accès privilégiés (PAM) demeure largement dépendante de méthodes manuelles dans les PME québécoises. À l'international, la situation est similaire : **52%** des répondants déclarent également s'appuyer sur des pratiques manuelles.

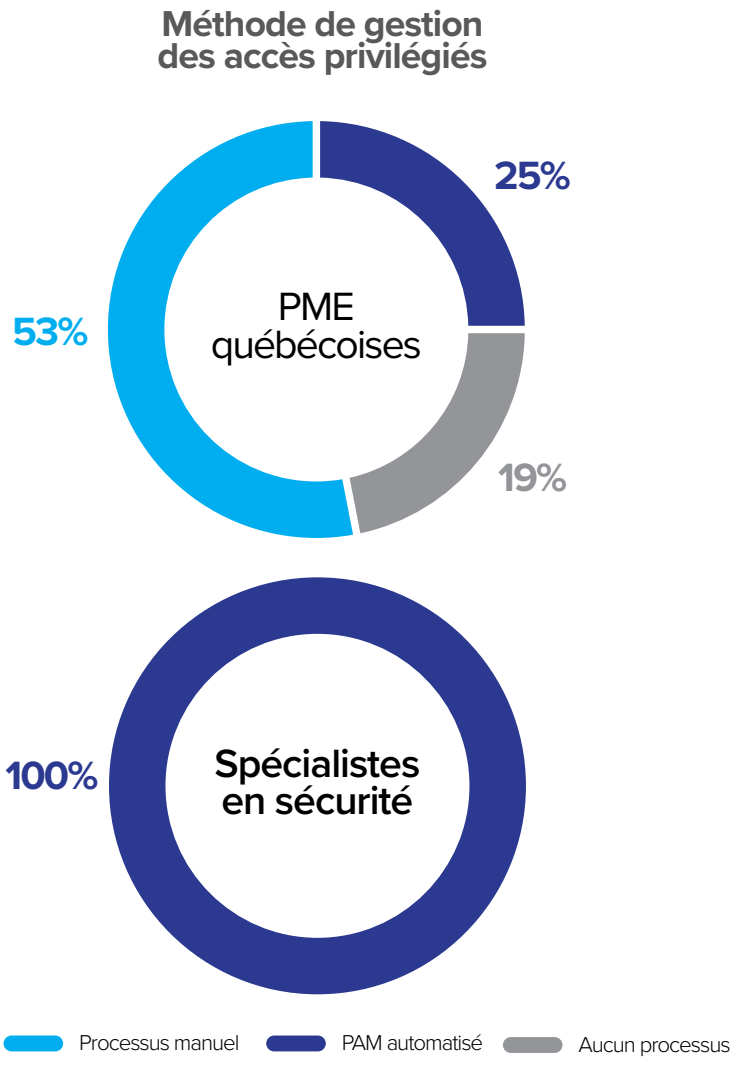
Plus préoccupant encore, **25% des organisations québécoises** n'ont **aucun processus spécifique** en place pour gérer leurs accès privilégiés.
Seule une minorité, soit **19%**, a mis en place une solution automatisée de gestion des accès privilégiés.

Ces chiffres témoignent d'un ralentissement inquiétant dans l'adoption de pratiques sécurisées modernes, particulièrement face à l'augmentation des risques liés aux comptes sensibles.

Les données montrent une **quasi-stagnation** dans la gestion des accès privilégiés au Québec entre 2023 et 2024. De plus, en 2024, **une PME québécoise sur quatre** n'a même **aucun processus spécifique en place**, un chiffre nettement plus élevé que celui observé à l'international (8%). Par ailleurs, l'adoption de solutions automatisées de gestion des accès privilégiés (PAM) progresse peu, atteignant **seulement 19%** au Québec contre **32%** à l'international.

Ces écarts soulignent que le Québec peine à moderniser ses pratiques en matière de gestion des accès sensibles, ce qui augmente les risques d'erreurs humaines, de violations d'accès et d'exposition prolongée en cas d'incident.

CE QUE CELA RÉVÈLE



Les accès privilégiés représentent un des vecteurs d'attaque les plus critiques en cybersécurité.
La dépendance à des méthodes manuelles expose les organisations à plusieurs risques :

- **erreurs humaines,**
- **accès persistants oubliés,**
- **difficulté de révoquer rapidement des permissions sensibles,**
- **manque de visibilité en temps réel.**

Ces vulnérabilités renforcent le constat selon lequel, sans gestion centralisée et automatisée, chaque mouvement de personnel ou chaque incident potentiel augmente mécaniquement l'exposition aux risques.

Le fait que **plus d'une PME sur deux** s'appuie encore sur des pratiques rudimentaires illustre **un écart majeur entre l'enjeu reconnu et la capacité de gestion réelle**. Ce constat est d'autant plus frappant lorsqu'on observe que **100% des spécialistes en sécurité** (dans notre sondage) utilisent déjà un PAM automatisé — montrant que **les experts savent où se situe le besoin**, mais que l'adoption par les autres groupes reste insuffisante.

Principales raisons de l'absence de PAM au Québec

19% Ressources limitées (manque de personnel ou d'expertise)

15% Préoccupations financières (coût jugé trop élevé)

15% Absence de besoin perçu (jugent que ce n'est pas nécessaire)

12% Solutions alternatives utilisées

8% Manque de connaissances sur ce qu'est un PAM

4% Complexité perçue de la mise en œuvre

4% Problèmes d'intégration avec les systèmes existants

12% Autres raisons (ex. : recherche de solution adaptée MSP, non applicable)

Au-delà des limites technologiques, les données révèlent **un décalage stratégique** dans l'adoption des bonnes pratiques. Au Québec, **50% des directeurs TI** utilisent encore des méthodes manuelles pour gérer les accès privilégiés, et à l'international, **44% des dirigeants** déclarent également se reposer sur des pratiques similaires. En revanche, **les spécialistes en sécurité** adoptent presque systématiquement des solutions automatisées.

Ce constat montre que la modernisation de la gestion des accès privilégiés n'est pas qu'une question d'outils : elle exige aussi un alignement clair entre les ambitions stratégiques et les pratiques opérationnelles. Tant que cette cohérence ne sera pas atteinte, les risques liés aux accès sensibles resteront sous-estimés et sous-contrôlés.

Cependant, l'écart observé n'est pas uniquement d'ordre technologique ou stratégique : des facteurs financiers et culturels freinent également l'adoption de solutions de gestion des accès privilégiés.

Défis de gestion des mots de passe

Tant que la gestion des accès privilégiés reposera sur des processus manuels, les organisations exposeront inutilement leurs données sensibles. Aujourd'hui, les outils existent pour automatiser, sécuriser et simplifier la gestion des accès privilégiés. **Il n'y a plus d'excuse pour rester vulnérable.**

Maurice Côté, vice-président produit, Devolutions

3 L'intelligence artificielle séduit, mais son adoption tarde

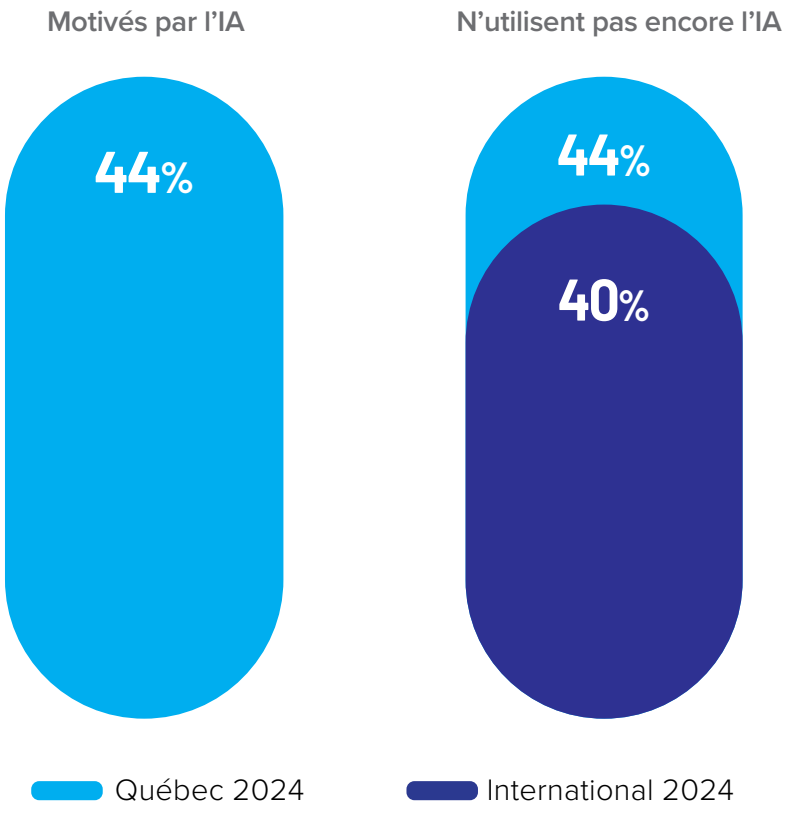
44% sont motivés par la présence d'IA dans les outils qu'ils choisissent, mais près de **44%** ne l'utilisent pas encore dans leurs opérations.

Ce constat reflète une **tendance claire** : l'IA exerce une forte attraction auprès des décideurs et influence les choix technologiques, mais **son intégration réelle dans les pratiques demeure limitée**.

À l'international, la situation est similaire. En 2024, **40% des PME** interrogées déclarent **ne pas encore utiliser l'IA** dans leur stratégie de cybersécurité, malgré un optimisme généralisé concernant son potentiel.

L'intérêt est donc bien là, mais il peine encore à se traduire en actions concrètes, autant au Québec qu'ailleurs dans le monde.

Intérêt pour l'IA VS adoption effective



CE QUE CELA RÉVÈLE

La cybersécurité vit une transition importante : **l'intelligence artificielle est perçue comme une opportunité**, mais son adoption concrète reste encore largement théorique.

Le fait que **près de la moitié** des PME québécoises soient motivées par l'intégration d'**IA dans leurs outils sans pour autant l'utiliser montre que l'IA est aujourd'hui davantage une aspiration qu'une réalité** opérationnelle.

Plusieurs facteurs peuvent expliquer cet écart : le coût d'implantation, le manque de compétences internes, la prudence face aux risques associés à l'IA (notamment la confidentialité des données), ou simplement une incompréhension des cas d'usage applicables aux PME.

Cette dynamique n'est pas propre au Québec. À l'échelle internationale, **40% des PME** déclarent également **ne pas encore avoir franchi le pas**, malgré l'intérêt marqué pour l'automatisation et la détection proactive des menaces.

Cela souligne que l'enthousiasme pour l'IA doit être accompagné d'un véritable travail de préparation technologique, stratégique et culturel, afin de transformer l'intérêt en bénéfices tangibles pour la cybersécurité.

La prudence reste de mise face à l'enthousiasme pour l'IA

Déjà en 2023, Martin Lemay, notre ex-chef de la sécurité de l'information et maintenant PDG de Cyberspective, soulignait l'importance d'une approche encadrée dans l'adoption de l'intelligence artificielle :

> **L'intelligence artificielle (IA) est une avancée majeure et prometteuse, méritant une place dans l'histoire humaine. Cependant, comme le feu, son usage requiert prudence et discernement. Dépourvue de conscience éthique et non exempte de failles, l'IA s'appuie sur d'énormes quantités de données, susceptibles d'être exploitées à mauvais escient. Il est donc vital d'établir une gouvernance adéquate et une législation rigoureuse des données pour prévenir les abus.**

Un an plus tard, les résultats du sondage confirment que l'intérêt pour l'IA est bien là, mais que son adoption reste limitée et que les défis de gouvernance et de maturité demeurent centraux.

Comme le souligne Patrick Pilotte :

> **L'intelligence artificielle représente une opportunité réelle pour renforcer la cybersécurité, mais elle doit être intégrée avec lucidité et encadrée par des pratiques solides. L'innovation ne remplace pas la vigilance.**

4 Les budgets augmentent, mais restent insuffisants

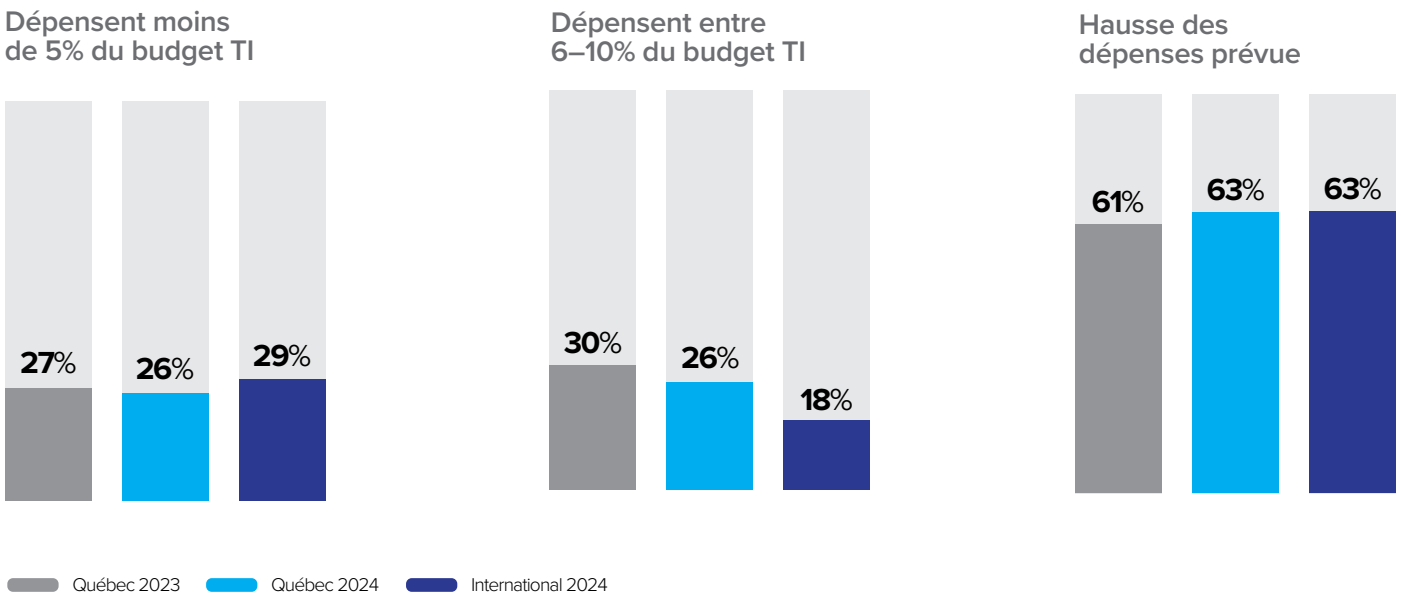
63% des PME québécoises prévoient augmenter leurs dépenses en cybersécurité en 2025

52% d'entre elles consacrent encore aujourd'hui moins de 10% de leur budget TI à la cybersécurité, et 26% y allouent même moins de 5%.

Ce contraste souligne que, malgré une volonté d'amélioration affichée,
la cybersécurité reste souvent sous-financée par rapport aux risques réels.

L'effort budgétaire progresse, mais il demeure insuffisant pour rattraper la sophistication croissante des cybermenaces.

Niveau de dépense en cybersécurité



CE QUE CELA RÉVÈLE

Il est probable que **les hausses budgétaires anticipées soient principalement absorbées par des initiatives de conformité minimale**, notamment pour répondre aux exigences de la Loi 25 sur la protection des renseignements personnels, laissant peu de ressources disponibles pour moderniser les infrastructures et renforcer réellement la posture de cybersécurité.

Les données montrent que **la conscience des enjeux** de cybersécurité progresse, mais **l'effort financier tarde à suivre**.

Le fait que **plus de 50% des PME québécoises** consacrent encore moins de 10% de leur budget TI à la cybersécurité, malgré une volonté majoritaire d'augmenter les investissements, souligne **un problème structurel** : la cybersécurité est reconnue comme prioritaire, mais **elle reste souvent abordée comme une dépense additionnelle**, et non comme une composante stratégique essentielle.

À l'international, le portrait est similaire. Cela confirme que **le sous-financement de la cybersécurité est un défi généralisé**, pas seulement une spécificité locale. **À défaut d'ajuster rapidement l'investissement aux risques actuels**, les organisations risquent de se retrouver dans une situation où l'augmentation des budgets arrive **trop tard**, après qu'un incident majeur a déjà compromis leur environnement.

Un frein réel au-delà des intentions

Ce constat est renforcé par les réponses des PME interrogées : **47% identifient le manque de budget comme un obstacle majeur à l'adoption de meilleures pratiques en cybersécurité.**

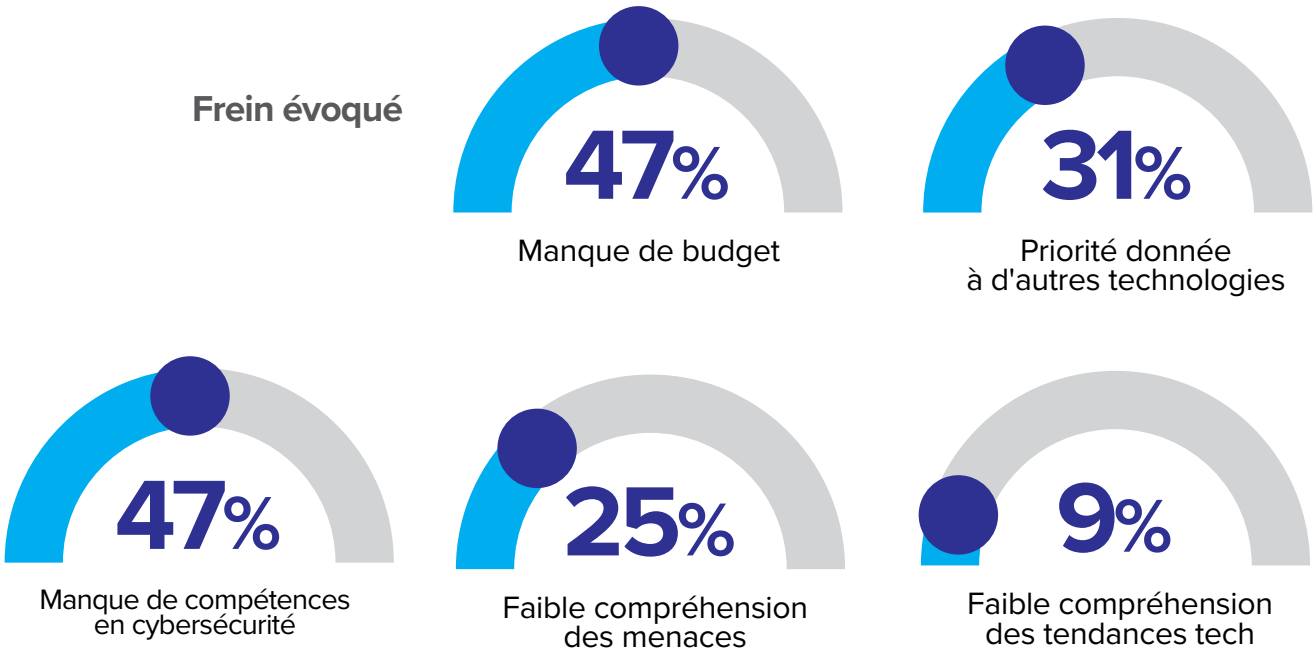
Ce paradoxe révèle que l'ampleur des augmentations prévues pourrait être insuffisante pour couvrir l'ensemble des besoins critiques.

« Ce frein budgétaire, bien qu'identifié globalement, est ressenti de manière particulièrement aiguë par les équipes en première ligne. »

Une contrainte vécue particulièrement par les équipes TI

Si le manque de budget est reconnu de manière assez large, **il est particulièrement ressenti par les équipes techniques** (professionnels TI, techniciens et spécialistes sécurité), qui constatent directement l'impact des ressources limitées sur leurs opérations quotidiennes.

Cette tendance était déjà visible en 2023, et **elle reste stable en 2024**, confirmant que **le frein budgétaire est un enjeu structurel durable**, malgré la montée des préoccupations cybersécurité.



Investir en cybersécurité n'est plus une dépense optionnelle, mais une condition de survie. Tant que les budgets resteront symboliques, la maturité organisationnelle restera hors de portée.

Patrick Pilotte, chef de la sécurité de l'information, Devolutions

5 Menaces internes : sensibilisation sans action

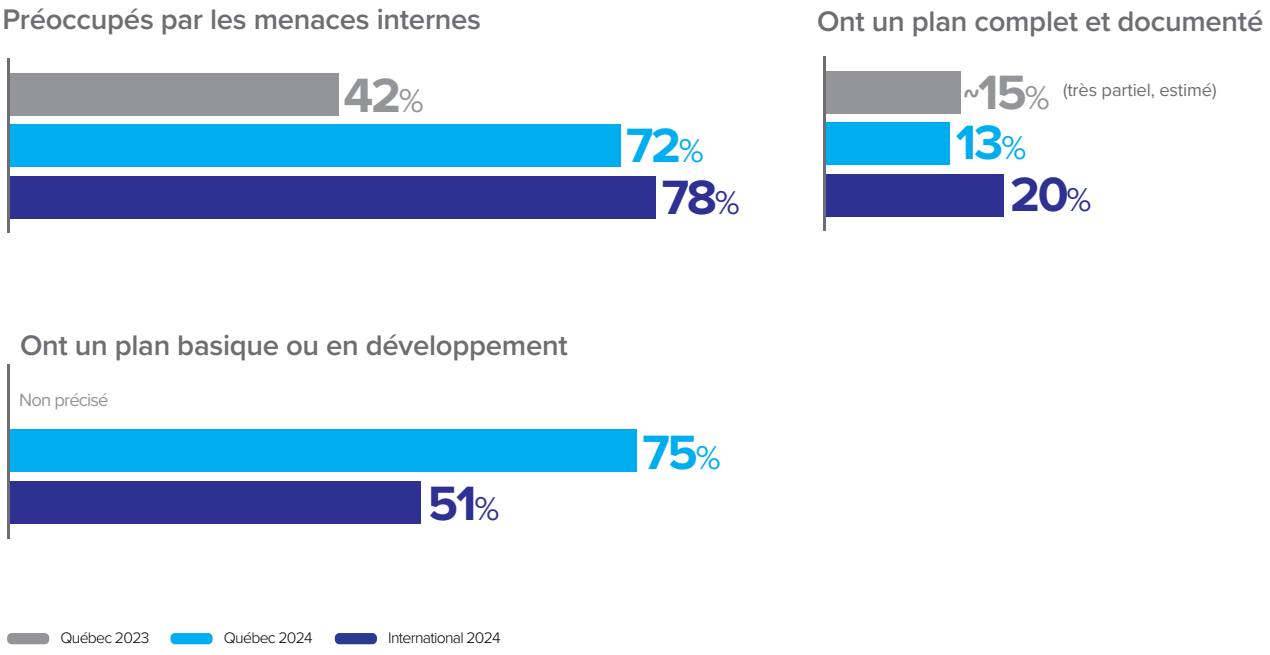
72% des PME québécoises se disent préoccupées par les menaces internes.

Pourtant, seulement 13% d'entre elles disposent d'un plan complet et bien documenté pour y faire face.

Il révèle que si la sensibilisation au risque interne progresse, la mise en place de mesures concrètes reste encore largement insuffisante.

Ce contraste est frappant.

Niveau de dépense en cybersécurité



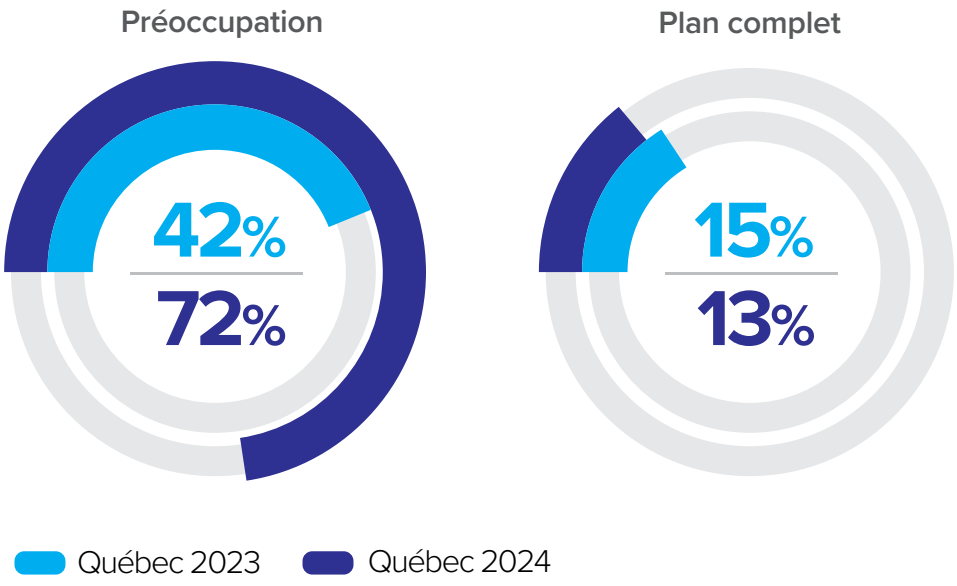
Résultat : plus de conscience, mais encore peu d'actions tangibles.

La préoccupation au Québec a presque doublé entre 2023 et 2024 (de 42% à 72%).

Mais la proportion d'organisations ayant un plan complet n'a pas progressé (voire légèrement diminué dans la précision du nouveau sondage).

Le Québec est encore moins structuré que l'international, où 20% des organisations ont un plan solide.

Évolution de la préoccupation et de la structuration face aux menaces internes (Québec)



CE QUE CELA RÉVÈLE

Cela signifie qu'environ 1 PME sur 5 pourrait potentiellement laisser des comptes actifs à des utilisateurs qui ne devraient plus y avoir accès — une faille opérationnelle qui ouvre la porte à des abus, erreurs ou intrusions involontaires.

Ce constat confirme que la gestion des risques internes ne repose pas uniquement sur la sensibilisation, mais aussi sur la rigueur des processus de sécurité de base.

Les résultats montrent **une prise de conscience significative** des menaces internes parmi les PME québécoises entre 2023 et 2024. Cependant, cette progression
en termes de sensibilisation **n'a pas été accompagnée d'une mise en œuvre proportionnelle de stratégies concrètes.**

Le fait que **seulement 13%** des organisations disposent d'un **plan formel** malgré une préoccupation forte démontre un **écart critique entre reconnaissance du risque et capacité réelle d'atténuation.**

À l'international, la situation est légèrement meilleure, avec **20% des entreprises** équipées d'un plan solide. Cela indique que **le Québec accuse un retard non pas dans la perception du problème, mais dans sa gestion opérationnelle.**

Sans planification structurée, la menace interne — qu'elle soit intentionnelle ou accidentelle — reste un point aveugle majeur, capable de provoquer des incidents coûteux
et difficilement détectables.

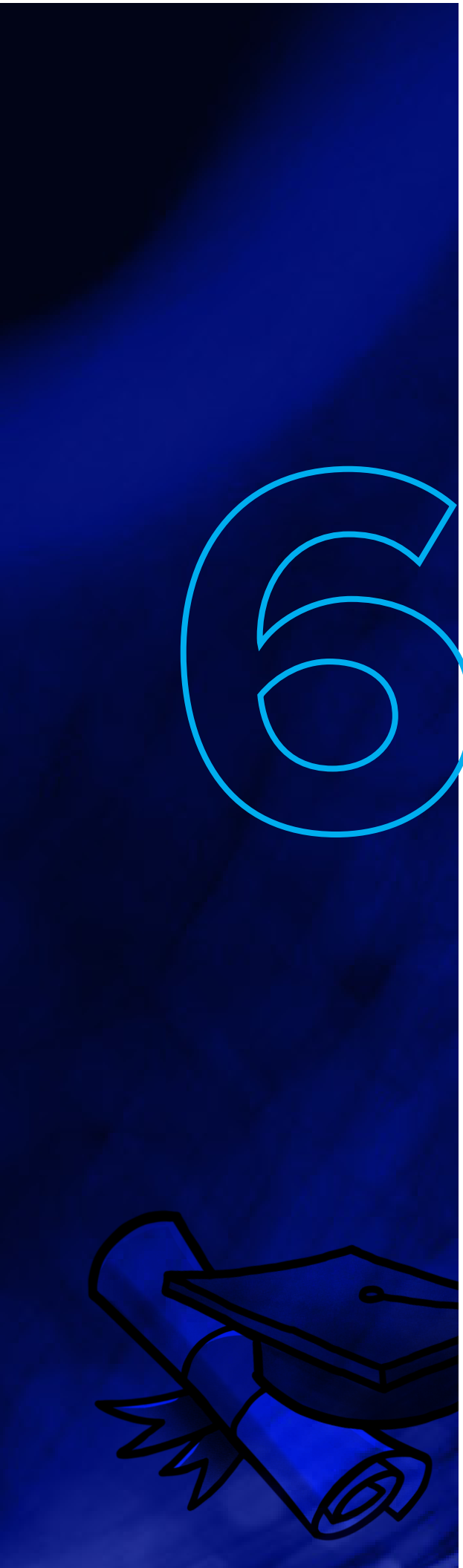
Une gestion des accès encore perfectible

Parmi les mesures de base pour se prémunir contre les menaces internes, la révocation rapide des accès aux anciens employés devrait aller de soi.

Pourtant, selon les résultats du sondage, **seulement 82% des organisations déclarent appliquer une politique formelle de révocation. 7% reconnaissent ne pas le faire**, et **11% ne savent pas ou préfèrent ne pas répondre.**

Reconnaître un risque sans agir, c'est accepter d'y être exposé. La sensibilisation est un premier pas, mais seule une approche structurée permet de transformer la connaissance du risque en véritable résilience.

Patrick Pilotte, chef de la sécurité de l'information, Devolutions



6 Formation en cybersécurité : des progrès, mais encore loin derrière

Une PME québécoise sur trois n'offre aucune formation formelle en cybersécurité à ses employés.

Ce constat est d'autant plus préoccupant que **l'erreur humaine demeure l'une des principales causes d'incidents de cybersécurité.**

À l'international, la situation est sensiblement meilleure : **seulement 17% des organisations** déclarent ne proposer aucune formation à leurs équipes.

Parmi les entreprises québécoises qui offrent une formation, **28% proposent une sensibilisation annuelle** et **28% offrent une formation continue.**

À titre de comparaison, **39% des organisations à l'international** misent sur la formation continue, démontrant une approche plus proactive.

Ces données révèlent un **retard préoccupant au Québec**, où la sensibilisation à la cybersécurité reste trop souvent **ponctuelle ou inexistante**, malgré une reconnaissance croissante des risques liés au facteur humain.

	Québec 2023	Québec 2024	International 2024
Aucune formation formelle offerte	50%	34%	17%
Formation annuelle de sensibilisation	Non précisé	28%	32%
Formation continue	Non précisé	28%	39%
Certifications externes	Non précisé	6%	6%

CE QUE CELA RÉVÈLE

Entre 2023 et 2024, les PME québécoises ont accompli des progrès notables en matière de sensibilisation à la cybersécurité.
La proportion d'organisations n'offrant aucune formation formelle est passée de près de **50% à 34%**, témoignant d'une prise de conscience croissante des enjeux liés au facteur humain.

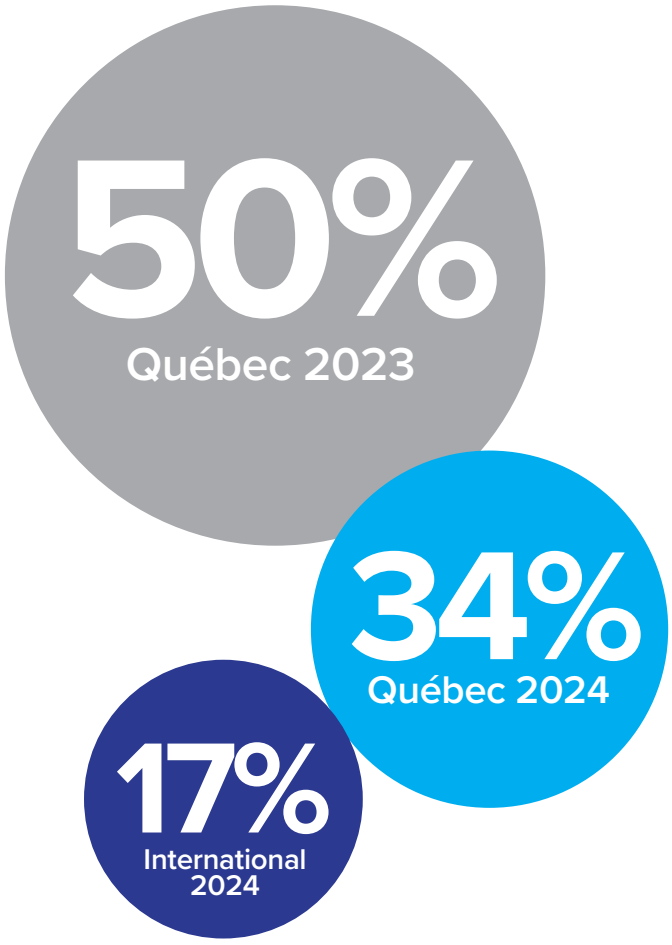
Cependant, cette amélioration ne masque pas un constat plus inquiétant : **la formation continue reste marginale.**

De plus, lorsque la formation est proposée, elle demeure souvent **ponctuelle et centrée sur quelques thématiques spécifiques**, plutôt que sur une approche structurée visant à développer une culture de cybersécurité durable.

Tant que la formation restera ponctuelle ou absente, les organisations continueront d'exposer leur premier vecteur de risque — leurs employés — aux tentatives d'ingénierie sociale, d'hameçonnage ou d'accès non autorisé.

Le progrès est donc réel, mais **il doit s'accélérer** pour transformer la sensibilisation initiale en **comportements sécuritaires durables.**

Taux d'absence de formation formelle en cybersécurité

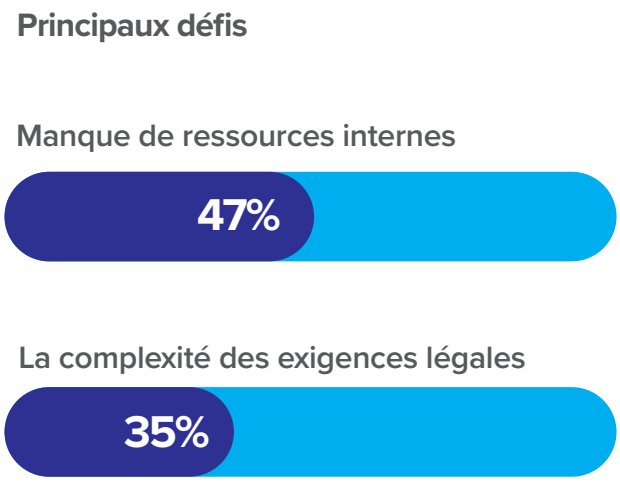


Former, ce n'est pas cocher une case : c'est bâtir une culture. Tant que la cybersécurité ne sera pas intégrée dans les réflexes du quotidien, les meilleures technologies resteront vulnérables aux erreurs humaines.

Simon Chalifoux, chef des technologies de l'information, Devolutions

7 La Loi 25 : entre conscientisation et incertitude

47% des PME québécoises déclarent être prêtes à respecter l'ensemble des exigences de la Loi 25 en 2025.



Mais derrière ce chiffre encourageant se cache une réalité plus nuancée : **29% des organisations reconnaissent ne pas être prêtes**, et **près d'un quart (23%)** ne savent pas ou préfèrent ne pas se prononcer sur leur niveau de préparation.

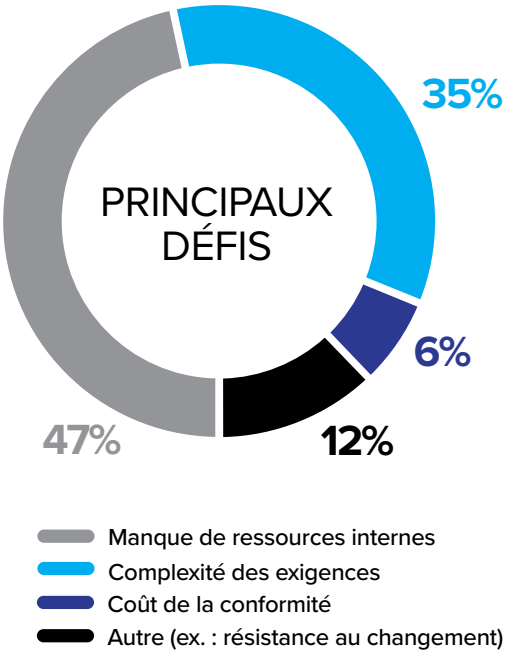
Au total, **plus de la moitié des PME québécoises se trouvent dans une zone d'incertitude ou de non-conformité potentielle**.

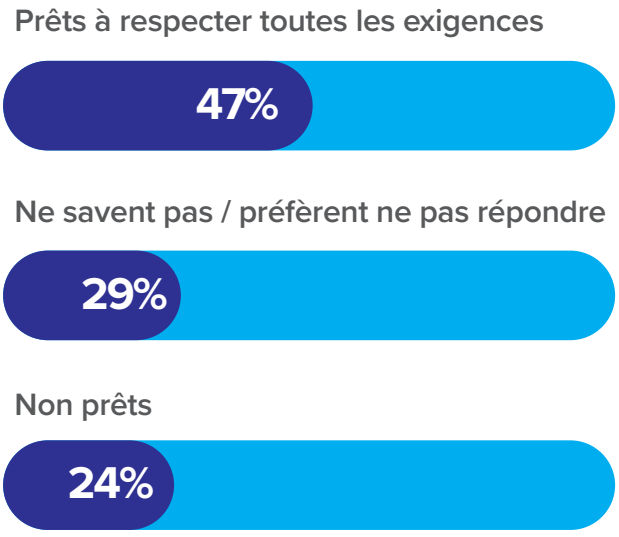
Lorsqu'on explore les principaux défis auxquels elles font face, **47% pointent le manque de ressources internes** (temps, personnel, expertise), tandis que **35% mentionnent la complexité des exigences légales.**

Fait notable : **le coût est rarement cité comme un obstacle majeur** (6%), ce qui laisse entendre que **les freins sont d'abord structurels et organisationnels, plutôt que financiers.**

Enfin, même si les sanctions prévues par la Loi 25 — pouvant atteindre 25 M$ ou 4% du chiffre d'affaires mondial — sont significatives, **41% des PME se disent peu ou pas préoccupées.** Un écart persistant subsiste donc entre la gravité potentielle des conséquences et la perception qu'en ont certaines organisations.

CE QUE CELA RÉVÈLE





Les résultats soulignent une dynamique ambivalente. D'un côté, **près de la moitié des PME affirment être prêtes** à respecter les exigences de la Loi 25, ce qui témoigne d'un progrès réel dans la compréhension des obligations en matière de protection des renseignements personnels.

D'un autre, **le fait que plus de 50% des organisations soient encore en retard ou dans le flou quant à leur niveau de préparation** montre que l'application de la loi reste inégalement comprise et intégrée. Le principal frein évoqué — **le manque de ressources internes** — confirme qu'il ne s'agit pas tant d'un problème d'intention ou de budget que d'un **défi structurel** : absence de temps, d'expertise, ou de capacité à prioriser la conformité dans un contexte déjà chargé.

Cela pose une question stratégique : **les PME disposent-elles des bons leviers — outils, accompagnement, temps — pour traduire la Loi 25 en actions concrètes?**

Par ailleurs, le fait que **près de 41% des PME ne se disent pas préoccupées** par les sanctions prévues par la loi suggère un **décalage préoccupant entre la portée réelle du cadre législatif et la perception qu'en ont certaines entreprises.**

Ce manque d'urgence perçue pourrait retarder davantage encore les démarches de mise en conformité.

La Loi 25 ne doit pas être perçue comme une contrainte administrative, mais comme une occasion de structurer durablement la gestion des données personnelles et de rehausser la confiance organisationnelle.

La Loi 25 ne devrait pas être vue comme un fardeau réglementaire, mais comme un catalyseur. Elle pousse les PME à revoir leurs pratiques, à structurer leur gestion des données et à bâtir une culture de confiance — à l'interne comme à l'externe.

David Hervieux, président-fondateur de Devolutions

Conclusion

Conclusion — Entre intentions et action

L'édition 2024-2025 du sondage révèle une dynamique marquée : la cybersécurité est désormais bien présente dans les préoccupations des PME québécoises, et les intentions sont affirmées.

Confiance, intérêt pour l'IA, volonté d'investir, attention portée aux menaces internes — tous les signaux indiquent une sensibilisation croissante.

Mais en creusant, un fil conducteur traverse les chapitres : un décalage persistant entre la reconnaissance des enjeux et la capacité réelle à y répondre.

Les pratiques demeurent souvent manuelles.
Les formations sont inégales, les plans incomplets.
La conformité, notamment à la Loi 25, progresse, mais de manière fragmentée.
Les budgets, bien qu'en hausse, restent insuffisants pour répondre à la complexité des menaces actuelles.

Il ne s'agit pas d'un simple retard technologique, mais d'une question de posture et de structuration.
D'une volonté de construire dans la durée, et non seulement de réagir sous pression.

Ce que ce sondage montre, c'est que les PME québécoises ne manquent pas d'intention, mais qu'elles ont besoin de repères concrets, d'outils adaptés et d'un accompagnement ciblé pour transformer ces intentions en actions efficaces.

Des angles morts encore bien présents

Malgré les progrès observés, certaines vulnérabilités importantes persistent :

- **Seulement 5%** des PME utilisent des **jetons d'accès temporaires** (Juste-à-Temps), une méthode reconnue pour limiter l'exposition aux accès sensibles.
- **47%** disposent d'une **cyberassurance complète**, laissant plus de la moitié des entreprises partiellement ou non couvertes face aux risques financiers liés à un incident.
- **Environ 1 PME sur 5** ne révoque pas systématiquement les accès de ses anciens employés — un oubli opérationnel critique.
- **Près de 35%** des PME ressentent déjà un **impact géopolitique direct** sur leur cybersécurité.
- **Plus de 40%** identifient des risques croissants liés à :
  - la chaîne d'approvisionnement,
  - les attaques parrainées par des États,
  - le cyberespionnage,
  - la désinformation alimentée par les deepfakes.

Dans ce contexte, penser la cybersécurité comme un exercice de conformité minimale ne suffit plus. Il faut la concevoir comme une démarche de **résilience globale**, intégrée aux priorités stratégiques, capable d'évoluer avec les menaces — locales ou internationales.

Ce passage ne se fera pas seul. Il exigera de la clarté, de la coordination et un engagement constant, mais il est à portée des PME qui souhaitent bâtir une cybersécurité à leur image : accessible, proactive et durable.

Tout au long du sondage, on observe que les PME québécoises sont de plus en plus conscientes des enjeux. Ce qu'il leur manque, ce sont des repères concrets, des outils adaptés et un accompagnement ciblé pour transformer cette intention en action.

David Hervieux, président-fondateur de Devolutions

Perspectives d'avenir

Perspectives d'avenir

L'édition 2024-2025 du sondage dresse un constat clair : les PME québécoises sont de plus en plus conscientes des enjeux liés à la cybersécurité.

La confiance est élevée, les intentions sont affirmées, et plusieurs organisations amorcent une transformation importante. Mais une question demeure : ces intentions se traduiront-elles en actions structurées, durables et efficaces?

Les résultats révèlent un écart persistant entre sensibilisation et mise en œuvre. Pour combler ce fossé, les PME devront aborder la cybersécurité comme un levier stratégique — pas simplement comme une réaction à une menace ou une exigence réglementaire.

> **On ne bâtit pas une entreprise durable sans une base solide.** La cybersécurité, c'est cette base. Elle ne garantit pas la croissance, mais son absence garantit le risque.
>
> *David Hervieux, président-fondateur de Devolutions*

Voici cinq grandes tendances que nous anticipons pour les prochaines années, et qui traceront la voie des PME les plus résilientes :

1. De la réaction ponctuelle à la structuration continued'accès temporaires

Les PME ne pourront plus se contenter de répondre aux incidents ou de mettre en place des mesures isolées. Une posture durable exigera des processus documentés, des plans formels et une gouvernance claire, soutenue par la direction.

2. L'IA passera de tendance à exigence

L'intelligence artificielle séduit, mais son adoption est encore inégale. À mesure que les solutions s'intègrent aux outils de cybersécurité, les PME devront renforcer leur capacité à évaluer, intégrer et encadrer l'IA pour en tirer des bénéfices réels — sans créer de nouvelles vulnérabilités.

3. L'automatisation deviendra un standard de maturité

Qu'il s'agisse de PAM, de révocation automatique des accès, ou d'authentification adaptative, les organisations matures abandonneront les outils manuels au profit de solutions automatisées. C'est à la fois une question de sécurité, d'efficacité… et de temps.

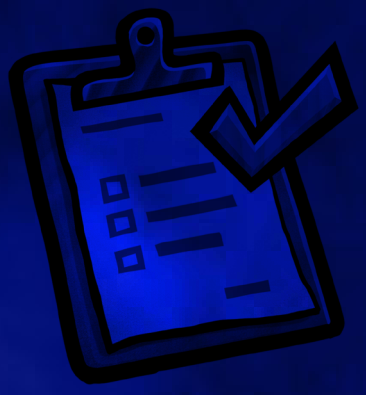
4. La conformité poussera vers l'alignement stratégique

La Loi 25 ne sera pas qu'un déclencheur technique. Elle deviendra un révélateur de maturité organisationnelle.
Les PME qui l'intègrent dans leur stratégie globale gagneront en crédibilité, en transparence et en compétitivité.

5. Le contexte géopolitique s'invitera dans les réflexes de gestion

Les chaînes d'approvisionnement, les attaques parrainées par des États et la désinformation ne sont plus des menaces "distantes". Les PME devront élever leur posture pour intégrer des risques globaux dans leur cybersécurité locale.

Recommandations



Recommandations
Ce qu'il faut mettre en place maintenant

La cybersécurité ne repose pas sur de grandes théories, mais sur des gestes concrets, répétés, intégrés dans la réalité quotidienne des PME. Ce qu'il reste à faire, c'est d'agir avec méthode.

Voici cinq priorités que les PME québécoises peuvent mettre en place, peu importe leur niveau de maturité.

1.

Abandonner la gestion manuelle des accès privilégiés

53% des PME utilisent encore des fichiers Excel ou des outils de base pour gérer les accès sensibles.

Passez à une solution de gestion des accès privilégiés (PAM) simple, flexible et intégrée, qui permet la consignation des sessions, le contrôle des droits et l'application du principe du moindre privilège — sans complexité inutile.

La solution Devolutions :

Gestion des mots de passe pour les équipes

Devolutions Workspace / Devolutions Hub / Devolutions Server

https://devolutions.net/fr/solutions/

2.

Intégrer la formation à la culture d'entreprise

Une PME sur trois n'offre toujours aucune formation formelle en cybersécurité.

Remplacez les approches ponctuelles par une stratégie de formation continue : modules courts, simulations d'hameçonnage, rappels ciblés selon les rôles.

La solution Devolutions :

Devolutions Academy

nous offrons une plateforme gratuite de formation continue, pensée pour les réalités des petites équipes.

https://academy.devolutions.net/

3.

Encadrer l'adoption de l'intelligence artificielle

44% des PME sont motivées par l'IA dans leurs choix d'outils, mais aussi nombreuses sont celles qui ne l'utilisent pas encore.

Déployez l'IA là où elle apporte de la valeur — gestion intelligente des identifiants, analyse d'activités — tout en gardant un contrôle clair sur les décisions automatisées.

La solution Devolutions :

Gestion des accès à distance

Devolutions Gateway / Devolutions Launcher
Devolutions Workspace / Devolutions Hub / Devolutions Server

https://devolutions.net/fr/solutions/

4.

Utiliser la Loi 25 comme levier de maturité

Moins de la moitié des PME se disent prêtes à respecter les exigences de la Loi 25.

Utilisez cette échéance pour clarifier vos processus, documenter les accès et renforcer la traçabilité.

La solution Devolutions :

Gestion des accès privilégiés

Devolutions PAM / Remote Desktop Manager / Devolutions Gateway / Devolutions Launcher / Devolutions Workspace / Devolutions Hub / Devolutions Server

https://devolutions.net/fr/solutions/

5.

Moderniser la gestion de l'accès à distance

77% des PME utilisent des portails d'accès distants, mais peu vont plus loin dans la segmentation ou le contrôle des sessions.

Adoptez une gestion centralisée des connexions à distance, avec journalisation, séparation des environnements et permissions limitées dans le temps.

La solution Devolutions :

Gestion des connexions à distance

Remote Desktop Manager / Devolutions Gateway / Devolutions Launcher / Devolutions Workspace / Devolutions Hub / Devolutions Server

https://devolutions.net/fr/solutions/

Ce qu'il faut retenir

La cybersécurité ne se renforce pas avec des intentions, mais avec de la structure.

Ce que les PME peuvent faire aujourd'hui, c'est démarrer petit, avancer avec constance — et s'équiper d'outils conçus pour soutenir leur croissance sans compromettre leur sécurité.

MOT DE LA FIN

David Hervieux,
président-fondateur de Devolutions

« **Ce rapport montre une chose très clairement : les PME savent que la cybersécurité est un enjeu.** Elles le reconnaissent, elles le nomment, elles veulent progresser. Maintenant, le défi, c'est de transformer cette conscience en capacité réelle.

Pas besoin de tout faire d'un coup. Ce qu'il faut, c'est structurer, stabiliser, avancer avec constance. Et surtout, ne pas attendre qu'un incident nous oblige à faire ce qu'on aurait pu anticiper.

Chez Devolutions, nous croyons profondément que les PME méritent des outils adaptés à leur réalité — et des repères clairs pour savoir par où commencer.

Si ce rapport peut aider, même un peu, à faire ce passage de l'intention à l'action, alors il aura rempli son rôle. »

Devolutions

Comment Devolutions peut vous aider

Conçus pour les PME. Pensés pour vous.

Chez Devolutions, nous croyons que les PME ne devraient jamais avoir à choisir entre simplicité, sécurité et efficacité. C'est pourquoi nous avons conçu une suite d'outils de gestion des accès privilégiés (PAM), de gestion des mots de passe et de connexions à distance — spécifiquement pour les petites équipes TI.

Ce qui nous distingue :

Pensé pour les PME

léger, abordable, rapide à déployer

Sécurisé par défaut

chiffrement de niveau entreprise, journalisation complète, contrôle granulaire des accès

Flexible et évolutif

installation sur site ou infonuagique, selon vos préférences

Accessible partout

compatible télétravail, appareils mobiles et environnements hybrides

Soutenu par des experts

accompagnement humain, formation continue, soutien local

Devolutions

Que vous débutiez votre transformation ou que vous cherchiez à structurer ce qui est déjà en place, nous vous donnons les moyens d'aller plus loin — avec maîtrise, confiance et contrôle.

Plusieurs ressources sont à votre disposition:

Devolutions Academy
https://academy.devolutions.net/

Documentation de Devolutions
https://docs.devolutions.net/fr/

Forum de Devolutions
https://forum.devolutions.net/

Blogue de Devolutions
https://blog.devolutions.net/fr/

Contactez-nous

Téléphone : +1 844 463-0419
Courriel : sales@devolutions.net
Site Web : www.devolutions.net/fr
Clavardage : Directement sur notre site