Édition 2026

PORTRAIT.TI

LE RAPPORT DE RÉFÉRENCE DES TI AU CANADA

DES DONNÉES POUR ÉCLAIRER VOS DÉCISIONS

IMPOSSIBLE DE L'IGNORER :

VOTRE STRATÉGIE EST-ELLE PRÊTE ?

NOVIPRO NOVA NETWORKS Léger IBM

MÉTHODOLOGIE

Les données présentées dans ce rapport ont été recueillies dans le cadre d'un sondage en ligne mené du 1er janvier au 3 février 2026. Cette 10e édition du sondage a été conçue pour recueillir des résultats comparables à ceux des années précédentes, ainsi que les tendances émergentes de 2026.

Le sondage a été mené par Léger auprès de petites entreprises (moins de 100 employés), de moyennes entreprises (de 100 à 499 employés) et de grandes entreprises (500 employés ou plus) au Canada.

Parmi les répondants, on comptait 300 décideurs spécialisés en TI, 76 gestionnaires non spécialisés en TI et 76 décideurs non spécialisés en TI et qui ne sont pas des gestionnaires. Parmi les répondants, aucun n'était client de NOVIPRO.

En raison de la nature non probabiliste de l'échantillon (associée à tout sondage en ligne), le calcul de la marge d'erreur ne s'applique pas. Aux fins de comparaison, un échantillon probabiliste de 452 répondants aurait une marge d'erreur globale de ±4,58 %, 19 fois sur 20, avec des marges plus élevées pour les sous-groupes.

10 ans de Portrait TI : bilan d'une décennie et perspectives d'avenir

NOVIPRO a lancé le rapport Portrait TI en 2017. À ce moment-là, Excel était encore l'outil de données par excellence, et les mégadonnées étaient considérées comme révolutionnaires. Les documents partagés n'existaient pas, et la collaboration et le contrôle des versions nécessitaient l'envoi par courriel d'un fichier que l'on pouvait appeler « final_v3_vraiment_final.xlsx ». Avoir un accès à distance signifiait que l'on se connectait une fois par semaine à partir de son domicile, et non que l'on dirigeait l'ensemble de l'entreprise depuis sa cuisine.

Même il y a 10 ans, la technologie évoluait rapidement, et NOVIPRO souhaitait offrir un outil conçu pour les entreprises locales, par des personnes qui les comprenaient. Dix ans plus tard, cet objectif s'est transformé en un accomplissement dont nous sommes très fiers : une référence citée par les universités et les médias, archivée par la bibliothèque nationale et, plus important encore, digne de confiance pour des décideurs de partout au Canada.

Au fil des ans, nous avons eu des milliers de discussions avec des dirigeants des TI, des cadres et des équipes à l'échelle nationale, et elles portaient toutes sur le même défi : comment s'adapter aux changements en continuant d'exploiter les entreprises.

Depuis lors, l'infonuagique est devenue le fondement opérationnel de l'entreprise moderne. Les rançongiciels constituent dorénavant un secteur d'activité. L'utilisation de mégadonnées est passée d'une solution innovante à une pratique courante. Du jour au lendemain, le travail à distance a modifié la réflexion des entreprises sur les infrastructures, les talents et la productivité. En 2017, l'IA relevait encore de la science-fiction, mais elle fait maintenant partie de toutes les discussions stratégiques pertinentes.

Ce rapport offre bien plus qu'un aperçu : il s'agit d'un miroir qui reflète la situation des organisations ainsi que leur façon de penser, de prendre des décisions et d'évoluer. La réflexion est un thème important de cette 10e édition. Pour la première fois, nous avons inclus une section **Suivi des tendances** tout au long du rapport. Celle-ci retrace l'évolution des indicateurs clés durant toute la décennie et présente une vision sur 10 ans des mouvements, des obstacles et des surprises dans le paysage des TI au Canada. Nous avons également ajouté une section **Pleins feux sur les secteurs d'activité,** qui examine en profondeur les réalités des TI dans des secteurs où les enjeux sont de taille, comme les finances, l'industrie manufacturière et les soins de santé.

Si la dernière décennie nous a appris quelque chose, c'est que le changement se manifeste rarement seul. L'IA, l'informatique quantique, la fragmentation géopolitique et l'accélération de la cybercriminalité comme arme ne sont pas des défis qui se surviennent un à un : ils se présentent tous en même temps. Les organisations qui réussiront le mieux à les relever seront celles qui croient que les TI constituent non pas une fonction à gérer, mais bien un fondement sur lequel tout le reste repose.

Nous sommes fiers de ce que ce rapport a permis de mettre en lumière au cours des 10 dernières années, et nous sommes ravis de savoir que nos analyses joueront un rôle clé dans les prises de décisions qui façonneront les 10 prochaines années.

Constats clés

Les organisations canadiennes accélèrent leurs investissements technologiques, mais la vitesse à elle seule n'est plus un facteur de différenciation comme elle l'était autrefois. Le rapport Portrait TI de cette année révèle un point de changement : les ambitions augmentent, les budgets s'accroissent et les équipes d'informatique ont gagné une place officielle à la table de la stratégie. Les organisations qui tireront leur épingle du jeu ne seront pas celles qui dépenseront le plus, mais celles qui géreront, exécuteront et développeront les talents de la façon la plus intentionnelle.

Les conclusions de cette année sont marquées par plusieurs tensions. L'adoption de l'infonuagique est devenue la référence opérationnelle, mais de nombreuses organisations ont évolué rapidement sans mettre en place les cadres de souveraineté, de gouvernance et de gestion des données nécessaires. Il est désormais impératif de réaliser des vérifications et de formaliser les processus afin de comprendre où se trouvent les données, qui les contrôle et si l'infrastructure en place est conçue pour la résilience autant que pour la souplesse. L'IA est passée du stade de projet pilote à celui de pratique, mais son niveau de maturité est inégal; les organisations qui n'ont pas encore défini ce qu'est une adoption responsable et un processus de gouvernance de l'IA à l'interne risquent de prendre encore plus de retard, car l'écart entre les chefs de file et les autres continue de se creuser.

Les investissements en cybersécurité augmentent, mais ils dépassent la capacité de responsabilisation organisationnelle nécessaire pour en assurer l'efficacité. Combler cet écart exige plus que des outils — cela nécessite des processus, de la formation et un alignement au niveau de la direction.

L'ÉLÉPHANT DANS LA PIÈCE

Cette synergie est également le principal défi auquel est confrontée la direction des TI en général : bien que les TI soient au cœur des discussions, elles n'influencent pas encore de manière systématique les décisions qui y sont prises. Combler le fossé de perception entre les dirigeants des TI et les dirigeants hors-TI n'est pas une priorité mineure. C'est la condition préalable au bon fonctionnement de tout le reste.

Enfin, les pressions liées aux ressources humaines qui pèsent sur les équipes informatiques – épuisement professionnel, fidélisation et écarts de compétences croissants – ne peuvent être gérées uniquement par le recours à des ressources externes. Le renforcement des capacités internes constitue un investissement stratégique, et non une simple note de bas de page en matière de ressources humaines.

Le message est clair : la transformation ne consiste plus à adopter la technologie la plus récente, mais à se doter des moyens organisationnels nécessaires pour bien l'utiliser. Ceux qui comblent les écarts – entre les équipes, entre les priorités, entre la vision et l'exécution – transforment leurs investissements technologiques en avantages durables.

Profitez de cette 10e édition du Portrait TI et découvrez des conseils pratiques pour aider votre organisation à renforcer sa stratégie de TI.

Message du président

« Il y a dix ans, les études technologiques étaient surtout centrées sur les États-Unis, sans véritable focus sur le Canada. Le rapport Portrait TI de NOVIPRO a été créé pour aider les organisations canadiennes à comprendre l'impact de la technologie sur leurs activités. Aujourd'hui, une chose est claire : la technologie n'est plus le principal frein. Le véritable défi réside dans la capacité des organisations à s'y adapter. »

Chers lecteurs,

Cette 10e édition capture un moment à la fois d'opportunité et de tension. Les intentions d'investissement sont fortes. L'intelligence artificielle passe rapidement de l'expérimentation à l'exécution. L'infonuagique est devenue fondamentale. Pourtant, quel que soit le secteur ou la taille de l'organisation, le même schéma se dessine : l'ambition croît souvent plus vite que la capacité d'exécution.

Les tendances révèlent des écarts persistants : entre les équipes de TI et la haute direction, entre la confiance et la préparation, et entre le désir de transformation et les structures nécessaires pour réaliser cette transformation. Ces écarts ne sont pas le résultat d'une négligence ou d'une résistance aux changements; ils sont la conséquence naturelle de l'évolution plus rapide des technologies par rapport aux modèles organisationnels, aux compétences et à l'expertise, ainsi qu'aux cadres décisionnels. Combler ces écarts exige une planification et des actions réfléchies, et pas seulement des dépenses.

Cette édition du Portrait TI va au-delà de l'observation; elle lance un appel à l'action. Les données offrent plus qu'un aperçu des pratiques actuelles; elles révèlent où les frictions s'accumulent et où l'inaction comporte un risque réel. Qu'il s'agisse d'intelligence artificielle, d'infonuagique, de cybersécurité ou de talents, le message est le même : le progrès n'est pas lié aux outils eux-mêmes, mais à la manière dont ils sont utilisés dans le cadre de la stratégie de l'entreprise.

Chez NOVIPRO, nous le constatons tous les jours. Les organisations qui réussissent ne sont pas nécessairement celles qui disposent des technologies les plus avancées, mais plutôt celles qui bâtissent une compréhension commune entre la direction et les équipes techniques, qui investissent dans les compétences aussi délibérément qu'elles investissent dans les plateformes, et qui prennent des décisions technologiques comme des décisions d'affaires.

Pendant votre exploration du rapport Portrait TI 2026, je vous encourage à vous interroger sur les décisions et les investissements avisés qui propulseront la croissance de votre organisation. La prochaine phase de la transformation numérique ne sera pas définie uniquement par l'innovation, mais par la capacité à passer de l'intention à l'exécution.

Il aurait été impossible de produire le rapport Portrait TI sans le soutien de nos partenaires de longue date, IBM et Léger, qui nous accompagnent depuis dix ans, ainsi que des partenaires de cette année : Microsoft, A10 et Data Sentinel. Merci d'avoir contribué à la réalisation de cette publication.

ALAIN CORMIER
Président-directeur général

NOVIPRO

Un mot d'IBM

Chers lecteurs,

Le rythme de l'évolution technologique n'a jamais été aussi rapide ni aussi important qu'aujourd'hui. Partout au Canada, les organisations traversent une période de profonde transformation alors que les technologies numériques refaçonnent les industries, les modèles d'affaires et la nature même du travail. Ce qui était autrefois considéré comme une technologie émergente est maintenant devenu un fondement du fonctionnement, de la compétitivité et de la valeur ajoutée des organisations.

Je suis ravie de vous présenter la 10e édition du rapport Portrait TI, une collaboration entre IBM Canada et NOVIPRO. Au cours de la dernière décennie, ce rapport est devenu une référence précieuse pour comprendre comment les organisations canadiennes font évoluer leurs stratégies technologiques. Cette 10e édition constitue une occasion importante d'examiner les tendances qui marqueront la prochaine année, ainsi que de réfléchir à la transformation radicale du paysage des TI au cours des 10 dernières années.

La technologie est devenue un multiplicateur de force. Il y a 10 ans, de nombreuses organisations n'en étaient encore qu'aux premiers stades de l'adoption de l'infonuagique. Les stratégies de données commençaient tout juste à émerger, l'intelligence artificielle était en grande partie expérimentale, et la cybersécurité était souvent considérée comme une fonction spécialisée des TI plutôt que comme une priorité opérationnelle. Ces mêmes technologies sont maintenant au cœur de la stratégie d'entreprise. L'infonuagique hybride est devenu le pilier des environnements informatiques modernes. Les données sont devenues un actif essentiel de l'entreprise, et l'IA n'est plus testée : elle est mise en œuvre.

Parmi les tendances qui façonnent 2026, l'intelligence artificielle continue de s'imposer comme une force dominante. Les organisations vont plus loin que les preuves de concept et misent sur le déploiement de l'IA à grande échelle, en l'intégrant aux flux de travail, aux applications et aux processus de prise de décision. Le dialogue concernant l'IA s'est également approfondi. Les dirigeants se concentrent de plus en plus sur des façons de déployer l'IA de manière responsable, de l'administrer efficacement, et de s'assurer que les données et l'infrastructure sur lesquelles elle repose sont sûres et fiables.

La cybersécurité n'est plus une préoccupation d'arrière-plan : elle comporte un risque commercial important en raison de sa complexité, de sa sophistication et de l'ampleur des cyberattaques. L'indice X-Force Threat Intelligence Index de 2026 affiche une augmentation de la fréquence et de la sophistication des attaques pilotées par l'IA, qu'il s'agisse de rançongiciels, de violations de données ou de risques liés à la chaîne d'approvisionnement. À l'heure actuelle, la cyberrésilience ne consiste pas qu'à renforcer la défense, mais aussi à assurer la continuité des affaires, à protéger les données et à maintenir la confiance dans un contexte de menaces de plus en plus instable.

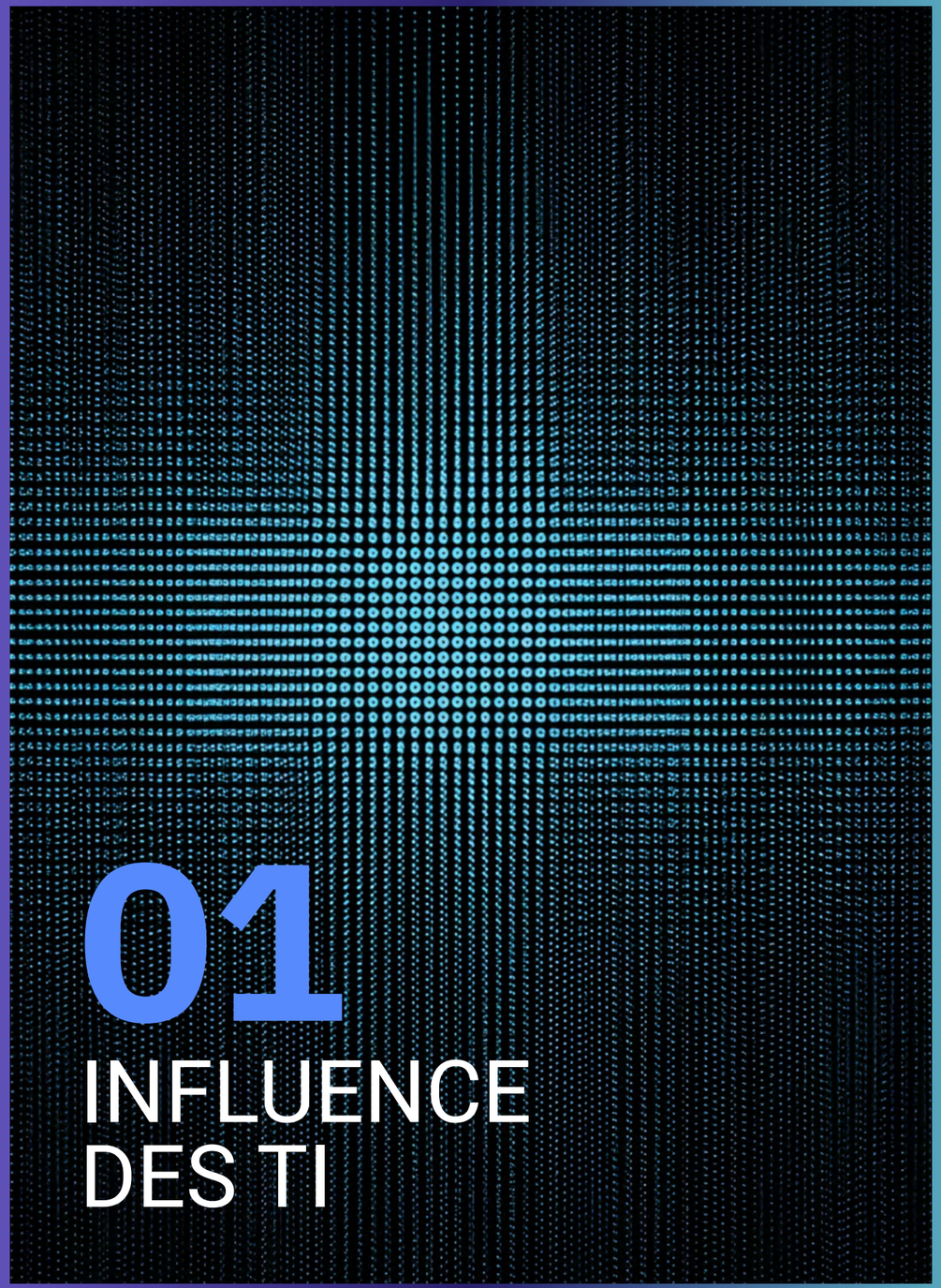
Tandis que les tensions géopolitiques s'exacerbent, la souveraineté des données est devenue un impératif stratégique. Le dialogue se poursuit au-delà de la résidence des données et s'articule autour de la gouvernance et du contrôle opérationnel. Les organisations canadiennes reconnaissent que le recours à des plateformes régies de l'extérieur peut entraîner des dépendances difficiles à gérer ou à éliminer. Pour atteindre la véritable souveraineté, il ne faut pas s'isoler, mais bien garder le contrôle, conserver le libre choix et éviter la fermeture. C'est pourquoi de nombreuses organisations adoptent des architectures ouvertes, hybrides et à infonuagiques multiples qui établissent un équilibre entre la flexibilité et la gouvernance sous contrôle canadien.

Le rapport de cette année présente également des points de vue d'acteurs de secteurs clés, tel que les services financiers, l'industrie manufacturière et les soins de santé, qui tirent activement profit de la technologie pour améliorer la productivité, accélérer l'innovation et obtenir de meilleurs résultats.

J'espère que les résultats de cette année vous aideront à élaborer votre propre stratégie technologique et qu'ils susciteront d'importantes discussions au sein de votre organisation. Le rythme de l'évolution technologique continuera sans doute de s'accroître, et les organisations auront encore plus d'occasions d'adopter l'innovation avec détermination et confiance.

DEB PIMENTEL
Présidente, IBM Canada

TABLE DES MATIÈRES



01
INFLUENCE DES TI

Dix ans plus tard, les TI ont tout changé. Dans dix ans, ce sera encore vrai.

En 2015, quand j'ai commencé à couvrir la transformation numérique des entreprises canadiennes, peu de gens auraient prédit l'ampleur de ce qui allait suivre. On parlait de « virage numérique » comme d'une option stratégique. Aujourd'hui, c'est une condition de survie.

Le secteur des TIC représente désormais 131,6 milliards de dollars, soit 5,8 % du PIB canadien, et a compté pour 19 % de la croissance économique entre 2019 et 2024. Ce ne sont plus des chiffres marginaux, mais ceux d'un pilier

L'impact sur l'emploi est tout aussi parlant. Chaque emploi direct dans les TIC en crée 1,1 ailleurs dans l'économie. Et les salaires suivent : plus de 103 000 dollars, soit près de 58 % au-dessus de la moyenne nationale. Mais la situation comporte des nuances. Au Québec, l'emploi des 15 à 29 ans en TI a reculé de 18 % entre 2022 et 2026. L'IA générative commence à se faire sentir, notamment sur les postes d'entrée.

L'essor technologique ne se limite pas au corridor Toronto-Montréal. La Colombie-Britannique compte plus de 12 000 entreprises et 182 000 travailleurs qualifiés, et Vancouver se classe au premier rang en Amérique du Nord pour la croissance de l'emploi technologique. Calgary affiche aussi une forte progression, avec plus de 60 % de croissance entre 2021 et 2024. L'Ouest canadien s'impose désormais comme un acteur clé de l'économie numérique.

Au Québec, l'enjeu reste particulier. La province regroupe plus d'un demi-million de travailleurs en technologie, soit environ un cinquième du total canadien. Mais le CTIC prévoit deux trajectoires d'ici 2030 : jusqu'à 196 400 nouveaux emplois dans le meilleur scénario, ou un léger déclin dans le pire. Tout dépendra des choix faits aujourd'hui.

Ottawa a commencé à agir. Le budget fédéral 2025 prévoit 925,6 millions de dollars sur cinq ans pour une infrastructure nationale en IA, incluant un nuage souverain canadien. Un signal concret, mais insuffisant sans règles claires, gouvernance solide et volonté politique.

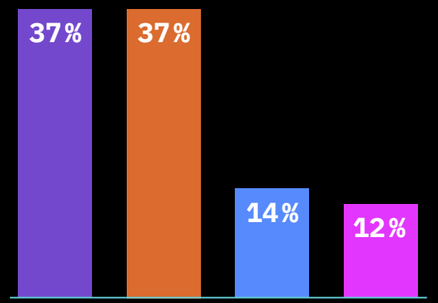
Après trente ans à observer cette industrie, un constat s'impose : la technologie n'est plus le cœur du débat. Le véritable enjeu, c'est notre capacité à nous adapter, à former la relève et à faire des choix courageux en matière de souveraineté numérique. Les TI ont transformé le Canada. Reste à voir si le Canada saura se transformer assez vite pour en tirer pleinement parti.

BRUNO GUGLIELMINETTI
Journaliste indépendant

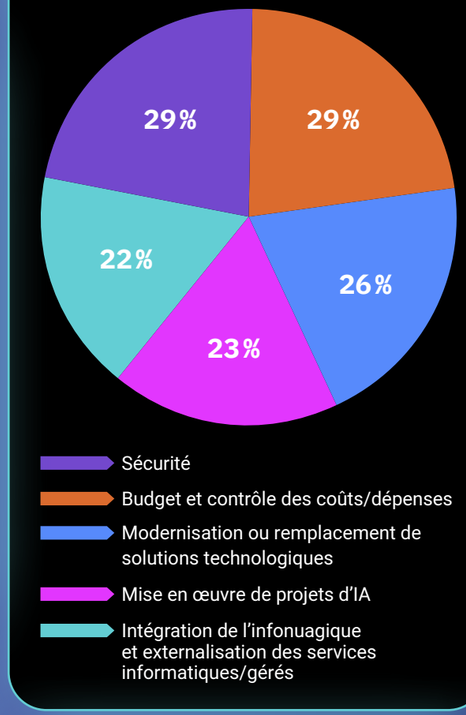
Bruno Guglielminetti est un journaliste québécois spécialisé dans les technologies et le numérique depuis plus de 30 ans. Basé à Montréal, il anime le podcast Mon Carnet, publie sur MonCarnet.com et présente le bulletin quotidien 120 secondes de Tech. Des productions qui rejoignent chaque semaine, plus d'un million et demi de francophones à travers la planète qui s'intéressent aux questions du numérique. Reconnu pour son talent de vulgarisateur, il intervient aussi régulièrement à la radio et à la télévision, au Québec comme en France, pour éclairer l'actualité technologique auprès d'un large public francophone.

TABLEAU DE BORD

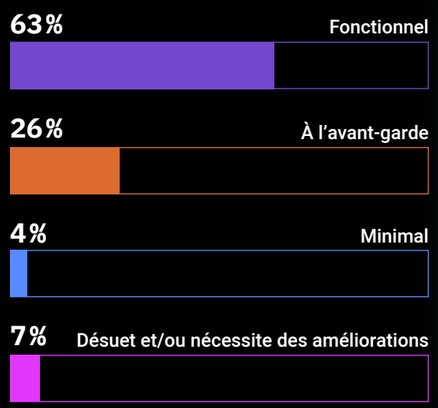
Perception des TI au sein des entreprises canadiennes :



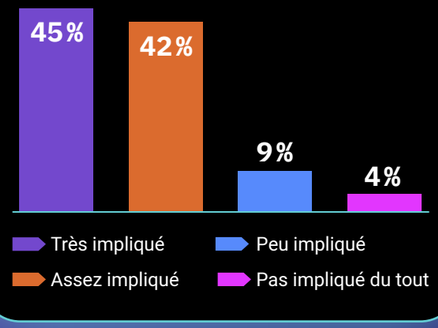
Les cinq principaux enjeux des entreprises canadiennes pour la prochaine année :



2/3 (63%) des organisations décrivent l'état de leur infrastructure TI comme «fonctionnel»



87% **des entreprises** impliquent leur service des TI dans la définition des stratégies de l'entreprise



« Bien que la cybersécurité se soit imposée comme le principal défi pour les entreprises pour la deuxième année consécutive, un écart subsiste entre cette préoccupation et les actions concrètes. Malgré son importance cruciale, la mise en œuvre de mesures tangibles peine encore à suivre le rythme de l'évolution des menaces. »

Alain Cormier, ***PDG, NOVIPRO***

Interprétation des données

LES TI SONT AU CŒUR DES DISCUSSIONS. MAIS LES PERSONNES IMPLIQUÉES SONT-ELLES D'ACCORD ?

Les organisations sont plus nombreuses que jamais à impliquer les TI dans la définition de la stratégie de l'entreprise – 87 % en 2026, contre 81 % l'année précédente. Mais l'inclusion formelle et la position stratégique réelle ne sont pas la même chose. Alors que 94 % des décideurs TI estiment qu'ils sont au cœur de la stratégie de l'entreprise, seuls 74 % des décideurs non-TI sont de cet avis, et les chiffres ne cessent de croître à partir de là. Parmi les dirigeants des départements autres que les TI, seuls 22 % considèrent les TI comme un partenaire stratégique. Près d'un quart d'entre eux les perçoivent comme une dépense.

Un total de 17 % les qualifient de mal nécessaire. Seuls 37 % les considèrent comme un investissement.

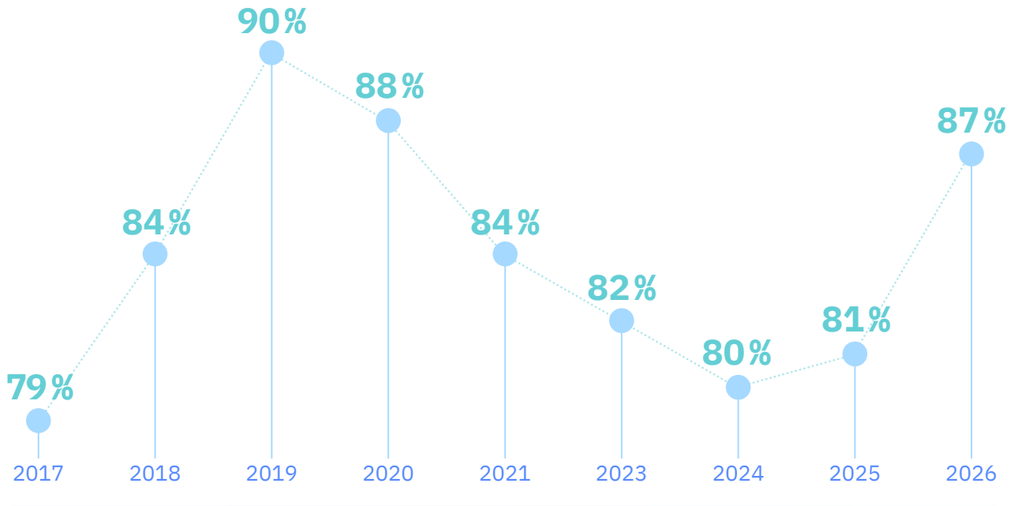
Cet écart a des conséquences réelles. Lorsque les TI sont consultées plutôt qu'intégrer, les considérations technologiques critiques arrivent trop tard pour influencer les décisions, ce qui ralentit la transformation, entraîne un sous-investissement et produit des stratégies dont l'exécution est bloquée. Pour combler cet écart, il faut formaliser le rôle des TI au moyen d'indicateurs clés de performance partagés, d'une participation systématique aux premières étapes de la prise de décision et de structures de gouvernance qui font de l'apport des TI une exigence plutôt qu'une simple courtoisie.

« L'influence des TI se mesure désormais à la capacité d'une organisation à intégrer les risques technologiques dans sa vision stratégique. Pourtant, on assiste à une banalisation des incidents qui freine l'élan de transformation. Le véritable effet des TI réside dans le maintien d'un sentiment d'urgence là où les entreprises ont naturellement tendance à accepter passivement les risques opérationnels. »

Randy Mckee, ***Directeur des ventes, A10 Networks***

Suivi des tendances

Implication des TI dans la stratégie de l'entreprise



Ces chiffres reflètent un problème plus tenace qu'un malentendu : des idées profondément ancrées au sein de l'organisation sur la raison d'être des TI. La part des entreprises qui considèrent les TI comme un véritable partenaire stratégique est passée de 31 % à 37 %, mais le rythme est lent par rapport à la rapidité avec laquelle la technologie elle-même évolue. Les suppositions culturelles formées au fil des décennies ne disparaissent pas simplement grâce à des organigrammes ou à la participation à des comités. Tant que les dirigeants non-TI n'auront pas pris conscience que les TI sont un moteur de la performance de l'entreprise plutôt qu'une simple fonction administrative, leur rôle restera plus symbolique que stratégique – et cela se traduira par une mauvaise allocation des ressources, un sous-investissement dans les technologies essentielles et une perte de terrain par rapport à la concurrence.

UN PAYSAGE AUX PRIORITÉS CHANGEANTES

La sécurité et le contrôle budgétaire sont à égalité en tant que premier défi commercial de 2026 (29 % chacun), la modernisation des TI arrivant juste derrière (26 %). Mais les dirigeants TI et les dirigeants non-TI ne voient pas le problème sous le même angle. Les dirigeants TI placent la sécurité au premier rang de leurs préoccupations, en raison de leur exposition directe aux menaces. Les dirigeants hors TI évoquent simultanément le contrôle budgétaire et la modernisation – des priorités qui vont dans des directions opposées. En l'absence d'un cadre commun, les organisations risquent de ne réussir ni l'un ni l'autre : les investissements se fragmentent, la prise de décision devient incohérente et l'organisation perd du terrain sur ces trois fronts.

« La conversation sur le CRM (plateforme de gestion de la relation client) est en grande partie derrière nous. Après des années de mise en œuvre réussie, notre attention s'est organiquement déplacée vers l'IA, et notre stratégie d'investissement reflète cette évolution. »

Danny Crevier, ***Directeur des services informatiques, Fonds de solidarité FTQ***

La voie à suivre est celle d'un cadre de priorisation qui évalue chaque défi par rapport à des objectifs commerciaux communs, plutôt que de les laisser se concurrencer en vase clos.

Cette divergence s'étend à la manière dont les organisations perçoivent leur propre position technologique. La plupart (63 %) décrivent leur infrastructure comme fonctionnelle, tandis qu'une sur quatre se considère à l'avant-garde, en particulier au Québec (39 %) et en Ontario (32 %). La proportion de personnes qualifiant leur infrastructure de minimale a fortement diminué, passant de 10 % à 4 %, ce qui est un signe encourageant. Pourtant, l'écart persiste : 32 % des dirigeants TI perçoivent leur infrastructure comme étant à l'avant-garde, comparativement à seulement 17 % des dirigeants non-TI. Lorsque les dirigeants ont des points de vue fondamentalement différents sur leur situation technologique, il devient très difficile de parvenir à un consensus sur les priorités et les investissements, ce qui se traduit par un ralentissement de la transformation et des occasions manquées.

COMBLER LE FOSSÉ : PERSPECTIVES TI VS NON-TI

Les dirigeants TI et ceux d'autres départements ne sont pas en désaccord. Ils ne tiennent même pas la même conversation.

Lorsqu'un dirigeant TI affirme qu'il est au cœur de la stratégie de l'entreprise, il entend qu'il contribue à définir l'orientation future de l'entreprise. Lorsqu'un dirigeant non-TI l'entend, il peut s'imaginer quelqu'un qui veille au bon fonctionnement des serveurs. Même salle, même organigramme – conversation complètement différente.

Il ne s'agit plus d'un problème d'intégration informatique, mais d'un problème d'organisation. Les TI sont la base sur laquelle reposent la résilience opérationnelle, la sécurité et l'avantage concurrentiel. Les dirigeants qui la considèrent comme un centre de coûts prennent une décision dont les conséquences s'étendent bien au-delà du secteur des TI. Formaliser le rôle des TI dans la gouvernance, aligner le budget sur la stratégie et placer la responsabilité au plus haut niveau – voilà par où commence le travail.

« Notre priorité actuelle est la cybersécurité, plus précisément, tester et sécuriser les outils d'intelligence artificielle avant un déploiement à plus grande échelle. Nous considérons la gestion des risques non pas comme une contrainte, mais comme un véritable levier de différenciation concurrentielle sur le marché. »

Alexandre Derégel, ***Directeur des technologies de l'information (TI), CDMV***

RISQUES

« INFORMEL » EST SYNONYME DE « JETABLE »

Lorsque la place des TI à la table de la stratégie reste informelle, elle devient facultative. Sans mécanismes définis pour la contribution des TI – points permanents à l'ordre du jour, séances d'information structurées, approbation explicite des décisions dépendant de la technologie – la participation devient superficielle, ce qui entraîne une prise de décision technologique critique trop tardive et des retards dans les projets en raison d'investissements mal hiérarchisés.

SI VOUS NE DÉFINISSEZ PAS LE RÔLE, QUELQU'UN D'AUTRE LE FERA

Si les dirigeants TI et les dirigeants non-TI ne travaillent pas à partir de la même définition de l'implication stratégique dans la pratique, l'écart se comble de lui-même – avec une duplication du travail entre les équipes, une confusion dans les responsabilités conduisant à des erreurs coûteuses, et une perte d'efficacité organisationnelle.

PERSONNE NE CRÉE DE CONSENSUS AUTOUR D'UN PROBLÈME QU'IL NE PENSE PAS AVOIR

Lorsque les dirigeants des départements autres que les TI ne partagent pas la compréhension des menaces par les TI – normalisant les risques de sécurité, sous-estimant les lacunes de l'infrastructure ou considérant la modernisation comme discrétionnaire – votre organisation passe d'une position proactive à une position réactive face aux cybermenaces, perdant ainsi la capacité d'agir rapidement en cas d'incidents de sécurité.

OPPORTUNITÉS

LA RÉUNION QUI CHANGE TOUT EST CELLE À LAQUELLE VOUS N'AVEZ PAS ENCORE PARTICIPÉ

La formalisation du rôle des TI dans la planification stratégique – et pas seulement dans l'approbation des projets – est le levier le plus puissant qu'un dirigeant TI puisse activer. Lorsque les TI sont intégrées aux cycles budgétaires et aux comités clés avant la prise de décisions, les priorités sont fixées correctement dès le départ.

PARLEZ LEUR LANGUE, OBTENEZ LEUR BUDGET

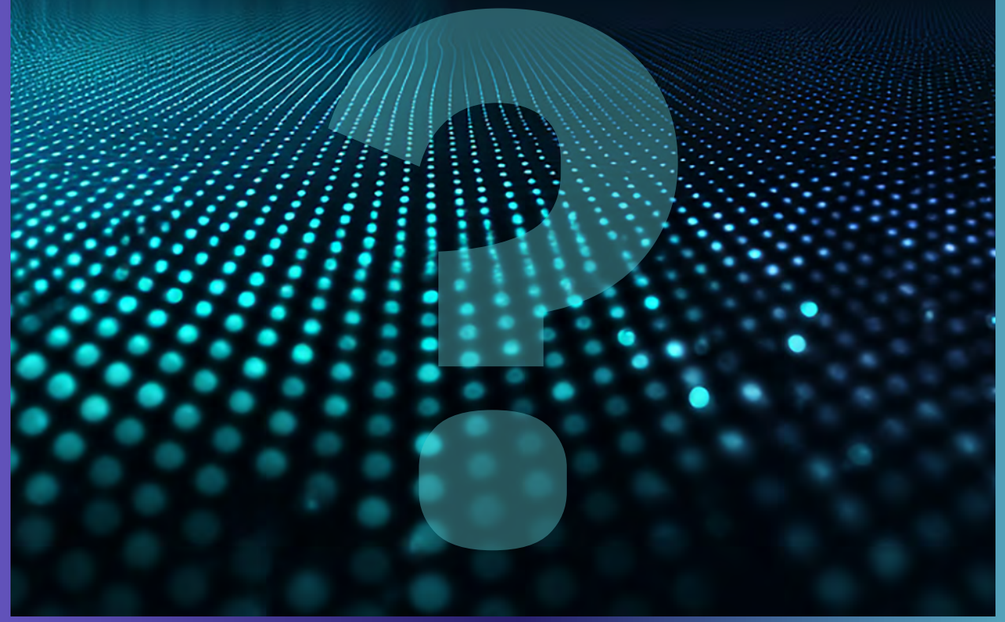
La migration vers l'infonuagique permet une prévisibilité des coûts. La révision de l'infrastructure permet une réduction des risques. Un investissement dans la sécurité permet une protection des revenus. Ce repositionnement n'est pas superficiel – il change qui écoute, qui défend l'initiative et qui signe le budget. Les dirigeants TI qui s'expriment en termes de résultats d'affaires ne se contentent pas de mieux communiquer, ils acquièrent une réelle influence.

FAITES DE LA SÉCURITÉ UNE CONVERSATION FINANCIÈRE

La cybersécurité n'est pas un coût technique, c'est un risque financier dont le prix est lié à l'inaction. Les dirigeants TI qui présentent la sécurité comme un enjeu de gestion des risques et de rentabilité de l'investissement accélèrent les décisions, améliorent la répartition du budget et transforment fondamentalement la position de l'organisation : d'un centre de coûts à un moteur de valeur. Ce changement commence par la manière de présenter les choses.

La grande QUESTION

Si votre organisation devait prendre demain une décision technologique critique – une décision ayant des conséquences financières, sécuritaires ou opérationnelles réelles – vos dirigeants TI et ceux des autres départements seraient-ils suffisamment alignés pour prendre la bonne décision ensemble ? Êtes-vous convaincu que cette décision soutiendra la trajectoire de votre entreprise à long terme ?



02
ENVIRONNEMENT ÉCONOMIQUE

2026 : le temps n’est plus à l’attente

Malgré un environnement économique incertain, marqué par des tensions géopolitiques persistantes, la prudence ne dicte plus systématiquement les décisions d’investissement des entreprises canadiennes. Dans un contexte de croissance modérée, de pressions sur les coûts et de pénurie de main-d’œuvre qualifiée, les investissements technologiques s’inscrivent désormais dans une logique à la fois défensive et stratégique. Les intentions de dépenses TI demeurent soutenues, signe que les organisations leur accordent une place croissante. Cette perception reste toutefois inégale : certains dirigeants y voient un moteur de croissance et de résilience, tandis que d’autres les considèrent encore comme un poste de dépenses à contrôler.

L’évolution des dix dernières années illustre ce changement. En 2018, les priorités visaient surtout les infrastructures, la cybersécurité, les services professionnels et l’analyse de données afin de consolider les fondations et optimiser les opérations.

En 2026, le portrait est différent. La cybersécurité demeure centrale, mais son poids relatif recule, reflétant sa normalisation comme composante ou risque inévitable. Les priorités se redéploient autour de deux leviers : l’infonuagique et l’intelligence artificielle.

Ce repositionnement traduit une transformation des mentalités. Là où les organisations privilégiaient le contrôle et l’hébergement interne, elles recherchent aujourd’hui rapidité d’exécution et capacité d’adaptation. Dans un environnement en évolution rapide, cette flexibilité devient un avantage concurrentiel clé.

L’infonuagique répond à cet impératif par son évolutivité et sa rapidité de déploiement, bien que ses bénéfices dépendent de la gouvernance. L’intelligence artificielle, quant à elle, dépasse l’expérimentation pour s’intégrer aux opérations, à la prise de décision, au service client et à l’automatisation. Ensemble, ces technologies redéfinissent la création de valeur.

Le message du marché canadien est clair : en 2026, attendre comporte plus de risques qu’agir. Les organisations qui retardent leur modernisation s’exposent à une perte d’efficacité, d’attractivité et d’innovation face à des concurrents plus agiles.

La question n’est plus de savoir s’il faut transformer l’entreprise, mais à quel rythme. Dans un marché en mouvement, l’avantage revient à celles capables de s’adapter rapidement. L’agilité devient une capacité organisationnelle essentielle.

GUS ISAAC
Président et chef de la direction, Nova Networks

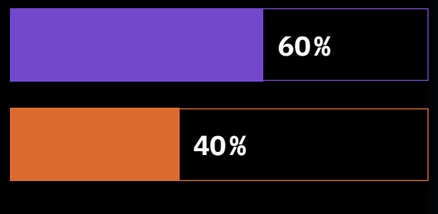
Gus Isaac est entrepreneur et investisseur, reconnu pour son approche pragmatique et sa rigueur financière. Propriétaire de Nova Networks, l’une des principales entreprises canadiennes en technologies de l’information depuis plus de 30 ans, il a bâti une organisation spécialisée dans la livraison de solutions TI complètes et sur mesure, allant du conseil stratégique à l’implantation.

Impliqué et orienté vers le concret, Gus se distingue par une vision axée sur la croissance durable et la performance. Son parcours reflète un équilibre entre esprit entrepreneurial et discipline d’investisseur, guidé par la création de valeur et l’excellence opérationnelle.

TABLEAU DE BORD

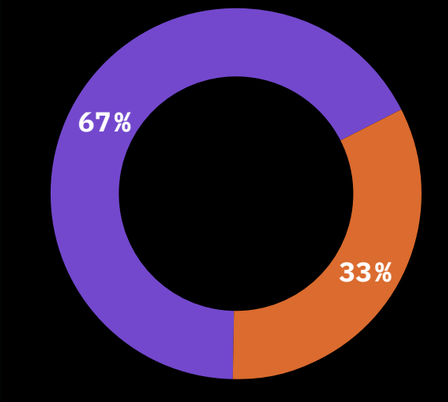
La majorité des entreprises prévoient conserver la propriété des équipements utilisateurs (**60%**), tandis qu'une part importante (**40%**) opte pour des services de gestion du cycle de vie

Au cours des deux prochaines années, prévoyez-vous d'être :



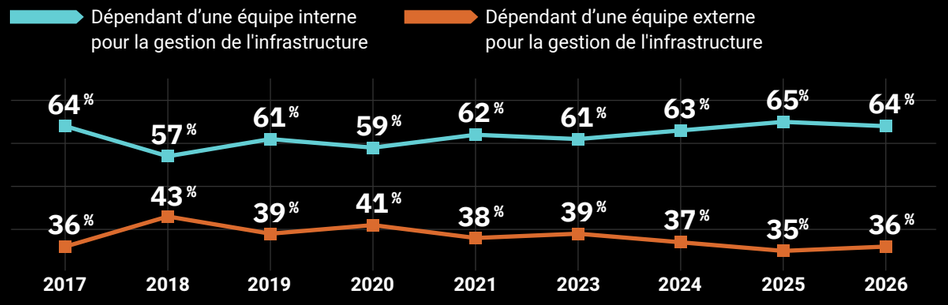
Quelle que soit leur taille, deux entreprises sur trois s'attendent à rester dépendantes d'équipes internes pour la gestion des équipements des utilisateurs

Au cours des deux prochaines années, prévoyez-vous d'être :

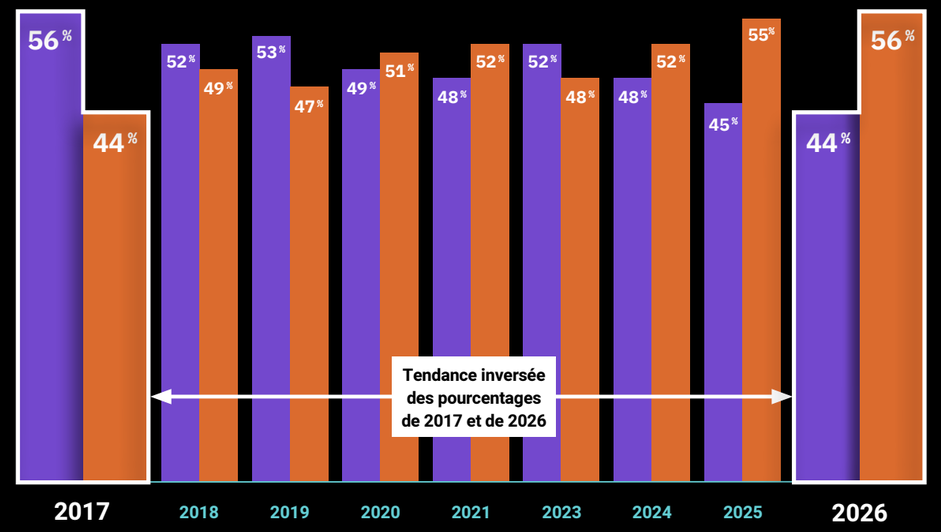


Deux tiers des organisations, s'attendent à rester dépendantes des équipes internes pour gérer l'infrastructure, une proportion inchangée par rapport à 2017 et qui est restée assez stable au cours de la dernière décennie

Au cours des deux prochaines années, pensez-vous être :



Au cours des dix dernières années, la propriété des technologies a évolué progressivement. En 2017, les entreprises conservaient **56%** de leur infrastructure en interne, contre **44%** dans l'infonuagique. En 2026, ces proportions se sont inversées.

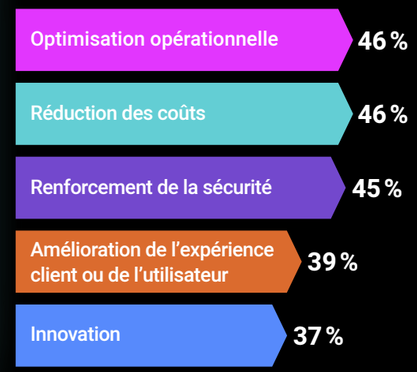


85% **des entreprises** prévoient de faire des investissements technologiques importants au cours des deux prochaines années

Les cinq principaux domaines d'investissement :

Intelligence artificielle et apprentissage automatique	33%
Solutions infonuagiques	31%
Solutions/services de cybersécurité	29%
Modernisation des applications	26%
Solutions d'infrastructure	25%

Les cinq principaux objectifs des investissements technologiques :



Interprétation des données

Prenons le cas d'une entreprise qui investit massivement dans une migration vers l'infonuagique, déploie une nouvelle plateforme de données et commence à piloter de nouveaux outils d'IA, le tout au cours du même exercice financier. Douze mois plus tard, l'infrastructure est en place, mais l'adoption est inégale, la plateforme de données n'est pas intégrée aux systèmes que les gens utilisent réellement, et le projet pilote d'IA est bloqué dans l'attente d'un cadre de gouvernance que personne ne possède.

La technologie a fonctionné, mais pas la stratégie. C'est exactement le scénario auquel sont confrontées les entreprises du Canada : elles sont prêtes à investir des sommes importantes dans la technologie, mais elles manquent de concentration et d'engagement pour aligner ces priorités sur des objectifs commerciaux plus larges. Cela signifie qu'elles risquent de voir leurs investissements technologiques gaspillés dans des solutions qui ne permettront pas de progresser ou d'améliorer les résultats.

Soutien informatique interne ou externe

La plupart des entreprises ont l'intention de conserver la responsabilité de la gestion de l'infrastructure à l'interne au cours des deux prochaines années (64 %), même si elles délaissent les équipements qu'elles possèdent au profit des solutions infonuagiques. Cela porte à croire qu'en ce qui concerne l'infrastructure logicielle, les entreprises accordent une certaine valeur aux connaissances particulières qu'une équipe TI interne peut appliquer à son travail, même lorsque cette infrastructure est hébergée à l'externe.

En ce qui concerne l'équipement des utilisateurs, les entreprises se tournent encore plus vers les capacités internes : 60 % s'attendent à rester propriétaires de l'équipement de l'utilisateur et 67 % à dépendre d'équipes internes pour la maintenance de cet équipement.

Cela peut exposer les entreprises à un certain degré de risque.

Les équipements possédés vieillissent rapidement et deviennent défaillants, devenant ainsi un passif plutôt qu'un actif; le recours à un service de gestion externe a un prix, mais permet d'atténuer ce risque. Cela ne signifie pas qu'une équipe TI interne ne sert à rien, mais plutôt que les entreprises doivent faire un choix conscient et structuré quant à la manière dont les ressources internes et externes sont utilisées et équilibrées. Avec du recul, les organisations peuvent constater que l'expertise de leurs ressources internes est mieux déployée dans la stratégie, la gestion et les situations où la rapidité d'exécution est la plus critique, tandis que les ressources externes peuvent fournir un soutien significatif qui complète leurs équipes, plutôt que de leur faire concurrence.

« Bien que nous soyons trop petits pour justifier une ressource dédiée à plein temps, nous avons choisi de conserver la majorité de nos opérations à l'interne. Garder le contrôle de nos données, gérer plus efficacement les coûts de licence et garder la maîtrise de notre infrastructure sont des priorités qu'une approche sur site nous permet tout simplement de mieux réaliser. »

Don Bower, ***Chef d'équipe réseau, Vision Extrusions***

VOLONTÉ DE DÉPENSER

Un budget technologique plus important n'est un avantage que si l'organisation sait ce qu'elle essaie d'accomplir et si elle alloue les ressources de manière appropriée pour atteindre ses objectifs.

Alors que 85 % des organisations canadiennes prévoient des investissements technologiques importants au cours des deux prochaines années – principalement en IA (33 %), infonuagique (31 %) et en solutions de sécurité (29 %), la volonté de dépenser est clairement présente. Toutefois, lorsque les objectifs relatifs aux dépenses sont définis de manière trop générale, sans hiérarchisation claire, aucun investissement ne bénéficie de l'attention soutenue nécessaire pour produire des résultats significatifs. L'effet cumulé est un portefeuille d'engagements partiels qui, collectivement, sous-performent.

Les objectifs qui motivent ces investissements – l'optimisation opérationnelle et la réduction des coûts (46 % chacun), suivis de près par le renforcement de la sécurité (45 %) – sont des objectifs valables, mais ils sont également suffisamment larges pour justifier presque n'importe quelle décision de dépense. Les organisations ont besoin d'un cadre structuré qui ne se contente pas de définir des priorités, mais qui leur permet de les évaluer et de prendre des décisions lorsque des compromis sont nécessaires. La mesure n'est pas négociable : en l'absence d'indicateurs de performances clés qui relient les investissements technologiques à des résultats commerciaux concrets, les organisations perdent la capacité de distinguer ce qui fonctionne de ce qui ne fait que ressembler à des progrès.

PRIORITÉS MAL ALIGNÉES ET ÉCART DÉCISIONNEL

Même les dépenses les mieux intentionnées peuvent rater la cible lorsque les priorités qui les motivent ne sont pas ancrées dans une stratégie d'entreprise commune. Nulle part ce risque de désalignement n'est plus évident que dans les différences de perception entre les décideurs TI et les dirigeants hors TI. On observe d'ailleurs un écart dans leurs intentions d'investissement. Ce désalignement crée un potentiel de conflit réel en l'absence d'un cadre pour orienter les décisions d'investissement technologique.

COMBLER LE FOSSÉ : PERSPECTIVES TI VS NON-TI

Principales différences en matière d'investissement entre les décideurs TI et les dirigeants d'autres départements

Investissements dans les deux prochaines années	Décideurs TI	Dirigeants non-TI
Solutions infonuagiques	36 %	21 %
Modernisation des applications	28 %	16 %
Analyse avancée des données	28 %	13 %
Gestion des relations avec la clientèle	17 %	26 %
Aucun investissement prévu	6 %	24 %

Lorsque les responsables de la stratégie technologique et ceux qui contrôlent les budgets partent d'hypothèses différentes sur les besoins des deux prochaines années, les décisions de dépenses se fondent sur des pressions départementales concurrentes plutôt que sur une orientation organisationnelle cohérente. Les données montrent que les décideurs TI sont nettement plus enclins à planifier des investissements technologiques majeurs dans des domaines comme l'infonuagique, la modernisation et l'analyse de données avancée que leurs homologues non-TI, tandis que les dirigeants non-TI sont près de quatre fois plus susceptibles de ne prévoir aucun investissement majeur (24 % contre 6 %).

Un cadre commun d'évaluation des priorités informatiques par rapport aux résultats de l'entreprise – qui relie les décisions d'investissement aux objectifs sur lesquels les deux groupes s'entendent déjà, comme la réduction des coûts, la sécurité et l'efficacité opérationnelle – donne aux organisations le point d'ancrage nécessaire pour prendre des décisions ciblées et défendables plutôt que des choix réactifs. Tout investissement implique des compromis; l'essentiel est de s'assurer que ces choix sont mûrement réfléchis et pesés.

Automatisation et productivité

L'infonuagique et les solutions de sécurité arrivent juste derrière l'intelligence artificielle parmi les domaines les plus fréquemment ciblés par les investissements technologiques prévus.

	2026	2025	2024	2023	2021	2020	2019	2018	2017
Solutions de sécurité (ex : gouvernance, logiciels, formations, audits, etc.)	**29%** ↑	23%	29%	17%	25%	25%	42%	40%	N/A
Solutions infonuagiques	31%	29%	28%	14%	34%	38%	N/A	N/A	N/A
Intelligence artificielle (ex : Apprentissage automatique, apprentissage profond, etc.)	33%	30%	25%	13%	18%	N/A	na	na	na
Solutions d'affaires (ex : ERP 10 %, CRM 17 %, etc.)	**34%** ↑	27%	23%	16%	17%	25%	37%	36%	43%
Solutions d'infrastructures (ex : matérielles et logicielles)	25%	21%	22%	19%	21%	28%	40%	43%	52%
Services professionnels (ex : consultation, implantation, etc.)	**20%** ↑	14%	19%	14%	15%	21%	34%	24%	39%
Analyse de données avancées (ex : Apprentissage automatique, apprentissage profond, etc.)	**25%** ↑	15%	17%	13%	18%	29%	36%	34%	23%
Solutions de modernisation d'applications (ex. : automatisation, conteneurisation, orchestration, etc.)	**26%** ↑	19%	17%	12%	19%	N/A	N/A	N/A	N/A
Informatique en périphérie de réseau (ex : monitorage à distance, smart grid, cloud gaming, gestion de trafic, etc.)	15%	11%	15%	9%	N/A	N/A	N/A	N/A	N/A
Internet des objets (IoT)	13%	11%	14%	7%	14%	20%	N/A	N/A	N/A
Technologie 5G	13%	10%	14%	7%	12%	N/A	N/A	N/A	N/A
Commerce en ligne	9%	11%	14%	6%	11%	18%	N/A	N/A	N/A
Non, je ne compte pas faire des investissements importants dans les deux prochaines années	10%	12%	13%	14%	12%	8%	2%	6%	7%
Technologies propres (qui aident à réduire les impacts environnementaux)	9%	7%	11%	7%	N/A	N/A	N/A	N/A	N/A
Technologie chaîne de blocs	8%	6%	10%	4%	8%	11%	23%	22%	N/A
Service de gestion du cycle de vie des équipements utilisateur	13%	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Réalité étendue (ex : Metavers, réalité augmentée, réalité virtuelle, etc.)	7%	7%	7%	3%	N/A	N/A	N/A	N/A	N/A
Solutions de reconnaissance vocale et faciale	6%	4%	6%	5%	5%	10%	N/A	N/A	N/A

« Nous constatons une forte évolution vers les modèles d'abonnement et de paiement à l'utilisation, même pour le matériel. Les organisations recherchent une plus grande flexibilité financière, mais aussi une meilleure prévisibilité des coûts, tout en réduisant la complexité de la gestion des actifs. Cette évolution reflète un changement plus large dans la façon dont les entreprises consomment la technologie en tant que service aligné sur leurs besoins opérationnels. »

Gus Isaac, ***Président et chef de la direction, Nova Networks***

La recherche de l'alignement nécessitera des concessions. Les entreprises accordent une grande importance à l'expertise des équipes TI. Deux entreprises sur trois (64 %) prévoient qu'elles continueront à dépendre d'équipes internes pour la gestion de leur infrastructure dans un avenir prévisible. Plusieurs raisons expliquent cette protection des ressources TI internes : un marché du travail tendu, la volonté de garder le contrôle et la souveraineté des données, ainsi que les retards potentiels liés au recours à des ressources externes. Pour de nombreuses applications, il est extrêmement utile de disposer d'une ressource interne connaissant le contexte commercial et capable d'effectuer le travail rapidement, mais cela ne signifie pas pour autant qu'il faille renoncer totalement aux ressources externes. Le défi consiste à trouver un équilibre entre les ressources internes et externes, un équilibre qui correspond aux réalités actuelles et aux objectifs futurs de l'organisation.

Pour leur part, les équipes TI doivent comprendre suffisamment bien les objectifs de l'entreprise pour formuler des recommandations qui permettront aux autres d'obtenir un bon rendement.

Par ailleurs, les dirigeants doivent faire confiance à leurs équipes TI pour jouer un rôle de premier plan dans les décisions d'investissement technologique. Le service TI ne peut pas agir sur la base de simples directives, il doit être impliqué dans des conversations stratégiques, afin que des technologies telles que les solutions infonuagiques, l'IA et les mises à niveau relatives à la sécurité puissent être incorporées de manière réfléchie. Une équipe TI qui comprend vraiment où l'organisation veut aller peut positionner la technologie là où elle sera la plus efficace, au bon moment.

Suivi des tendances : L'évolution vers l'infonuagique

En 2026, les entreprises prévoient que, d'ici deux ans, plus de la moitié de leur infrastructure (56 %) sera hébergée dans l'infonuagique, les 44 % restants étant des équipements appartenant à l'entreprise. En 2017, lorsque ce rapport a été publié pour la première fois, ces chiffres étaient inversés (44 % pour l'infonuagique, 56% pour les équipements appartenant à l'entreprise), et la tendance semble s'être accélérée depuis 2024. Bien que cette évolution soit en partie due au développement rapide des solutions infonuagiques au cours des dernières années, il ne s'agit pas d'un simple remplacement. Les modèles hybrides deviennent l'approche dominante, car les organisations apprennent à conserver les avantages de la technologie sur place là où elle est nécessaire, tout en profitant de la flexibilité, de l'évolutivité et de l'innovation que les solutions infonuagiques peuvent apporter dans certaines applications.

RISQUES

QUAND LA RAPIDITÉ DE L'INVESTISSEMENT DÉPASSE CELLE DE L'ADOPTION

Déployer simultanément des plateformes infonuagiques, d'IA et de données, sans gouvernance, plans d'intégration ou attribution des responsabilités, mène inévitablement ces initiatives à l'échec. Le résultat : des plateformes sous-utilisées, un rendement du capital investi (RCI) retardé et un scepticisme croissant à l'égard des investissements futurs, ce qui rend plus difficile l'obtention de l'adhésion pour la suite.

S'ENGAGER À TOUT, NE RIEN LIVRER

Lorsque des priorités telles que « l'optimisation » sont suffisamment larges pour justifier n'importe quelle initiative, tout va de l'avant, et rien ne reçoit l'attention nécessaire. La dispersion des investissements se traduit par des projets qui se disputent le temps et les ressources et qui finissent par produire des résultats médiocres en dépit d'un budget élevé.

MANQUER D'HARMONIE

Lorsque les dirigeants TI et non-TI ne partent pas des mêmes hypothèses en matière d'urgence et de priorités, les décisions d'investissement se fragmentent. Les détenteurs de budget et les dirigeants TI finissent par tirer dans des directions différentes, ce qui se traduit par des décisions retardées, des dépenses mal réparties et des choix technologiques qui ne soutiennent pas les résultats à long terme de l'entreprise.

OPPORTUNITÉS

ÉCHELONNER LES INVESTISSEMENTS AU LIEU DE LES EMPILER

L'échelonnement des initiatives/investissements en fonction des dépendances – la gouvernance avant l'IA, l'intégration avant la mise à l'échelle – accélère le délai de rentabilité et favorise une adoption plus forte que si on lançait tout en même temps. Les organisations qui définissent des phases d'investissement claires, ainsi que des critères d'appropriation et de réussite pour chaque phase, sont plus susceptibles de convertir l'investissement en résultats mesurables.

ASSOCIER CHAQUE INVESTISSEMENT À UN RÉSULTAT COMMERCIAL

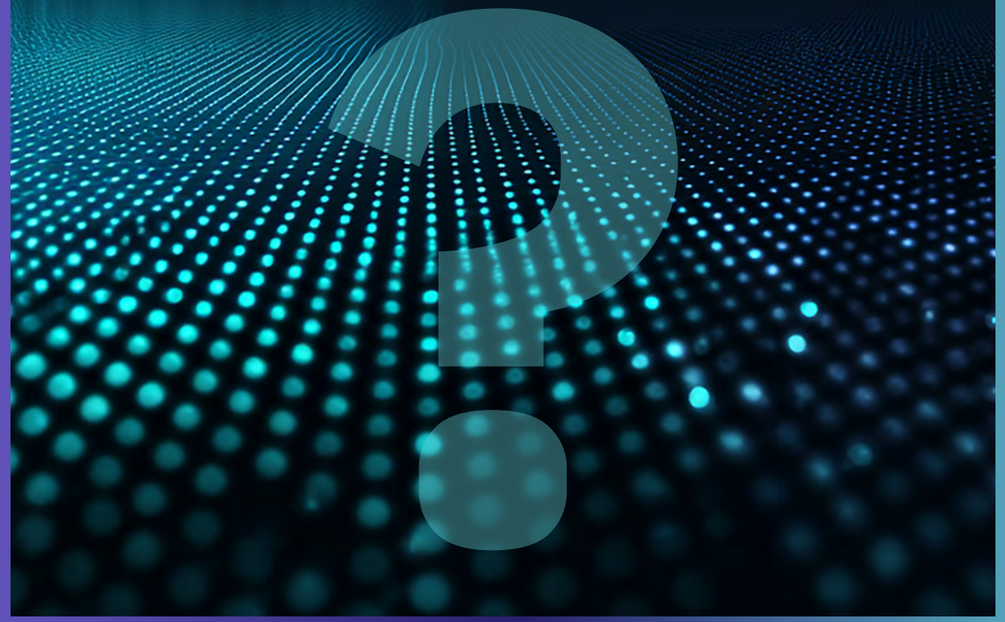
La transition des décisions basées sur la technologie à des cadres d'investissement axés sur les résultats est ce qui permet aux organisations chefs de file de prendre de l'avance. Lorsque chaque initiative est liée à une incidence commerciale mesurable (par exemple la réduction des coûts, l'atténuation des risques ou l'augmentation des revenus), il devient plus facile d'établir des priorités, de faire des arbitrages et de démontrer le RCI. La valeur de vos investissements sera basée sur leur incidence, et non sur la perception.

FAIRE DU SERVICE TI LE CO-PROPRIÉTAIRE DE LA STRATÉGIE D'INVESTISSEMENT

Les organisations qui tirent pleinement parti des TI vont au-delà de l'exécution, en positionnant les dirigeants TI en tant que partenaires pour décider où investir, quand et pourquoi. L'intégration des TI dans la planification initiale, les discussions budgétaires et la gouvernance des investissements permet une meilleure allocation des capitaux, une réduction des risques et des décisions technologiques qui soutiennent directement la stratégie à long terme de l'entreprise.

La grande QUESTION

Investissez-vous dans la technologie pour avoir une incidence ou simplement pour agir ? Vos équipes TI participent-elles pleinement à l'élaboration des décisions et disposez-vous d'un cadre de mesure pour savoir ce qui fonctionne vraiment ? Si la réponse est « ce n'est pas clair », il faudrait régler cela avant le prochain cycle budgétaire.



03
INTELLIGENCE ARTIFICIELLE

Intelligence artificielle : de l'expérimentation à l'intégration

L'intelligence artificielle a atteint un tournant décisif. Autrefois considérée comme une technologie émergente, elle est désormais un moteur essentiel du fonctionnement, de la compétitivité et de la croissance des organisations. En 2026, le débat ne porte plus sur l'opportunité d'adopter l'IA, mais sur une question bien plus importante : **comment intégrer l'IA de manière responsable, sécurisée et à grande échelle afin d'apporter une réelle valeur ajoutée aux entreprises.**

Dans tous les secteurs d'activité, les entreprises passent d'expérimentations ponctuelles à une intégration réfléchie et stratégique. L'IA n'est plus confinée aux équipes techniques ou aux laboratoires d'innovation. Elle est désormais intégrée aux flux de travail quotidiens, aux processus décisionnels et aux interactions avec les clients. Cette évolution nécessite plus que de nouveaux outils. Elle exige une stratégie claire, une harmonisation entre les différents niveaux de direction et une volonté de repenser la manière dont le travail est effectué à l'échelle de l'entreprise.

LA CONFIANCE EST LE FONDEMENT DE L'IA ÉVOLUTIVE

À mesure que l'IA s'intègre plus profondément dans les opérations d'affaires, la confiance s'impose comme le facteur déterminant de la réussite. Les organisations doivent avoir confiance dans les données qui alimentent leurs modèles, dans la transparence des résultats qu'ils génèrent et dans la sécurité des environnements dans lesquels ils fonctionnent.

Cette confiance est de plus en plus renforcée par une forte observabilité. Cela signifie une visibilité continue sur le comportement des systèmes d'IA en production, sur la manière dont les décisions sont prises et sur les situations où les résultats s'écartent des normes attendues. Sans une telle visibilité, les risques peuvent passer inaperçus à mesure que l'IA évolue, ce qui freine à la fois la confiance dans cette technologie et son adoption.

La confiance ne repose pas sur un simple point de contrôle; elle doit être construite tout au long du cycle de vie de l'IA, de la gouvernance des données et du développement des modèles jusqu'au déploiement et à la surveillance continue.

LEANNE CLARKE
Directrice des ventes de l'écosystème, IBM Canada

Leanne Clarke est responsable des ventes écosystémiques chez IBM Canada, où elle développe des partenariats stratégiques pour accélérer l'innovation. Forte de plus de 25 ans d'expérience au sein d'IBM, notamment comme CFO, elle possède une expertise approfondie en finance, transformation des talents et création de valeur par la technologie. Elle est également CPA, CMA et engagée dans des initiatives communautaires et de leadership.

Lorsque la confiance est établie, les capacités de l'IA peuvent passer du simple soutien pour des tâches individuelles à la prise de décisions plus intelligentes, plus rapides et plus cohérentes à grande échelle. Sans cette confiance, même les capacités les plus avancées peinent à dépasser le stade de l'expérimentation.

L'IA COMME LEVIER DE TRANSFORMATION DES MODÈLES OPÉRATIONNELS

La véritable valeur de l'IA ne réside pas uniquement dans l'automatisation, mais dans la transformation. Les organisations de premier plan utilisent l'IA pour renforcer l'expertise humaine, rationaliser des processus complexes et créer des boucles de rétroaction qui permettent à l'entreprise d'apprendre et de s'adapter en temps réel. Cela représente un changement fondamental dans les modèles opérationnels, qui exige de repenser les processus, d'améliorer les compétences des équipes et de favoriser la collaboration entre les dirigeants, les services des TI et les spécialistes des données.

Le succès repose sur l'alignement. Lorsque les dirigeants et les équipes techniques partagent la responsabilité des stratégies d'IA, les organisations peuvent avancer plus rapidement et avec confiance, en évitant le piège courant des initiatives déconnectées qui ne se développent jamais à grande échelle.

DE L'ANALYSE À L'ACTION

Le Portrait TI 2026 est clair : l'IA est devenue un impératif opérationnel. Les organisations qui se démarqueront dans les années à venir ne sont pas celles qui multiplient les projets pilotes, mais celles qui passent à l'action avec détermination en investissant dans leur personnel, en mettant en place une gouvernance solide et en intégrant l'IA au cœur de leurs activités.

Le moment est venu de passer de l'exploration à l'exécution, et de l'expérimentation aux résultats concrets. En fondant leurs initiatives d'IA sur la confiance, en assurant l'alignement entre la direction et le service des TI, et en misant sur une intégration significative, les organisations peuvent libérer tout le potentiel de l'IA et jeter les bases d'un succès à long terme.

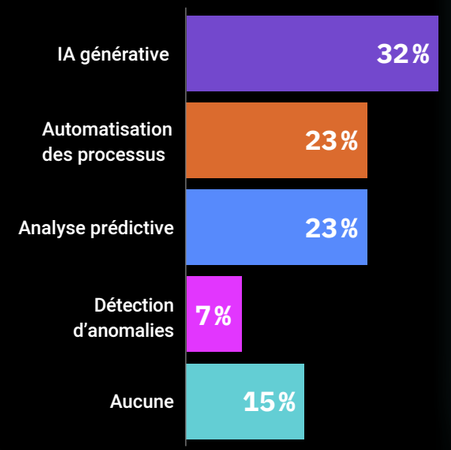
TABLEAU DE BORD

38 % **Plus d'un tiers des organisations** ont progressé dans leur parcours vers l'IA, passant de la phase d'expérimentation à celle de l'intégration

Le parcours d'intégration de l'IA :

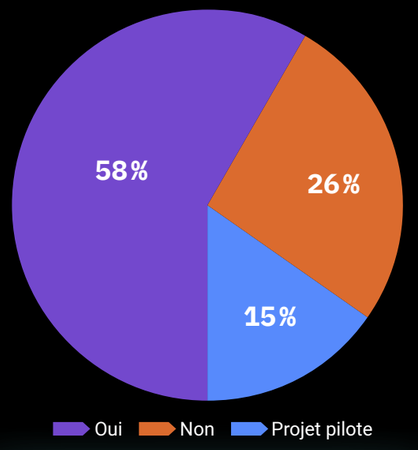
Aucune utilisation notable de l'IA	20 %
Expérimentation de l'IA via des projets pilotes isolés	42 %
Déploiement de l'IA dans plusieurs fonctions	21 %
L'IA est intégrée dans la plupart des activités	13 %
L'IA est au cœur du modèle d'entreprise	4 %

Types de solutions d'IA actuellement utilisées ou envisagées



L'utilisation de l'IA a franchi le seuil de la majorité en 2026, avec **58 %** des entreprises utilisant des solutions d'IA

Utilisation de solutions d'intelligence artificielle :



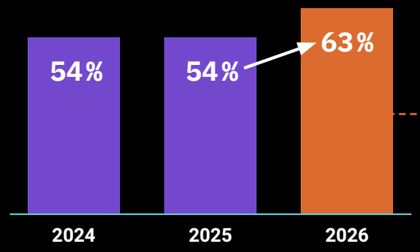
91 % **des organisations** utilisent les données pour éclairer leurs décisions d'affaires

Les données sont utilisées pour prendre des décisions dans les domaines suivants :

Opérations	52 %
Développement de produits ou de services	44 %
Finances	38 %
Soutien pour les demandes de renseignements officielles, les demandes d'information et les rapports de responsabilisation	37 %
Ventes	34 %
Marketing	33 %
Chaîne d'approvisionnement	25 %
Autre	1 %

Parmi les entreprises qui prévoient d'investir dans des services professionnels ou dans l'analyse avancée des données, l'analyse statistique avancée est la solution la plus couramment envisagée, avec une augmentation considérable par rapport aux années précédentes.

Pourcentage (%) des entreprises prévoyant de mettre en œuvre l'analyse statistique avancée*



Mises en œuvre prévues*

Analyse statistique avancée	63 %
Visualisation des données	54 %
Analyse par apprentissage profond	44 %
Analyse par apprentissage automatique	39 %
Analyse statistique de base	39 %

*Parmi les entreprises qui prévoient d'investir dans des services professionnels ou l'analyse avancée des données.

Interprétation des données

LE PARCOURS DE L'IA

Les promesses initiales de l'intelligence artificielle (IA) ont cédé la place à des solutions plus précises et plus abouties, permettant aux entreprises de dépasser le simple dilemme de l'adoption (oui ou non) pour s'engager dans une véritable intégration. En 2026, les entreprises devront intégrer l'IA dans leurs stratégies commerciales afin de conserver un avantage concurrentiel.

Cela implique de préparer minutieusement les équipes, d'investir dans le développement des compétences et d'agir avec détermination au-delà des projets pilotes et exploiter pleinement le potentiel des solutions d'IA. Les entreprises freinées par l'incertitude et la prudence se retrouveront à la traîne alors que cette technologie révolutionne rapidement le paysage commercial.

« Aujourd'hui, chaque investissement dans l'IA est évalué en fonction du RCI, mais nous assistons également à une évolution rapide de la maturité des organisations : certaines en sont encore à l'expérimentation, tandis que d'autres déploient déjà l'IA à grande échelle et l'intègrent au cœur de leurs opérations. Cette évolution confirme que l'IA est en train de devenir un véritable levier de transformation, capable d'accélérer la prise de décision, d'optimiser les processus et de redéfinir les modèles économiques. »

Gregory Denniel, ***Directeur de pratique en matière d'IA & Analytique, NOVIPRO***

Pour les organisations moins avancées dans leur parcours d'adoption de l'IA, le rythme effréné de son développement exerce une pression considérable sur les équipes TI, créant des tensions croissantes entre les dirigeants et les équipes des TI chargées de concrétiser les solutions d'IA dans la pratique. Les entreprises capables de doter leurs équipes TI, des effectifs et des moyens nécessaires pour suivre ce rythme bénéficieront d'un avantage stratégique.

Quelle que soit la position d'une organisation sur la voie de l'intégration, le message pour 2026 est clair : **les progrès en matière d'IA ne se résument plus à une simple adoption, mais consistent à maîtriser les compétences, à personnaliser et à intégrer les outils d'IA afin de tirer pleinement parti des avantages qu'ils peuvent apporter.**

DÉPLOIEMENT DE L'IA EN 2026

Une entreprise sur trois (32 %) utilise des solutions d'IA générative, mais il ne s'agit pas de la seule option disponible, et elle n'est pas toujours exploitée à son plein potentiel. Si les outils de type clavardage grand public sont déjà largement utilisés pour des tâches simples telles que la traduction, la relecture et la rédaction de courriels, ces plateformes peuvent en réalité prendre en charge des tâches bien plus vastes et complexes. Une formation à l'échelle de l'organisation est essentielle pour aider les équipes à comprendre les capacités de l'IA générative et à l'utiliser efficacement.

Les entreprises doivent également envisager des outils basés sur l'IA au-delà des agents conversationnels. D'autres solutions, telles que l'automatisation des processus (23 %) et l'analyse prédictive (23 %), sont déjà bien implantées parmi les entreprises canadiennes, en particulier celles opérant à plus grande échelle. La détection des anomalies est moins répandue (7 %), mais son utilisation devrait croître rapidement à mesure que les organisations intensifient leurs investissements et le développement des compétences.

L'un des risques liés à l'intégration de l'IA réside dans la possibilité d'erreurs coûteuses. C'est pourquoi certaines organisations freinent leurs efforts de développement en matière d'IA : les exemples très médiatisés d'erreurs liées à l'IA suscitent, à juste titre, une certaine hésitation. Cependant, atténuer les risques ne doit pas signifier y renoncer : celle-ci doit être déployée à partir de données précises et bien structurées, et dans le cadre de processus soigneusement gérés.

Une fois encore, le développement des compétences est essentiel, et cela ne se limite pas aux équipes TI. Le personnel qui utilisent ces outils doivent être en mesure de développer leur expertise et leur aisance. Par ailleurs, les organisations doivent s'engager à mettre en place des pratiques de gestion permettant d'assurer à la fois la qualité des données d'entrée et celle des résultats produits.

La question de la réglementation

Alors que les entreprises s'efforcent de suivre le rythme des avancées technologiques en matière d'IA, les gouvernements cherchent eux aussi à en comprendre l'incidence. Ils doivent trouver un équilibre entre la demande de réglementation et la nécessité de favoriser l'innovation et la croissance économique, tout en reconnaissant que cette technologie évolue à une vitesse fulgurante.

Il est donc difficile de prédire l'orientation que prendront les décisions réglementaires; les organisations doivent donc se préparer à différents scénarios.

Il est essentiel de surveiller de près des enjeux tels que :

- la protection des données
- les biais algorithmiques
- la responsabilité en matière de décisions automatisées
- le respect de la propriété intellectuelle

Lorsque des règlements sont mis en place, ils entraînent un risque de conséquences graves, d'amendes et d'atteinte à la réputation. Les organisations qui ne sont pas prêtes à faire face à la réglementation pourraient voir leurs projets retardés, ou devoir revenir sur des décisions non conformes à la réglementation.

« Il est surprenant de constater que 39 % des vice-présidents hors TI indiquent ne pas utiliser l'IA de manière significative. Il a pourtant été démontré que l'IA s'avère particulièrement pertinente au-delà des TI… L'IA est utilisée dans différents secteurs d'activité pour accroître la productivité sans remplacer les humains. Grâce à l'IA, les employés consacrent désormais moins de temps à des tâches répétitives et fastidieuses pour se consacrer davantage à des fonctions décisionnelles à valeur ajoutée. »

François Morin,
Partenaire et spécialiste principal en matière de technologies, Québec, IBM Ecosystem, Canada

À mesure que l'on se projette vers l'avenir, de nombreuses entreprises intègrent l'IA à leurs plans à court terme, 33 % d'entre elles prévoyant réaliser des investissements importants en intelligence artificielle au cours des deux prochaines années.

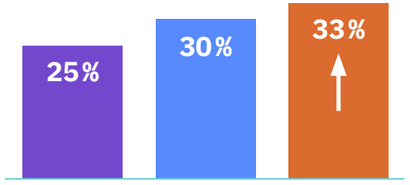
Une proportion importante des entreprises a l'intention d'investir dans des services professionnels ou dans l'analyse avancée des données au cours des deux prochaines années (42 %). Plus précisément, la majorité de ces organisations ont l'intention d'investir dans l'analyse statistique avancée (63 %), la visualisation des données (54 %) et l'analyse de type apprentissage profond (44 %), des domaines de plus en plus dominés par des outils basés sur l'IA.

COMBLER LE FOSSÉ : PERSPECTIVES TI VS NON-TI

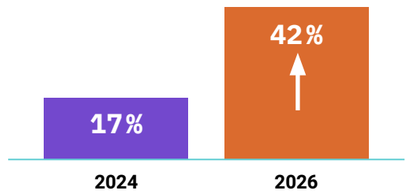
Les dirigeants sont souvent déconnectés des réalités quotidiennes de leurs équipes TI, notamment en matière de mise en œuvre de l'IA. Les tendances pour 2026 indiquent un décalage croissant entre les dirigeants et les équipes TI; la réussite passera par une collaboration qui tire parti de l'expertise des TI afin d'assurer une intégration réfléchie et transversale. Le service des TI ne peut pas se contenter d'opérer en arrière-plan; il doit avoir son mot à dire dans les décisions pour assurer que l'intégration de l'IA soit efficace et rentable.

Les décideurs non-TI sont bien plus susceptibles de déclarer que leur organisation n'utilise pas l'IA. Compte tenu de l'adoption généralisée d'au moins certains outils d'IA dans les entreprises de toutes tailles et de tous secteurs, cela semble indiquer un manque de sensibilisation lié au point de vue des TI : les dirigeants ne connaissent pas toujours l'étendue de l'intégration de l'IA au sein de leur organisation.

Les investissements prévus dans l'IA ont augmenté de manière considérable entre 2024 et 2026

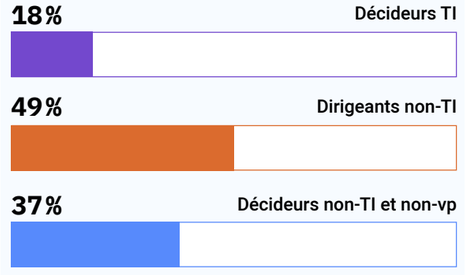


Au cours des trois dernières années, **les organisations qui prévoient d'investir dans des services professionnels ou l'analyse avancée des données** ont été regroupées et interrogées sur les détails de leur investissement. Non seulement leurs projets se sont orientés vers des analyses plus complexes, souvent pilotées par des outils d'IA, mais le nombre d'entreprises prévoyant ce type d'investissement a explosé. En 2024, elles ne représentaient que 17 % des entreprises interrogées; en 2026, elles en représentent 42 %.



Ce décalage peut créer des angles morts; la direction peut croire qu'une simple directive pour autoriser des tests d'IA ou approuver de petits projets suffit. Pourtant, à mesure que les équipes TI cherchent à déployer et optimiser les solutions d'IA à plus grande échelle, elles doivent obtenir l'adhésion des dirigeants pour avancer plus rapidement, de manière plus structurée et avec plus de profondeur.

Pourcentage (%) de répondants déclarant que leurs entreprises n'utilisent pas de solution d'IA



Résoudre les tensions entre une direction prudente et un service TI orienté vers le progrès fera la différence entre le succès et l'échec pour les organisations qui se trouvent à un tournant décisif en matière d'IA. Même celles qui ont été plus lentes à s'adapter jusqu'à présent peuvent espérer des gains rapides grâce à une action délibérée, et cela commence par permettre aux équipes des TI d'en faire davantage.

Pour tirer le meilleur parti de l'IA, les dirigeants doivent partager la prise de décision avec leurs experts TI, qui sont les mieux placés pour savoir quelles solutions et compétences privilégier.

Le rôle de l'équipe TI n'est pas seulement de faciliter, mais aussi de conseiller : n'hésitez pas à lui demander son avis sur ce qui doit être fait et sur les ressources dont elle a besoin pour y parvenir.

En retour, la responsabilité des TI dépasse le simple rôle technique et réactif. Les équipes TI doivent elles-mêmes favoriser les avancées en mobilisant leurs collègues non-TI autour de la vision de l'IA. Tissez des liens à travers l'organisation et envisagez de créer des groupes de travail chargés de collaborer à la prise de décision en matière d'IA.

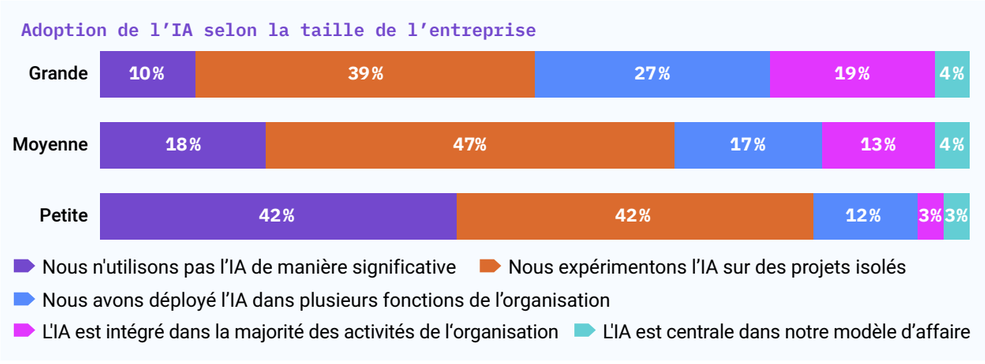
Lorsque les entreprises parviennent à engager des discussions de haut niveau sur l'IA au-delà de cloisonnements, leur prudence et leur aversion au risque cèdent la place à une intégration plus assurée.

UN RISQUE DIFFÉRENT POUR LES PETITES ORGANISATIONS

Les données de 2026 montrent que, tandis que les grandes organisations à la pointe de la technologie progressent rapidement vers l'intégration, la plupart des petites organisations n'en sont qu'à leurs premiers pas; quatre petites entreprises [moins de 100 employés] sur dix (42 %) en sont encore au stade des projets pilotes et la même proportion (42 %) n'utilise pas l'IA de manière importante.

Les moyennes et grandes entreprises déploient de plus en plus de solutions avancées, tandis que les petites entreprises n'utilisent souvent que l'IA générative, voire rien du tout. Cet écart suggère que les petites entreprises peuvent être confrontées à des contraintes qui limitent leur capacité à réaliser des gains d'efficacité, à améliorer la prise de décision ou à innover dans leurs opérations grâce à l'IA.

Adoption de l'IA selon la taille de l'entreprise



Remédier à ces contraintes par le biais d'une mise à niveau des compétences ciblée, d'un soutien consultatif ou d'une planification stratégique peut contribuer à s'assurer que l'IA apporte une valeur ajoutée mesurable aux entreprises de toutes tailles. **(Pour voir la donnée complète voir la page 29 du tableau de bord)**

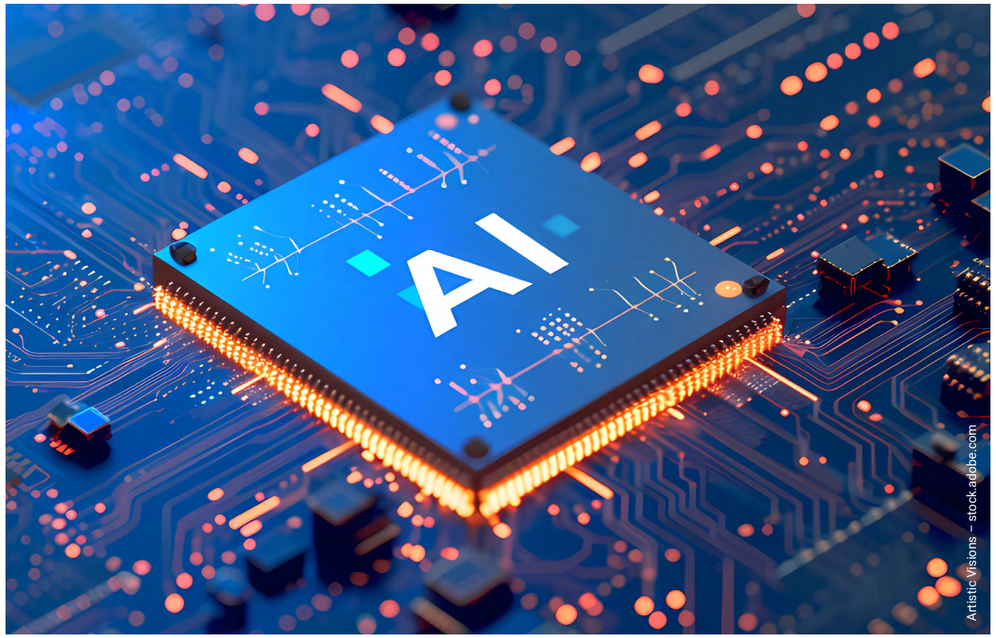
Pour les petites entreprises, le risque lié à l'investissement dans l'intelligence artificielle est évalué à une échelle différente de celle des grandes entreprises. Cependant, la véritable question n'est pas le risque d'investir, mais celui de ne pas investir.

Si le coût de l'adoption de l'IA peut sembler important, il doit être mis en balance avec le coût de l'inaction : occasions manquées et perte de compétitivité. Dans le contexte actuel, où l'automatisation, l'optimisation et la prise de décision basée sur les données sont des moteurs clés de la performance, rester immobile représente un risque stratégique majeur.

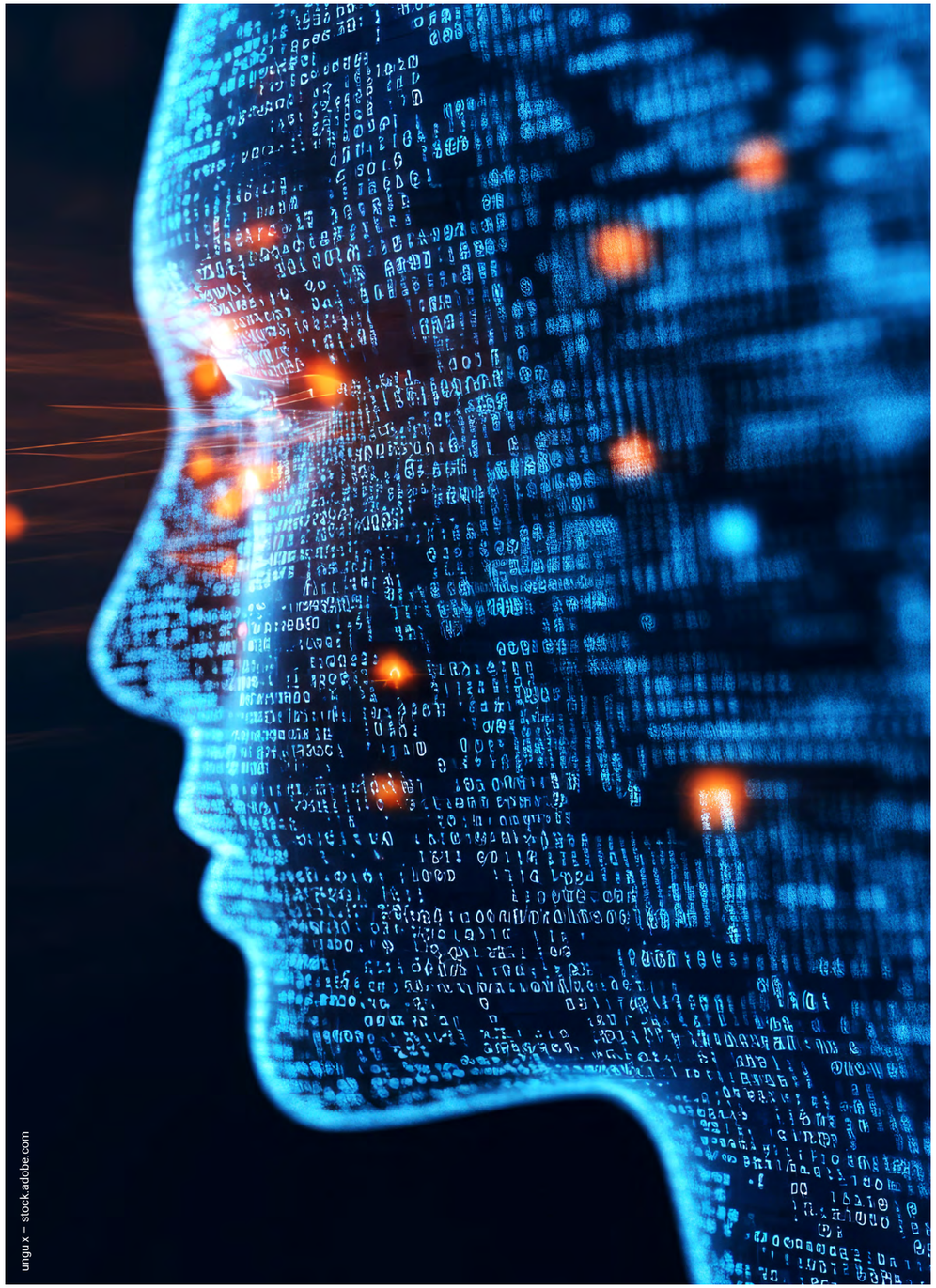
Lorsqu'elles sont correctement ciblées, les solutions d'IA peuvent être déployées rapidement au sein des petites entreprises, générant de la valeur dans un délai plus court et offrant des taux de rendement du capital investi (RCI) équivalents, voire supérieurs, à ceux des grandes entreprises.La raison est simple : dans les petites entreprises, chaque gain d'efficacité a une incidence directe et immédiate sur la productivité. Alors que les grandes organisations peuvent diluer ces gains en raison de leur taille et de leur complexité, les petites entreprises peuvent obtenir des résultats plus rapides et plus tangibles.

Cela nécessite toutefois une volonté d'investir de manière stratégique, d'agir avec détermination et d'éviter de s'enliser dans un cycle sans fin d'expérimentation sans aller au-delà de celle-ci.

La révolution de l'IA offre également aux précurseurs l'occasion de se démarquer de leurs pairs grâce à leur leadership éclairé et à l'échange d'idées. Les avantages d'un dialogue ouvert entre les organisations sont réciproques. Les entreprises les plus innovantes ont tout à gagner à partager leurs réussites et à démystifier cette technologie, contribuant ainsi à dissiper les craintes et le scepticisme qui entourent l'IA. Parallèlement, les organisations qui n'en sont qu'à leurs débuts se verront ainsi encouragées à prendre elles-mêmes des initiatives plus audacieuses.



Artistic Visions – stock.adobe.com


ungu.x – stock.adobe.com

RISQUES

MANQUE DE COORDINATION ENTRE LA DIRECTION ET LE SERVICE TI

En dehors des équipes TI, les décideurs peuvent ne pas avoir une vision complète de la manière dont l'IA est déployée, ni la capacité de suivre le rythme des avancées technologiques rapides. Parallèlement, il peut être difficile pour les équipes TI de communiquer avec la direction afin d'obtenir son adhésion lorsque la technologie évolue si rapidement. Les conséquences potentielles de ce décalage sont considérables : retards dans les progrès, gaspillage de ressources, décisions stratégiques non alignées sur les capacités informatiques et désavantage face à des concurrents plus agiles.

DES DONNÉES PEU FIABLES PEUVENT ENTRAÎNER DES ERREURS, DES BIAIS ET DES INEFFICACITÉS

La qualité du résultat dépend de celle des données d'entrée; cette leçon existe depuis que le monde est monde, mais il semble que nous devions la réapprendre à chaque révolution technologique. Les erreurs de l'IA coûtent cher et peuvent rapidement devenir un risque pour la réputation d'une entreprise. Une IA efficace repose sur une stratégie de données solide qui tient compte de la structure et de la qualité des données d'entrée, ainsi que sur un suivi minutieux des résultats.

LES DÉCISIONS DESCENDANTES ABOUTISSENT À DES DIRECTIVES IMPOSSIBLES À METTRE EN ŒUVRE

Comme nous l'avons indiqué au début de ce chapitre, l'IA n'est pas une question de tout ou rien. Elle doit être intégrée de manière réfléchie, en s'appuyant sur les connaissances de ceux qui la mettront en œuvre (les équipes TI) et de ceux qui l'utiliseront (tous les membres de l'organisation). Les décisions concernant l'IA doivent être fondées sur la réalité et les capacités disponibles, sans quoi l'intégration n'est tout simplement pas envisageable.

OPPORTUNITÉS

AGISSEZ AVEC DÉTERMINATION

Il est temps de choisir des solutions et des outils d'IA et de s'y engager pleinement. Pour les organisations qui en sont encore aux prémices de leur parcours, fixez des délais pour les phases d'expérimentation et préparez-vous à prendre des décisions rapidement une fois la période d'essai terminée. La puissance des outils d'IA réside dans leur personnalisation, qui nécessite du temps, de l'engagement et de l'expertise pour porter ses fruits.

INVESTISSEZ DANS LES PERSONNES

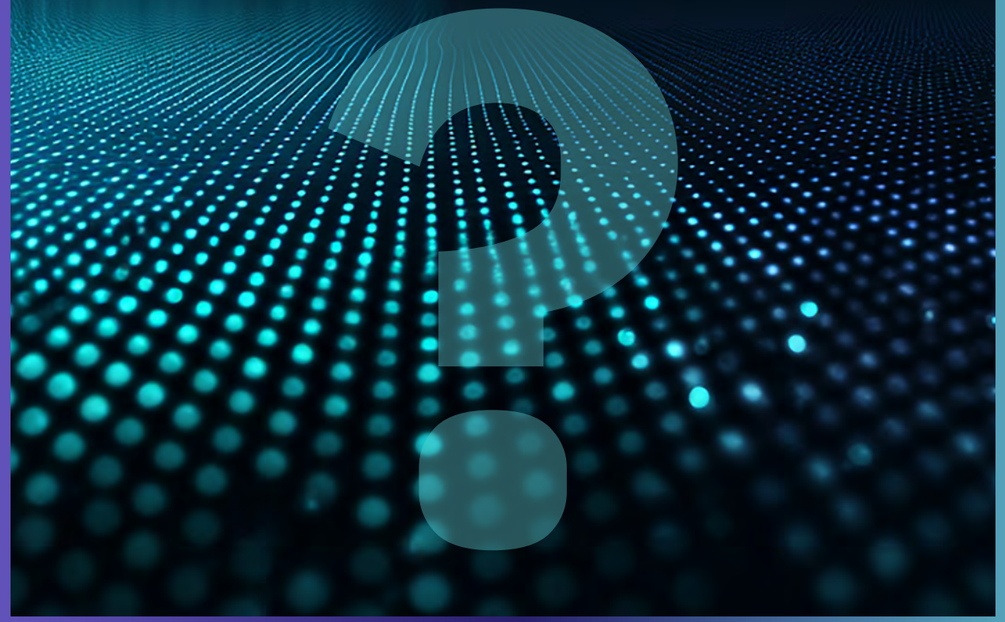
Réorientez les investissements des essais de solutions et des petits projets vers le renforcement des compétences internes afin de permettre une intégration réelle et stratégique de l'IA au sein de votre organisation. La réussite de l'intégration de l'IA dépendra des capacités et des compétences de l'équipe, et non des outils eux-mêmes.

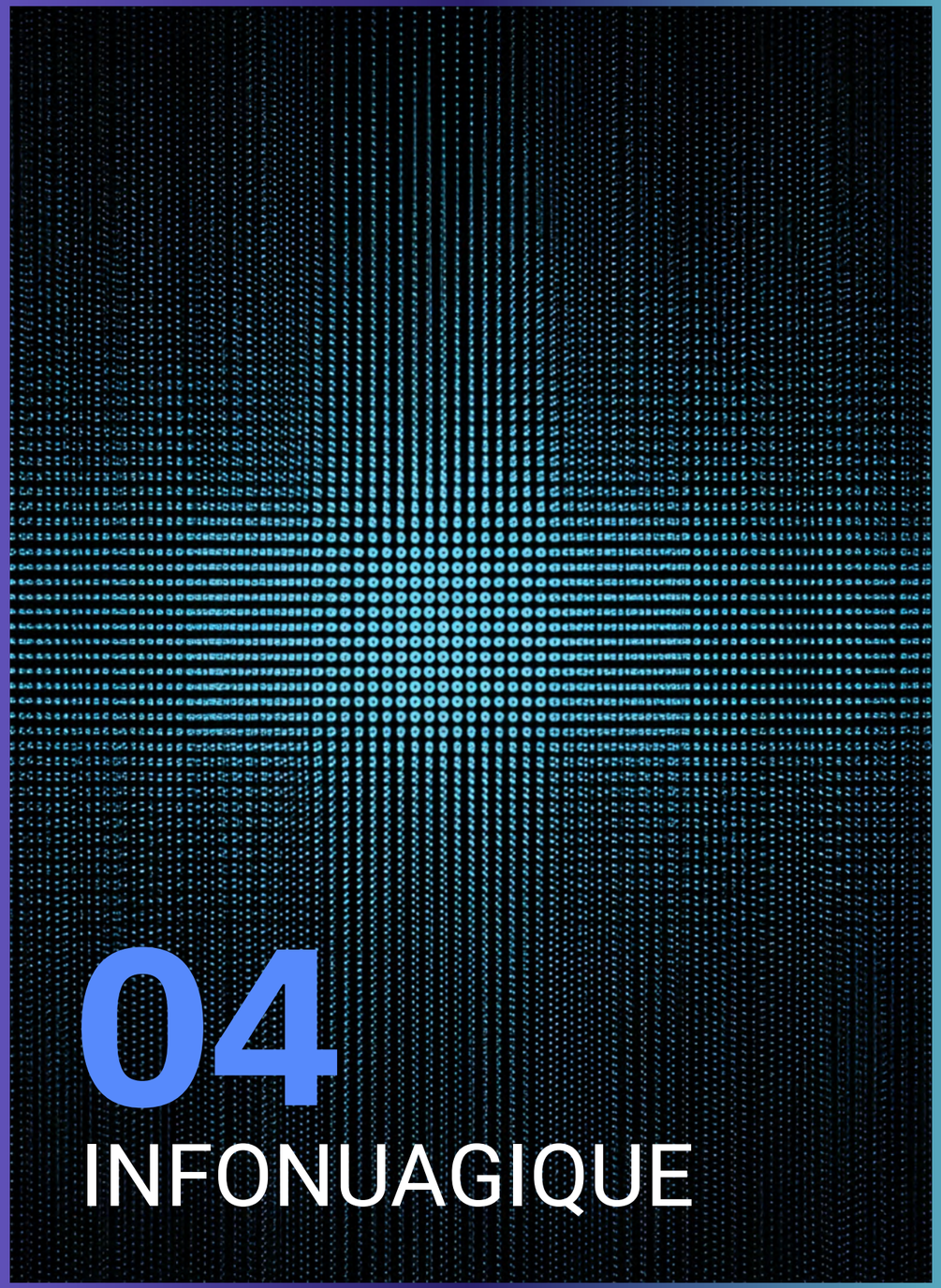
COLLABOREZ POUR TRACER LA VOIE À SUIVRE ET DONNEZ LES MOYENS D'AGIR AU SERVICE TI

La direction et le service TI doivent travailler ensemble pour développer une structure de gouvernance de l'IA claire, avec des priorités, des normes, une mesure du RCI et des ICP qui permettront aux dirigeants de constater de réels progrès. Une fois une stratégie solide en place, donnez aux équipes TI les moyens d'agir afin qu'elles puissent avancer sans obstacle inutile. Il doit y avoir des attentes et des garde-fous, mais laissez les experts prendre les décisions sur le terrain.

La grande QUESTION

La grande question va bien au-delà du choix de l'outil ou de la plateforme à adopter. Les entreprises doivent se poser les questions suivantes : La direction et l'équipe TI sont-elles sur la même longueur d'onde concernant les décisions relatives à l'IA ? Notre structure de gouvernance est-elle claire, avec des rôles, des responsabilités, des ICP et des indicateurs de RCI bien définis ? Sommes-nous prêts à agir de manière décisive pour passer de l'expérimentation à l'intégration ?





04
INFONUAGIQUE

Souveraineté numérique : vers une autonomie stratégique maîtrisée

La souveraineté numérique s'impose comme une tendance de fond qui met en lumière un risque longtemps sous-estimé : celui des dépendances technologiques. Dans un contexte marqué par les tensions géopolitiques, l'extraterritorialité de certaines législations et la concentration du marché infonuagique, ces dépendances ne sont plus uniquement techniques : elles conditionnent la capacité des organisations à agir, à sécuriser leurs données et à évoluer.

Face à ce constat, la souveraineté numérique peut être définie comme la capacité pour une organisation de garder le contrôle sur ses données, ses infrastructures et ses choix technologiques, tout en s'inscrivant dans des écosystèmes ouverts et performants.

La question n'est donc plus seulement celle de la localisation des données, mais celle de la maîtrise effective des ressources numériques : qui opère les infrastructures, sous quel droit, et avec quelle capacité de contrôle et d'arbitrage.

UN CHANGEMENT DE POSTURE EN COURS

Au Canada comme au Québec, la souveraineté numérique devient un sujet opérationnel. L'Énoncé de politique de souveraineté numérique et d'approvisionnement en technologies de l'information en est une illustration : il encourage le recours à des infrastructures maîtrisées, le développement de capacités locales et l'adoption de technologies ouvertes.

Le débat sort désormais d'une opposition binaire entre solutions « souveraines » et « non souveraines » pour se recentrer sur la criticité des données et des usages.

Cette approche permet de structurer des stratégies graduées, en mobilisant différents acteurs, à condition qu'ils s'inscrivent dans le cadre juridique local, offrent des garanties de conformité et limitent l'exposition aux législations extraterritoriales.

Elle implique des architectures conçues pour rester évolutives, interopérables et réversibles, afin de maîtriser les dépendances dans le temps.

GUILLAUME GILBERT
Responsable des communications et des affaires publiques, OVHcloud Canada

Guillaume Gilbert est responsable des communications et des affaires publiques chez OVHcloud au Canada. Diplômé en sciences politiques et relations internationales, il y pilote la stratégie d'influence et contribue à structurer le positionnement de l'entreprise autour des enjeux de souveraineté numérique et d'innovation durable.

DES PRATIQUES QUI SE STRUCTURENT

Trois évolutions devraient structurer les stratégies numériques dans les prochaines années :

- **Piloter les dépendances :** cartographier les dépendances technologiques (infonuagique, logiciels, données) devient essentiel pour identifier les risques et éclairer les décisions d'investissement.
- **Préserver la liberté de choix :** les architectures hybrides et multicloud, combinées à des technologies ouvertes, permettent de limiter les situations de verrouillage et de maintenir une capacité d'arbitrage.
- **S'appuyer sur des environnements de confiance :** au-delà de la performance, les organisations privilégient des environnements offrant des garanties claires en matière de sécurité, de cadre juridique, de transparence et de gouvernance des données.

RECOMMANDATIONS POUR LES DÉCIDEURS

Trois leviers peuvent être activés dès aujourd'hui :

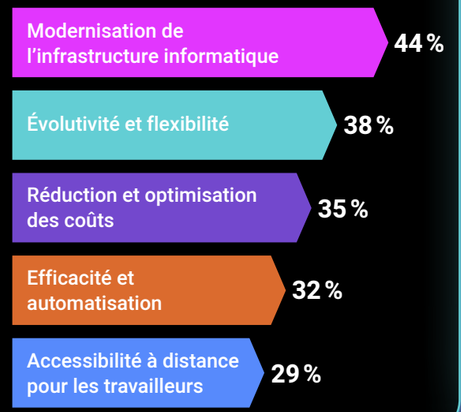
- **Intégrer les dépendances technologiques comme un risque stratégique,** au même titre que la cybersécurité ou la continuité d'activité.
- **Faire des standards ouverts, de la réversibilité et de l'interopérabilité des critères clés,** dès la conception et dans les processus d'achat.
- **Aligner les choix technologiques avec les contraintes réglementaires et géopolitiques,** afin de sécuriser les trajectoires à moyen terme.

La souveraineté numérique repose sur des choix d'architecture et de partenaires capables de garantir, dans la durée, sécurité, conformité et prévisibilité. Les approches intégrant maîtrise opérationnelle, transparence des environnements et capacité réelle de réversibilité offrent aujourd'hui des leviers concrets pour concilier exigences réglementaires, performance et liberté d'arbitrage.

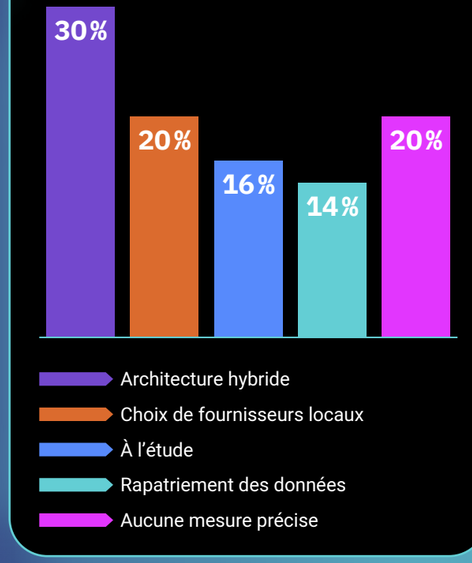
Fournisseur mondial de solutions infonuagiques, OVHcloud est implantée au Canada depuis 2012, où elle opère plusieurs centres de données au Québec et en Ontario ainsi qu'une usine d'assemblage de serveurs à Beauharnois (QC). Acteur industriel du cloud, OVHcloud se distingue par un modèle intégré lui permettant de maîtriser l'ensemble de sa chaîne de valeur, de la conception de ses serveurs à l'exploitation de ses infrastructures. Cette approche lui permet d'offrir des solutions performantes, sécurisées et compétitives, tout en garantissant une conformité aux cadres réglementaires locaux et une protection contre les lois extraterritoriales. Présente sur quatre continents et au service de clients dans plus de 140 pays, OVHcloud accompagne entreprises et organisations publiques dans leurs enjeux de transformation numérique, au service de la performance et de l'autonomie stratégique.

TABLEAU DE BORD

Les cinq principales raisons pour lesquelles les entreprises utilisent l'infonuagique :

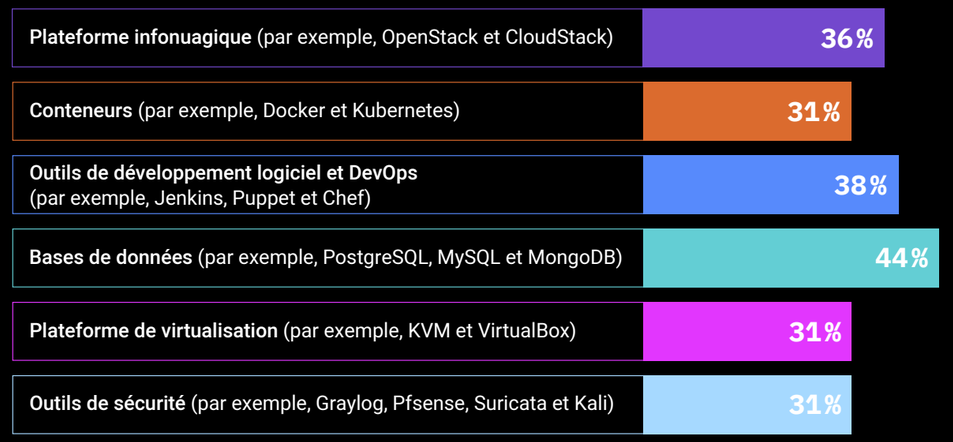


Mesures que les entreprises mettent en œuvre ou envisagent de mettre en œuvre en matière de souveraineté des données



75 % des entreprises utilisent déjà une solution à code source ouvert dans leur environnement de production ou pour des projets futurs

Voici les types de solutions à code source ouvert qu'elles utilisent:



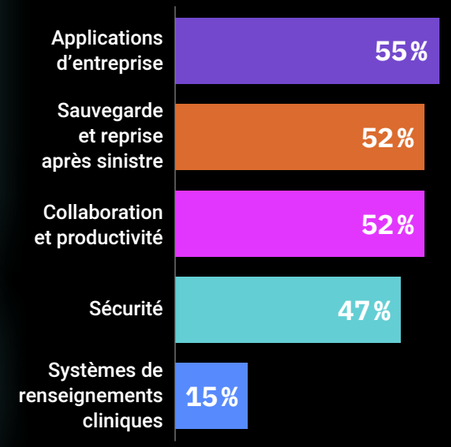
Les cinq principaux défis liés à la gouvernance des données :

Protection des données sensibles	56 %
Qualité et fiabilité des données	54 %
Conformité réglementaire	43 %
Accès aux données et leur partage	40 %
Soutien pour les demandes de renseignements officielles	20 %

77 % des entreprises déclarent que les enjeux de souveraineté des données sont plus importants aujourd'hui qu'ils ne l'étaient il y a deux ans

91 % des entreprises hébergent au moins un système ou un cas d'utilisation dans l'infonuagique

Les cinq principaux systèmes hébergés dans l'infonuagique :



Interprétation des données

GÉOPOLITIQUE ET SOUVERAINETÉ DES DONNÉES

La souveraineté des données est devenue une préoccupation majeure pour les organisations canadiennes. En raison des tensions commerciales croissantes entre les États-Unis et le Canada et du renforcement des exigences réglementaires, plus de trois quarts des entreprises estiment qu'elle est aujourd'hui plus importante qu'il y a deux ans. Et près de deux tiers d'entre elles ont déjà mis en œuvre des mesures ou envisagent activement de le faire. **(Pour voir la donnée complète voir la page 41 du tableau de bord)**

La plupart des organisations réagissent aux pressions liées à la souveraineté non pas en rebâtissant leur système en entier, mais en se tournant vers des architectures infonuagiques hybrides et des fournisseurs locaux qui offrent un contrôle plus direct de l'emplacement des données. Dans ce contexte, l'infonuagique est recadrée : elle représente moins un moteur d'innovation qu'un instrument de gestion des risques. Cependant, ce recadrage génère ses propres tensions. La même flexibilité qui permet le développement peut subtilement miner le contrôle en introduisant des dépendances aux fournisseurs, en dupliquant les coûts et en fragmentant les données d'une manière qui ralentit les prises de décisions et ébranle la confiance dans les données elles-mêmes.

« Lorsque les organisations n'ont pas le contrôle de l'emplacement où se trouvent leurs données, il devient exponentiellement plus complexe d'en assurer la sécurité, la qualité et la conformité réglementaire. Les questions d'infrastructure et de gouvernance convergent de plus en plus; par conséquent, elles ne sont plus considérées comme deux aspects distincts, mais comme un seul et même élément. »

Yves Veillette, ***Directeur de l'exploitation, NOVIPRO***

L'agilité et la souveraineté ne sont pas des alliés naturels, et le fossé qui les sépare a un coût.

Cette vision ne semble pas aussi claire pour toute la haute direction. Les décideurs en matière de TI sont beaucoup plus susceptibles de considérer la souveraineté des données comme un enjeu crucial (81 % comparativement à 5 % chez leurs homologues non-TI), et cette préoccupation se traduit directement par des mesures : 72 % des dirigeants TI ont pris ou envisagé au moins une mesure liée à la souveraineté, comparativement à seulement 47 % pour ceux non-TI. Sans alignement, les investissements en gouvernance ne sont plus prioritaires et l'exposition aux risques de non-conformité s'accroît lentement. Ce décalage est plus marqué en fonction de la taille de l'entreprise : alors qu'une organisation sur cinq déclare ne prendre aucune mesure précise, ce chiffre atteint 39 % du côté des petites entreprises – celles qui ont le moins de capacité à absorber les chocs sont aussi les moins préparées à y faire face.

Les trois principaux défis liés à la gouvernance des données auxquels les entreprises canadiennes sont confrontées :

- Protection des données sensibles
- Qualité et fiabilité des données
- Conformité réglementaire

Le sentiment d'urgence entourant la souveraineté des données est renforcé par les défis liés à la gouvernance qui la sous-tendent. La protection des données sensibles arrive en tête de liste (56 %), suivie par la qualité et la fiabilité des données (54 %), et la conformité réglementaire (43 %), un trio à l'image de la pression croissante à laquelle les entreprises canadiennes sont confrontées lorsqu'elles gèrent des données qu'elles ne peuvent pas toujours voir, vérifier ou contrôler totalement. Pour relever ces défis, la souveraineté doit être considérée comme une priorité opérationnelle : savoir où se résident les données, renforcer constamment les contrôles d'accès et intégrer la gouvernance aux activités quotidiennes.

« Pour une municipalité, l'emplacement où les données sont stockées et traitées ne constitue pas un détail technique : c'est une question de confiance du public. Le passage à des fournisseurs de services infonuagiques canadiens était une étape naturelle, et même s'il n'a pas été formalisé dans une politique officielle, il est devenu un principe fondamental qui influence chaque demande de proposition, chaque analyse de rentabilité et chaque conversation sur le budget que nous avons. »

Mark Aiken, ***Gestionnaire des services TI, Municipalité de Meaford***

Lorsque les entreprises peuvent réellement contrôler l'emplacement de leurs données, elles transforment un risque croissant en un avantage maîtrisable.

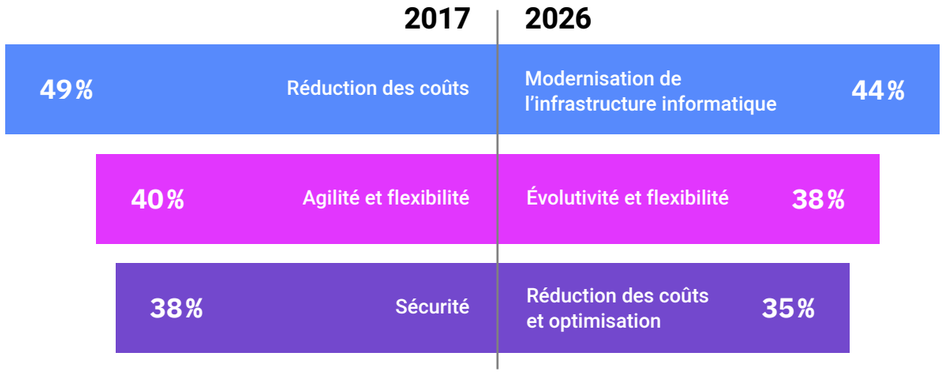
L'UTILISATION DE SOLUTIONS À CODE SOURCE OUVERT EST MAINTENANT RÉPANDUE.

Les trois quarts des organisations canadiennes utilisent déjà au moins une solution à code source ouvert, et 64 % d'entre elles prévoient en étendre l'adoption, ce qui montre clairement que le code source ouvert ne se situe plus en marge des TI d'entreprise, mais bien au cœur de celles-ci. L'utilisation actuelle est principalement effectuée par les bases de données (44 %), suivies par les outils de développement logiciel et DevOps (38 %) et les plateformes infonuagiques (36 %). Le modèle d'adoption nous révèle ce qui suit : les solutions les plus utilisées (les bases de données relationnelles comme MySQL, et les outils NoSQL comme MongoDB et PostgreSQL) sont bien documentées, faciles à déployer et prises en charge par un vaste bassin de talents. L'adoption future prévoit des plateformes d'orchestration infonuagique, comme OpenStack et CloudStack. Elle est donc ambitieuse non pas en raison d'une réticence, mais d'une préparation. L'orchestration à grande échelle nécessite des pipelines d'automatisation, une expertise en systèmes multiplateformes et une discipline opérationnelle que la plupart des organisations sont encore en train de développer. En résumé, l'écart entre les solutions que les entreprises adoptent actuellement et celles qu'elles prévoient d'adopter réside davantage dans la préparation que dans la volonté.

Pour la première fois en trois ans, la modernisation de l'infrastructure TI a délogé la réduction des coûts en tant que principale raison pour laquelle les organisations canadiennes se tournent vers l'infonuagique. Ce changement est le signe d'un marché bien établi pour lequel on ne se pose plus la question « qu'est-ce que cela nous permet d'économiser ? », mais bien « qu'est-ce que cela nous permet de faire ? ». Il s'agit d'une évolution encourageante, d'autant plus que l'infonuagique ne permet pas toujours de réduire les coûts : elle permet de développer de nouvelles méthodes de travail.

Suivi des tendances : La tête dans les nuages

Évolution des priorités infonuagiques d'hier à aujourd'hui



« L'infonuagique est encore loin de tenir sa promesse de réduction des coûts — du moins dans notre secteur, où la sensibilité aux dépenses opérationnelles rend le sur site un choix financièrement plus judicieux. Nous utilisons encore l'infonuagique lorsque cela a du sens, cependant. »

Stephan Brisson, ***Directeur Principal - Infrastructure et Opérations TI, UAP Inc.***

Toutefois, ce changement ne s'opère pas de façon uniforme dans l'ensemble de la direction. Alors que 51 % des dirigeants TI affirment que la modernisation de l'infrastructure TI est leur principale priorité en matière d'infonuagique, seuls 16 % des dirigeants hors TI partagent cet avis, et ceux-ci sont plus susceptibles de prioriser la flexibilité, l'agilité et la réduction des coûts. Cette divergence est importante, car la modernisation et la réduction des coûts ne sont pas des objectifs contradictoires. Une stratégie de modernisation mise en œuvre avec succès permet de créer un environnement plus simple et plus adaptable qui entraîne des gains d'efficacité au fil du temps. Les dirigeants TI et les fournisseurs externes devraient présenter des analyses de rentabilité et des exemples de rendements d'investissements concrets afin d'obtenir l'adhésion de la haute direction nécessaire à une mise en œuvre complète.

L'infonuagique est passée d'une technologie émergente à une référence opérationnelle. Il y a 10 ans, 14 % des entreprises canadiennes n'avaient pas encore adopté l'infonuagique, alors qu'aujourd'hui, ce chiffre a chuté à 9 %. Maintenant, l'adoption est presque universelle parmi les entreprises qui perçoivent leur infrastructure comme étant à l'avant-garde (98 %), ainsi que dans les secteurs manufacturier (100 %), et des technologies, des médias et des télécommunications (96 %). L'infonuagique est devenue un indicateur de la préparation de l'organisation en général chez les entreprises qui traitent l'informatique non pas comme des frais généraux, mais comme une infrastructure favorisant la résilience et la croissance. Pour la plupart des organisations, la question n'est plus de savoir s'il faut adopter l'infonuagique, mais plutôt de savoir l'utiliser de façon plus stratégique.

RISQUES

LA FAILLE CACHÉE

Le fossé qui se creuse entre les décideurs TI et les décideurs hors TI en ce qui concerne la souveraineté des données n'est pas qu'un problème de perception : c'est un facteur de risque pour l'exécution. Sans un alignement au niveau de la haute direction sur une stratégie de souveraineté, votre entreprise pourrait être exposée à des risques comme des retards dans les projets critiques, une mauvaise affectation des ressources, une incapacité à répondre aux exigences réglementaires et une perte d'avantage concurrentiel.

PETITE ENTREPRISE, GRANDE EXPOSITION

Les petites organisations sont beaucoup moins susceptibles d'avoir pris des mesures en matière de souveraineté ou de gouvernance des données. Cette inaction risque de compromettre leur capacité de développement, d'accroître leur dépendance à des solutions externes mal contrôlées, de leur faire perdre des clients, de perturber leur fonctionnement, et même de ralentir ou d'interrompre leur croissance.

ON NE PEUT PAS PROTÉGER CE QUE L'ON NE VOIT PAS

Si votre organisation n'a pas dressé un plan de l'emplacement de ses données dans des environnements hybrides, publics ou multicloud, vous ne pouvez pas évaluer efficacement votre exposition aux risques en matière de souveraineté des données. En plus de nuire à votre capacité à prendre des décisions éclairées, ce manque de clarté risque d'accroître les erreurs stratégiques et de miner la confiance dans les données, ce qui peut entraîner des inefficacités opérationnelles.

OPPORTUNITÉS

TOUT COMMENCE PAR UNE PRISE DE CONSCIENCE

Il y a une différence entre le fait de savoir que la souveraineté des données est importante et celui d'agir en conséquence. Commencez par dresser un plan de vos flux de données et par classer les données sensibles par niveau de risque, puis évaluez les fournisseurs en fonction de la conformité réglementaire, et non uniquement du coût. Mettez en œuvre des politiques de contrôle d'accès qui correspondent à l'emplacement réel de vos données. Les gains seront tangibles : une meilleure visibilité, un contrôle accru et une réduction mesurable de l'exposition.

ALLER AU-DELÀ DU SERVICE DES TI

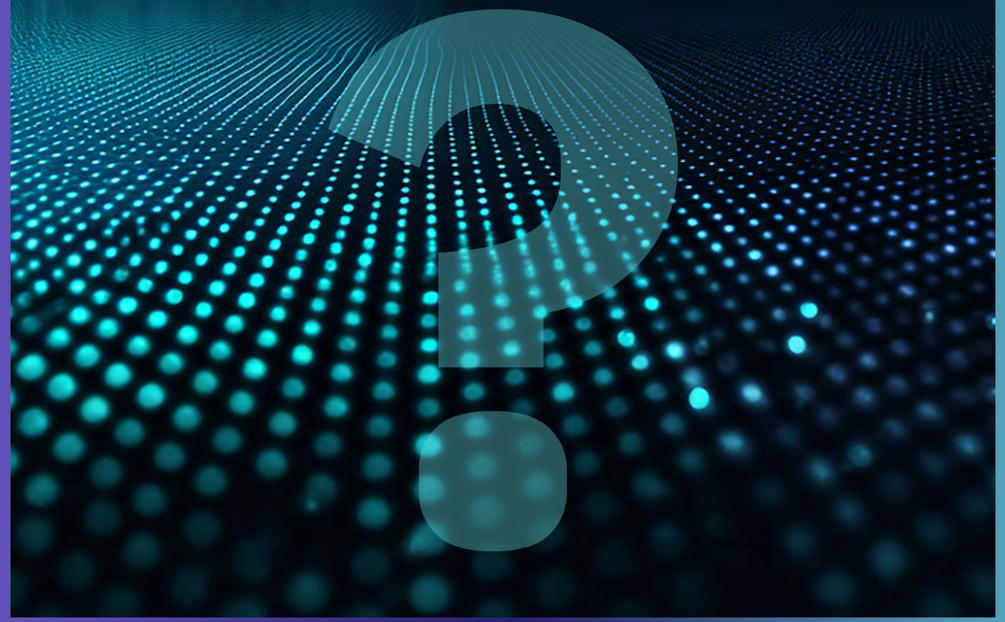
La souveraineté des données cesse d'être un problème de TI lorsqu'elle a des effets sur les résultats (et cela finit toujours par arriver). Il faut mettre en place des structures de gouvernance conjointes entre les dirigeants TI, faire en sorte que les risques liés aux données se traduisent en indicateurs de rendement clés pour l'entreprise, et fournir aux dirigeants d'autres services : des tableaux de bord qu'ils peuvent réellement comprendre et qui leur permettent d'agir en conséquence.

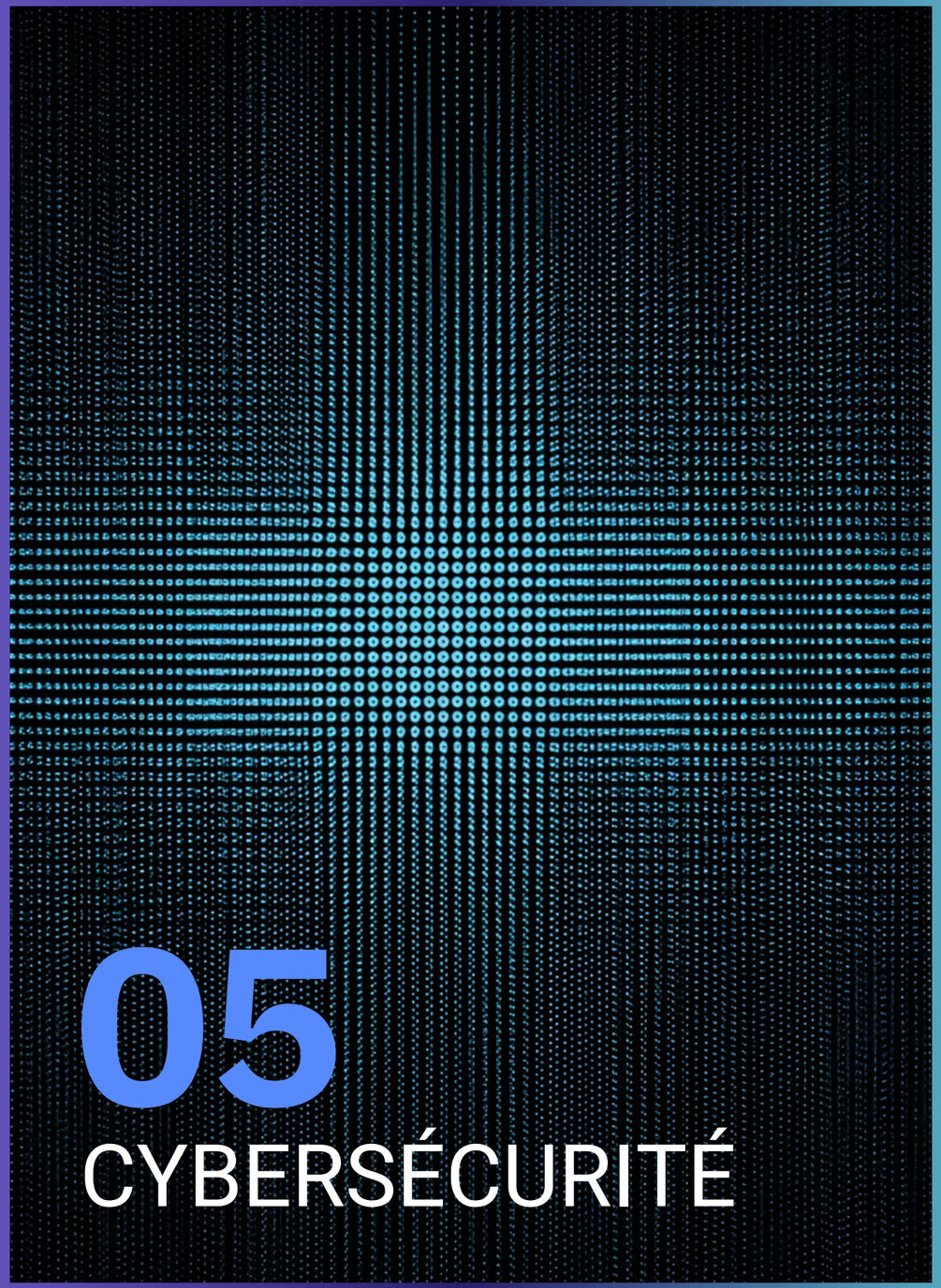
MODERNISER INTELLIGEMMENT POUR ÉCONOMISER GRANDEMENT

La modernisation et la réduction des coûts peuvent aller de pair uniquement si la mise en œuvre est mûrement réfléchie. Il faut tout d'abord rationaliser la charge de travail pour éliminer les redondances, ajouter un niveau d'automatisation pour réduire les tâches manuelles et adopter des pratiques en matière d'opérations financières pour gérer activement les dépenses en infonuagique. Les économies sont bien réelles, mais elles sont réalisées graduellement et elles dépendent de la mise en place réussie des éléments fondamentaux.

La grande QUESTION

Votre organisation a une stratégie infonuagique. Est-elle pleinement alignée avec vos priorités d'affaires et les exigences de souveraineté des données ? Et surtout, vos décisions actuelles renforcent-elles réellement votre résilience et votre position concurrentielle pour l'avenir ?





05
CYBERSÉCURITÉ

Le prix de la productivité

La devise « *Le prix de la liberté, c'est la vigilance éternelle* », souvent attribuée à tort aux pères fondateurs américains, était une expression populaire dans l'Europe et l'Amérique du Nord du début du XIXe siècle. Les nations nouvelles et anciennes, qui ont lutté pour s'établir et définir des principes moraux de gouvernance et d'équité, savaient que ces libertés nouvellement acquises étaient fragiles et nécessitaient une protection constante.

Les technologies de l'information n'ont pas les mêmes deux siècles d'histoire. Cependant, les questions de sûreté, de sécurité et d'utilisation éthique ont pris de l'ampleur et ont évolué au cours des 75 dernières années, alors que le secteur des technologies de l'information a mûri et est devenu au premier plan de l'économie mondiale. Les avantages croissants de la technologie s'accompagnent de risques continus qui menacent la productivité et les occasions à venir.

Lorsque j'étais étudiant dans les années 1980 et que les réseaux de PC en étaient encore à leurs balbutiements, les virus informatiques étaient déjà monnaie courante. Insérer une disquette dans son ordinateur comportait le risque réel de l'infecter avec un code malveillant qui pouvait faire des ravages dans ses données et ses applications. La popularité de l'Internet, qui a commencé au début des années 1990, a facilité la propagation des virus, et les risques se sont étendus du particulier à l'entreprise. Les logiciels antivirus sont devenus obligatoires et sont désormais intégrés aux systèmes d'exploitation, avec des mises à jour fréquentes automatiquement téléchargées et installées pour notre protection.

Le risque de vol de données est tout aussi vieux. Alors que les particuliers et les entreprises confiaient de plus en plus leurs biens les plus précieux (leurs données) à leurs réseaux informatiques, le piratage informatique est devenu une nouvelle profession. L'insaisissable pirate informatique, opérant dans l'ombre, trouvant et exploitant les vulnérabilités des systèmes des grandes entreprises, était au départ presque un idéal romantique : un Robin des Bois moderne, en quelque sorte, visant à mettre les gouvernements et les grandes entreprises dans l'embarras. Mais les attaques sont devenues plus sophistiquées et il s'est avéré que les données volées avaient potentiellement une immense valeur monétaire, puisqu'elles pouvaient être utilisées par des logiciels de rançon ou au service de l'espionnage industriel.

Les défenses ont donc dû évoluer avec les menaces. La protection par mot de passe a été remplacée par l'authentification multifactorielle, par exemple, et tout un secteur fournissant des outils et des services de gestion de l'identité et de l'accès a vu le jour.

FEITE KRAAY
Responsable de la Commercialisation Quantique chez PINQ2 - Plateforme d'Innovation Numérique et Quantique

Un cadre supérieur avec quatre décennies d'expérience dans le secteur informatique canadien, Feite utilise sa devise « toujours être curieux » pour chercher constamment de nouvelles façons innovantes de résoudre les problèmes commerciaux de ses clients. Ses intérêts actuels incluent l'informatique quantique, l'intelligence artificielle et les relations entre ces disciplines. Il est un conférencier régulier lors d'événements tels que IBM TechXChange. Il publie des articles sur des sujets techniques et sociaux couvrant l'IA et l'informatique quantique, sur la plateforme Substack.

Aujourd'hui, tout est différent et pourtant rien n'a changé.

Au cours des cinq dernières années, l'intelligence artificielle s'est imposée comme l'innovation technologique dominante du XXIe siècle. Au-delà de l'engouement médiatique, l'IA a transformé une grande partie de nos méthodes de travail et de nos modes de vie. Les débats entre amis se règlent en posant une question à Copilot. Des itinéraires complets de vacances sont préparés par ChatGPT. Gemini ou Claude se chargent de certaines tâches laborieuses du développement logiciel, et chaque professionnel dispose d'un assistant IA pour résumer un document ou rédiger un courriel.

Mais n'oublions pas que si l'IA nous apporte de nombreux avantages dans notre vie professionnelle et privée, elle en apporte aussi aux acteurs malveillants qui cherchent à désactiver nos systèmes ou à voler nos données. Le rapport annuel Portrait TI de NOVIPRO a fait le suivi de la croissance exponentielle des cyberattaques, et il indique que le coût annuel de la cybercriminalité devrait atteindre 15,9 billions de dollars d'ici 2029.

En un sens, rien n'a changé puisque les mêmes menaces existent toujours. C'est seulement qu'avec l'IA, les attaques sont beaucoup plus faciles à exécuter et donc beaucoup plus répandues. Et tout est différent, car l'IA permet des types d'attaques entièrement nouveaux qui nécessiteront des défenses plus vigilantes.

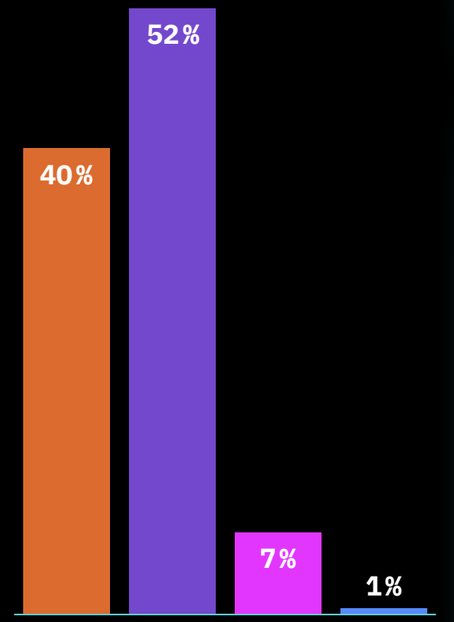
Par exemple, l'injection d'invite est l'une des nouvelles méthodes d'attaque les plus répandues. Des invites malveillantes peuvent facilement être ajoutées à des documents ou à des feuilles de calcul téléversés pour l'IA générative, trompant le système pour qu'il ignore les mesures de sécurité. Les résultats peuvent aller de la perte de données à la mauvaise orientation du flux de travail. De même, les développeurs qui utilisent des assistants IA pour le codage peuvent être vulnérables à l'insertion de logiciels malveillants dans leur code.

Il n'existe pas de moyen de défense infaillible contre ces attaques. Les particuliers et les organisations doivent plutôt déployer une stratégie d'atténuation des risques basée sur des principes de bon sens. Ils doivent veiller à ce que des politiques de contrôle d'accès soient mises en place et accordent aux grands modèles de langage le moins de privilèges possible lorsqu'ils travaillent avec du code ou des données sensibles; appliquer des procédures strictes de nettoyage et de validation à toutes les données d'entraînement; surveiller les invites de saisie en séparant clairement les invites du système et celles de l'utilisateur; et valider les résultats du grand modèle de langage, en les filtrant et en les vérifiant avant de les utiliser. Tout cela revient à garder l'humain au courant, et à traiter l'IA comme un assistant plutôt que comme un agent indépendant.

Pour tirer pleinement parti de l'utilisation de l'IA, modifions ce mot d'ordre du XIXe siècle : *« Le prix de la **productivité,** c'est la vigilance éternelle. »*

TABLEAU DE BORD

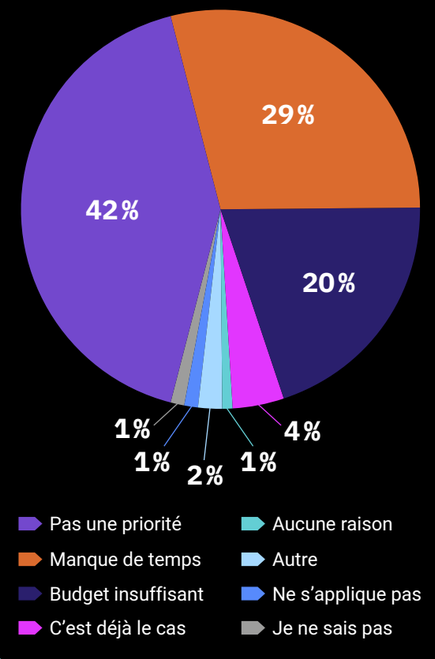
92 % **des répondants** déclarent faire confiance à leur organisation en matière de sécurité, et **40 %** d'entre eux indiquent avoir un niveau de confiance élevé



67 % **des entreprises** ont offert une formation en cybersécurité à leurs employés au cours de la dernière année

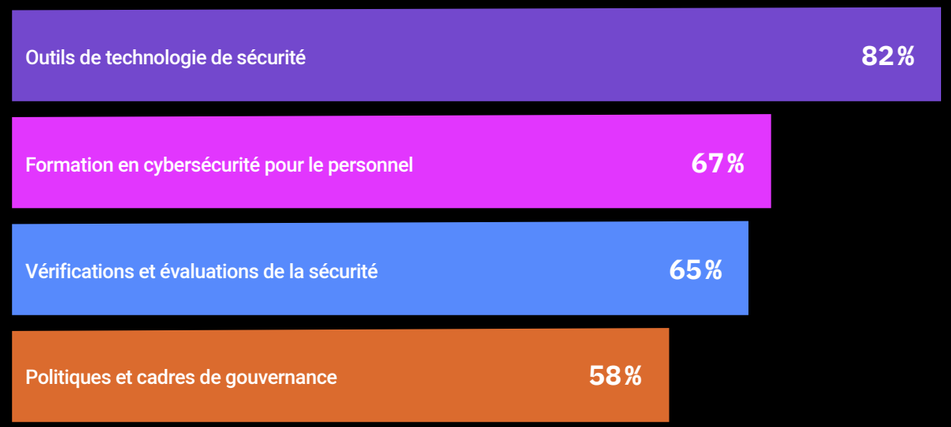
Les incidents de cybersécurité très médiatisés ont influencé les pratiques en matière de sécurité des données internes pour **52% des entreprises**

Raisons pour lesquelles les incidents de cybersécurité très médiatisés **n'ont pas** influencé les pratiques en matière de sécurité des données :



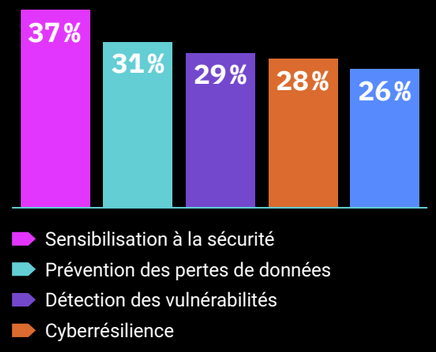
Les entreprises qui ont renforcé leurs pratiques en matière de cybersécurité en réponse à des attaques très médiatisées se sont surtout concentrées sur les outils plutôt que sur la formation et les politiques

Mesures mises en place pour renforcer la cybersécurité :



77 % des entreprises prévoient investir dans au moins une solution de sécurité au cours des deux prochaines années

Les cinq principaux domaines d'investissements prévus en matière de sécurité :



Les cinq principales mesures mises en place pour se protéger contre une violation de données :

Protection contre les logiciels malveillants	48 %
Chiffrement des données	43 %
Gestion de la sauvegarde	40 %
Outils de surveillance	39 %
Programme de sensibilisation des utilisateurs	39 %

93 % des répondants ont mis en place au moins une mesure de protection contre une possible violation de données

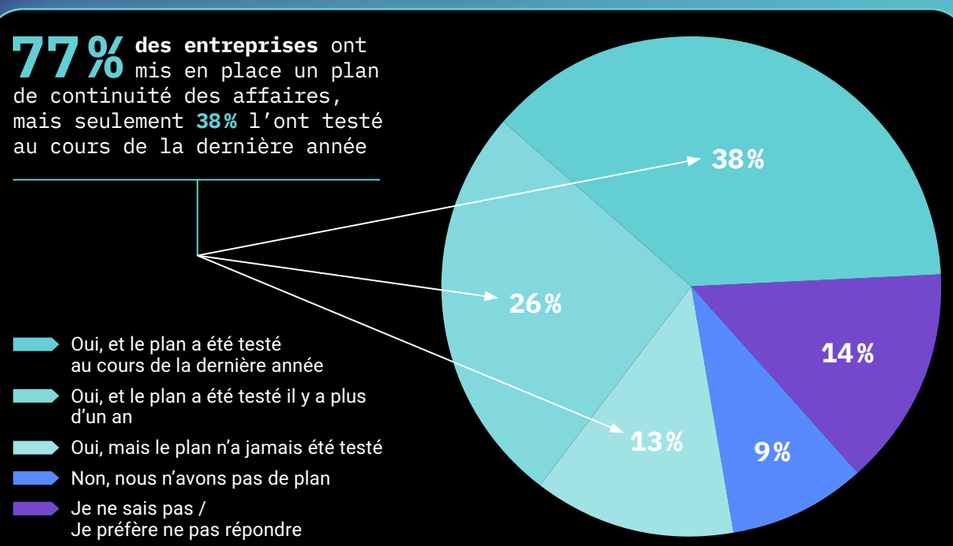
89 % des répondants déclarent avoir confiance en la capacité de leur entreprise à rester en conformité avec l'évolution des règlements en matière de confidentialité des données

60 % des entreprises détiennent maintenant une cyberassurance comparativement à **27 %** en 2025

Cependant, seulement **20 %** des polices couvrent à la fois les renseignements des clients et ceux des employés

Détient une assurance couvrant les renseignements des clients	21 %
Détient une assurance couvrant les renseignements des employés	19 %
Détient une assurance couvrant les renseignements des clients et des employés	20 %
Aucune assurance	14 %
Je ne sais pas / Je préfère ne pas répondre	26 %

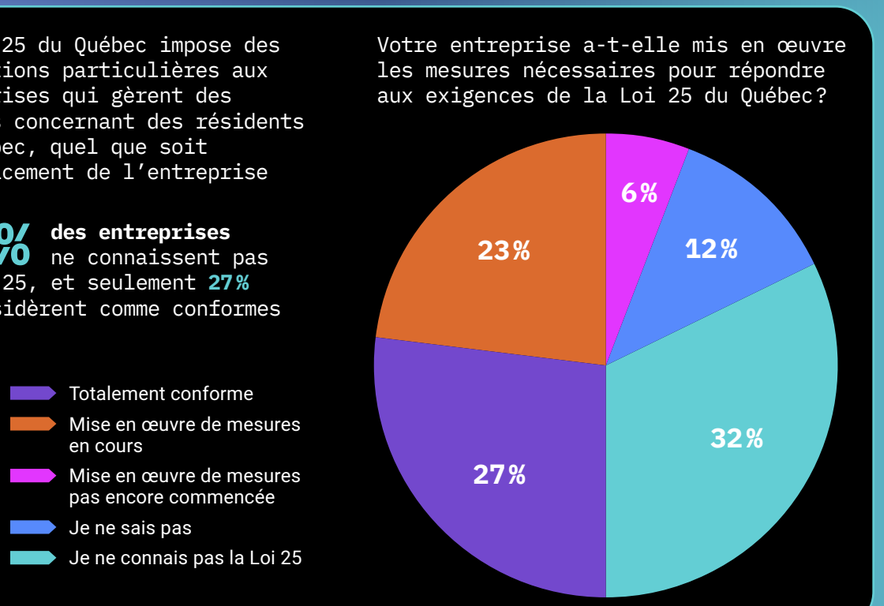
77 % des entreprises ont mis en place un plan de continuité des affaires, mais seulement **38 %** l'ont testé au cours de la dernière année



La Loi 25 du Québec impose des obligations particulières aux entreprises qui gèrent des données concernant des résidents du Québec, quel que soit l'emplacement de l'entreprise

32 % **des entreprises** ne connaissent pas la Loi 25, et seulement **27 %** se considèrent comme conformes

Votre entreprise a-t-elle mis en œuvre les mesures nécessaires pour répondre aux exigences de la Loi 25 du Québec ?



Interprétation des données

LA CONFIANCE SANS PRISE DE MESURES ENTRAÎNE DES VULNÉRABILITÉS

Même si 92 % des entreprises se déclarent confiantes en leur position en matière de cybersécurité (dont 40 % se disent très confiantes), les données révèlent un écart persistant entre la perception et la préparation réelle. Il s'avère que la confiance n'est pas synonyme de résilience. Une grande confiance, en particulier de la part des dirigeants non-TI, peut masquer une faible visibilité des outils de cybersécurité, de la formation et des structures de gouvernance de l'organisation.

Les cybermenaces sont devenues tellement omniprésentes et courantes qu'elles ont été normalisées. Les attaques ne sont plus considérées comme des événements exceptionnels, mais comme une partie intégrante de l'environnement opérationnel. Quand les organisations commencent à accepter les risques plutôt que de mettre en œuvre des mesures pour les réduire, elles arrêtent de se poser les bonnes questions. Cela peut être dangereux : lorsque les entreprises considèrent les cyberattaques comme un simple coût inhérent aux activités, elles s'exposent à des perturbations opérationnelles, à des pertes financières, à des sanctions réglementaires et à des atteintes réputationnelles sur le long terme qui sont difficilement réparables. Les entreprises doivent tenir compte des répercussions possibles des cyberattaques modernes et traiter ces dernières non pas comme des nuisances pour les TI, mais bien comme des **menaces existentielles** pour leurs opérations, leur réputation et leurs résultats.

Suivre une formation en cybersécurité est sans doute la principale mesure fondamentale que les entreprises peuvent prendre pour se protéger. **Pourtant, un tiers des entreprises canadiennes et plus de la moitié des petites entreprises n'ont pas offert de formation à leurs employés au cours de la dernière année.**

Les décideurs TI sont également beaucoup plus susceptibles que les dirigeants hors TI de déclarer qu'une formation en cybersécurité a eu lieu (76 % comparativement à 43 %). Ce résultat suggère que même si une formation a lieu, elle n'est pas toujours offerte à l'ensemble de l'organisation.

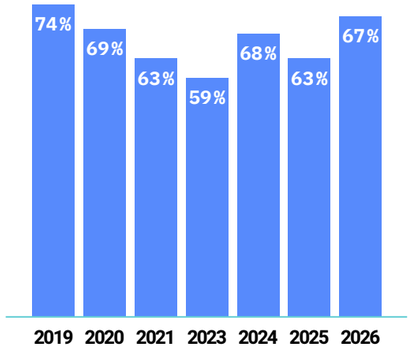
La cybersécurité demeure une priorité évidente pour les entreprises canadiennes :

- Le principal enjeu des entreprises pour la prochaine année
  À égalité avec le contrôle des coûts/dépenses
- Le troisième principal domaine où des investissements sont prévus
  Après l'IA et l'infonuagique
- Le troisième principal objectif des investissements technologiques
  Suivant de près l'optimisation et la réduction des coûts

Toutefois, **l'importance perçue de la cybersécurité ne suscite pas une prise de mesures décisives,** ce qui rend les entreprises vulnérables aux attaques.

Suivi des tendances

Malgré les menaces croissantes, la proportion des entreprises canadiennes qui offrent une formation en cybersécurité à leurs employés n'a pas encore retrouvé son niveau d'avant la pandémie :



Cet écart n'est pas anodin. Les employés demeurent l'un des points d'entrée les plus fréquents pour les cyberattaques, surtout à mesure que les menaces alimentées par l'IA deviennent de plus en plus sophistiquées, évolutives et ciblées. Ne pas offrir systématiquement la formation (et re-former) à tous les employés laisse l'organisation dans une situation de vulnérabilité critique face aux attaques.

Le manque de formation révèle un problème plus large; les mesures de cybersécurité de base ne sont pas appliquées de façon constante. Si la formation n'est pas assurée, les employés sont-ils réellement en mesure de mettre en œuvre des mesures de sécurité supplémentaires ? Et tous les outils disponibles dans l'entreprise sont-ils véritablement déployés ?

« Les menaces évoluent rapidement, et les tensions géopolitiques influencent de plus en plus la nature et la fréquence des attaques. Les entreprises qui traitent les questions de cybersécurité comme on traite une liste de vérification statique risquent d'être prises au dépourvu. Une stratégie de sécurité dynamique et mise à jour de façon continue n'est plus optionnelle : c'est un impératif opérationnel. »

Roger Ouellet, ***Directeur de la pratique sécurité, NOVIPRO***

« La formation en cybersécurité doit être traitée de la même façon que la formation en santé et sécurité au sein d'une organisation commerciale : elle doit être continue, ancrée dans la culture et toujours prioritaire. Lorsqu'elle deviendra un réflexe plutôt qu'un rappel, les organisations seront nettement mieux protégées. »

Francois Theoret, ***Vice-président exécutif, Recyclage de Métaux Intégré***

UNE MISE À NIVEAU NÉCESSAIRE

Il est encourageant de constater que **93 % des organisations ont mis en place au moins une mesure de protection contre une violation de données.** Pourtant, au sein de nombreuses entreprises, les progrès stagnent au niveau des contrôles de base, comme la détection des logiciels malveillants et le chiffrement. Ces éléments fondamentaux sont relativement abordables et plus faciles à déployer, et ils procurent des avantages visibles en matière de conformité, mais ils s'accompagnent d'un faux sentiment d'accomplissement alors que des risques plus importants subsistent.

Les capacités avancées telles que la surveillance continue, la gestion des informations et des événements de sécurité (GIES) et la prévention de la perte de données sont perçues comme étant coûteuses, complexes ou nécessitant une expertise que les entreprises ne possèdent peut-être pas. Dans plusieurs cas, les outils sont adoptés de manière isolée, sans élaborer de stratégie d'intégration permettant de transformer les alertes en détection et en réponse concrètes.

Ce déséquilibre entraîne des risques élevés : les outils de base ne suffisent plus pour contrer les attaques persistantes, automatisées et alimentées par l'IA. Pour tirer parti d'une protection adéquate, les entreprises doivent passer de la simple adoption d'outils à la priorisation de la surveillance et de la détection continues si elles veulent éviter les attaques et leurs conséquences potentiellement désastreuses.

« La Loi 25 du Québec a clairement attiré l'attention des organisations. En effet, 68 % d'entre elles la connaissent. Par contre, il ne suffit pas de connaître la loi pour protéger les données : il faut la mettre en application. Comme seulement 27 % des organisations sont totalement conformes à la loi et que la mise en œuvre des mesures est en cours dans près d'un quart des organisations, le risque réel réside dans l'écart entre l'intention et la préparation opérationnelle. »

Mark Rowan, ***PDG, Data Sentinel***

Loi 25

La Loi 25 du Québec impose des obligations particulières aux organisations qui traitent des données de résidents du Québec, y compris celles situées à l'extérieur de la province. Adoptée en 2021 et entrée en vigueur en 2024, elle demeure pourtant peu appliquée. À l'échelle canadienne, la moitié des entreprises n'ont pas mis en place les mesures requises pour s'y conformer, et un tiers ne connaissent pas la loi. Même au Québec, la situation reste préoccupante : 12 % des répondants ne la connaissent pas, 2 % n'ont pris aucune mesure et 9 % ne savent pas si leur organisation est conforme.

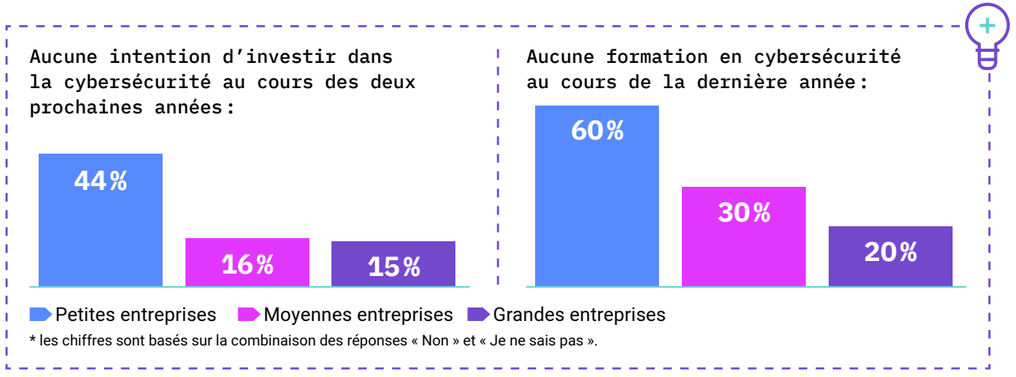
Les entreprises qui ne connaissent pas la loi ou qui n'ont pas mis en œuvre les mesures nécessaires pour s'y conformer s'exposent à de graves conséquences juridiques, et celles-ci peuvent inclure des frais importants : les sanctions en cas de non-conformité à la Loi 25 peuvent s'élever à 10 millions de dollars d'amendes ou à 2 % du chiffre d'affaires total de l'entreprise, selon le plus élevé des deux montants.

PETITE TAILLE, GRANDS RISQUES

La taille de l'entreprise demeure un facteur décisif pour atteindre la maturité en matière de cybersécurité. Les grandes entreprises sont plus susceptibles de déployer des mesures de sécurité à plusieurs niveaux, d'investir dans des outils avancés et d'organiser régulièrement des formations. Les petites entreprises, quant à elles, sont bien moins préparées, mais elles ne sont pas moins susceptibles d'être ciblées.

De nombreuses petites organisations affirment avoir des budgets limités et des priorités concurrentes. Cependant, elles sont également moins en mesure d'amortir les effets d'une attaque, qu'ils se traduisent par une interruption des activités, une perte de clients ou des coûts de reprise après sinistre.

Pour elles, le défi ne consiste pas à reproduire les architectures au niveau « enterprise », mais à développer des modèles de priorisation qui leur permettront d'investir dans des mesures réalistes et à grande incidence. Par exemple, des mesures relativement simples telles que l'externalisation de la surveillance, la mise en place de l'authentification multifacteur et la normalisation d'une cadence de formation en cybersécurité constante pour les employés peuvent contribuer de façon notable à la réduction de la vulnérabilité.



« Pour susciter un véritable engagement, nous avons adopté un format inspiré de Netflix : des vidéos concises et épisodiques conçues précisément en fonction du contexte et des défis de notre entreprise. Lorsque les employés visualisent un contenu qui reflète leur milieu de travail, ils perçoivent un message très différent de celui d'une approche unique. »

Amira Masood, ***Directrice de la technologie, The UPS Store (Canada)***

COMBLER LE FOSSÉ : PERSPECTIVES TI VS NON-TI

La cybersécurité met en lumière un écart persistant entre les décideurs TI et ceux non-TI en matière de connaissances et de perception des risques.

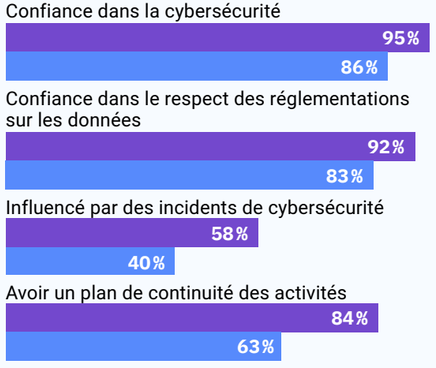
De façon générale, les responsables TI sont davantage informés des cybermenaces et des exigences réglementaires en matière de protection des données. Ils sont aussi plus susceptibles d'indiquer que leur organisation a mis en place des mesures pour y faire face et de se dire confiants dans sa capacité à respecter les cadres réglementaires.

Cet écart peut s'expliquer en partie par le fait que les grandes organisations disposent plus souvent de rôles spécialisés en technologies de l'information. Toutefois, il suggère également que les autres décideurs sont moins exposés au niveau réel de risque auquel leur organisation fait face, ainsi qu'aux mesures déployées pour y répondre.

Ce décalage peut entraîner des décisions stratégiques et financières basées sur une compréhension incomplète de la situation. **Des informations imprécises mènent inévitablement à des choix moins éclairés.**

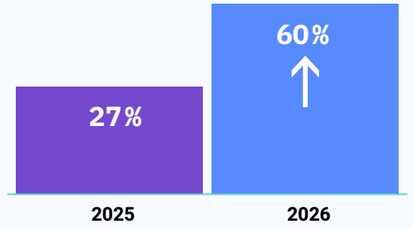
Des outils comme des tableaux de bord partagés, des indicateurs de performance en cybersécurité au niveau de la direction et des rencontres régulières sur les risques peuvent contribuer à renforcer le dialogue entre les différentes fonctions. En assurant une vision commune, les organisations peuvent mieux évaluer les risques et prioriser les bonnes stratégies de protection.

Perceptions divergentes entre les dirigeants TI (■) et non-TI (■)



CYBERASSURANCE : UN SIGNE POSITIF, AVEC QUELQUES RÉSERVES

L'un des changements les plus marquants cette année est la forte hausse de l'adoption de l'assurance cyber, qui passe de 27 % en 2025 à 60 % en 2026. Cette évolution est probablement motivée par des exigences imposées par certaines parties prenantes, comme les clients B2B ou les conseils d'administration, ainsi que par une reconnaissance croissante de la probabilité accrue des incidents cyber.



Bien que l'augmentation du nombre de cyberassurance soit une mesure positive, **l'assurance représente une prise de conscience, et non une préparation.** Les organisations peuvent se sentir protégées par une assurance sur le plan financier. Cependant, ont-elles pris en compte les risques opérationnels et d'atteinte à la réputation en cas d'attaque ?

Par exemple, parmi les entreprises assurées, seulement un cinquième d'entre elles disposent d'une couverture couvrant à la fois les renseignements des clients et ceux des employés. Si la sécurité des renseignements est compromise, les risques d'atteinte à la réputation et de perte de clients sont considérables.

De plus, même si 77 % des entreprises déclarent avoir mis en place un plan de continuité des affaires, moins de la moitié des entreprises l'ont testé au cours de la dernière année, et 13 % ne l'ont jamais testé. Un plan de continuité des affaires est de plus en plus exigé de la part des assureurs, et bien que les entreprises se soient dotées d'un tel plan, si elles ne l'ont pas testé, cela équivaut à ne pas en avoir du tout. Une procédure non testée que vos employés ne savent pas comment mettre en œuvre n'améliore aucunement la résilience de votre entreprise en cas d'attaque.

« Un casque de vélo offre une protection suffisante à basse vitesse, mais sur une moto, il est totalement inadéquat. La même logique s'applique à l'IA : à mesure que la vitesse et l'échelle de ces outils s'accroît, leur niveau de sécurité doit être ajusté en conséquence. »

Michaël Bélanger,
Spécialiste technique, Données et IA, IBM

L'assurance peut aider à absorber l'impact financier, mais en l'absence de plans de continuité testés et de mesures de sécurité proactives, elle ne peut pas protéger les entreprises contre les véritables effets d'une attaque, comme une interruption prolongée des activités, ni contre les conséquences juridiques si les plans de réponse échouent dans des conditions réelles.

LE COÛT DE L'INACTION

Les données l'indiquent clairement : **le niveau de confiance est élevé, mais la prise de mesures est parfois absente.** Ce décalage représente un risque de cybersécurité important, alors que l'IA alimente de nouvelles menaces et expose les entreprises à d'autres moyens d'attaque.

La cybersécurité n'est pas un problème de TI, mais bien une question de survie. Les entreprises qui ne considèrent pas la cybersécurité comme une préoccupation pour la continuité des affaires et comme une partie intégrante de la stratégie au niveau de la direction resteront vulnérables.

Les dirigeants TI et les dirigeants hors TI doivent travailler de concert pour s'assurer une vision commune et aligner les outils, les formations, les assurances et les politiques de données dans une stratégie cohérente. Les investissements financiers peuvent être adaptés à la taille et au niveau d'exposition au risque, et complétés par des investissements en temps, comme les tests de plans et la formation des employés, qui ont un réel impact sur la résilience opérationnelle.

Les cybermenaces font maintenant partie de notre quotidien, et le fait de tenir pour acquis que votre entreprise a déjà pris les mesures nécessaires pour se protéger représente une réelle vulnérabilité. En vérité, la cyberprotection n'est jamais terminée : elle doit toujours évoluer.

RISQUES

MAUVAISE ÉVALUATION DE L'EXPOSITION AU RISQUE

Les cybermenaces sont désormais courantes, mais de nombreux dirigeants sous-estiment leur ampleur et accordent une confiance excessive aux mesures en place. Ceux qui croient à tort que le risque est maîtrisé s'exposent à des perturbations, des pertes de clients et des atteintes à la réputation. Les dirigeants et les conseils d'administration devraient collaborer avec les TI pour remettre en question ces hypothèses par des vérifications régulières, des tests de résilience, des mises à jour et de la formation continue.

NIVEAUX DE SÉCURITÉ

Trop d'organisations investissent dans des outils de base puis relâchent leurs efforts. Or, ces outils ne suffisent pas face aux attaques alimentées par l'IA, capables de perturber les opérations et miner la confiance des clients. Une approche à plusieurs niveaux s'impose : contrôles de base, surveillance continue, plans de réponse aux incidents et outils avancés (comme la GIES et la prévention de la perte de données).

ABSENCE DE PROPRIÉTÉ PARTAGÉE

La cybersécurité est une responsabilité d'entreprise. Une attaque a des impacts organisationnels, et ne peut relever uniquement des TI. Elle doit être intégrée à la stratégie au plus haut niveau. Les dirigeants TI doivent soutenir cette approche par des rapports au conseil, des tableaux de bord partagés et une formation adaptée aux vice-présidents, afin de favoriser une compréhension commune et des décisions éclairées.

OPPORTUNITÉS

PRIORISATION DES RESSOURCES

Les entreprises doivent évaluer le coût des investissements en sécurité par rapport aux risques de ne pas agir. Des investissements stratégiques — comme un centre des opérations de sécurité, des outils de GIES ou de prévention des pertes de données, des tests de résilience et de la formation — permettent de réduire les perturbations et de protéger la valeur de l'entreprise. Les décideurs doivent prioriser selon la taille de l'organisation et établir un lien clair entre dépenses, interruptions potentielles, pertes de revenus et risques de non-conformité.

HARMONISATION DES OUTILS ET DE LA GOUVERNANCE

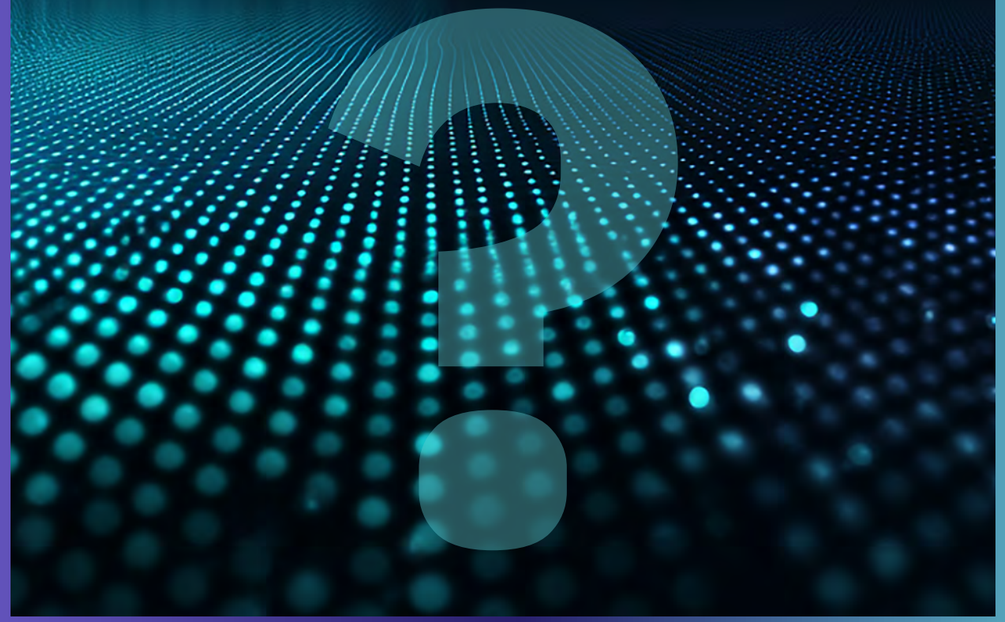
La résilience repose sur une coordination des outils, des politiques de données, des assurances et des décisions au sein d'un modèle de gouvernance intégré. Cela implique de cartographier les flux de données critiques, définir les accès, intégrer les outils clés et clarifier les rôles entre TI, direction et conseil d'administration. Un cadre cohérent renforce la capacité de réaction en cas d'incident.

AMÉLIORATION DES CONNAISSANCES INTERSERVICES

Les dirigeants hors TI peuvent mieux décider s'ils comprennent les risques et les mesures en place. Les organisations devraient adapter leurs actions : sensibilisation au niveau du conseil, simulations par rôle et scénarios, et processus budgétaires intégrant les risques. Le partage des connaissances permet d'ancrer la cybersécurité dans la stratégie et de limiter les erreurs pouvant entraîner des perturbations majeures.

La grande QUESTION

La confiance que vous accordez à vos mesures de cybersécurité repose-t-elle sur une résilience vérifiée ou sur des hypothèses ? Si un incident de cybersécurité perturbait vos opérations, votre organisation serait-elle en mesure de réagir rapidement, efficacement et en assumant des responsabilités claires ? Vos dirigeants hors TI ont-ils suffisamment de visibilité sur les risques et les contrôles de cybersécurité pour prendre des décisions éclairées au moment le plus crucial ?



06
RESSOURCES HUMAINES

IA et talents : le nouveau levier stratégique des entreprises canadiennes

Au cours des dernières années, l'intelligence artificielle a transformé le monde du travail. Pour les entreprises canadiennes, l'enjeu n'est plus seulement technologique : il est humain. Attirer, former et retenir les talents devient essentiel pour tirer parti de l'IA. Cette réalité s'inscrit dans la vision de Microsoft : l'IA agit comme un amplificateur des capacités humaines. La valeur repose moins sur les outils que sur leur usage par les équipes. Selon le Work Trend Index de Microsoft et LinkedIn, environ 75 % des travailleurs utilisaient déjà des outils d'IA en 2025 — souvent sans encadrement, révélant un écart entre potentiel et préparation.

UNE PRESSION ACCRUE SUR LES TALENTS

Les entreprises canadiennes font face à une rareté croissante des talents, amplifiée par la spécialisation et la rapidité des transformations technologiques. Les équipes doivent apprendre en continu tout en maintenant leur performance, ce qui génère pression et fatigue. L'IA ne réduit pas ce besoin — elle le transforme. Les organisations doivent miser sur des profils capables de collaborer avec ces technologies et d'en tirer de la valeur.

REPENSER LA CULTURE RH À L'ÈRE DE L'IA

Adopter l'IA sans transformer sa culture interne est voué à l'échec. Les entreprises doivent intégrer l'apprentissage au quotidien : formation continue, mentorat, partage des connaissances et temps dédié aux compétences. Microsoft structure cette transformation en combinant technologie et développement des talents. Les entreprises gagnantes investiront autant dans leurs employés que dans leurs outils.

LEVER LES CRAINTES ET MOBILISER LES ÉQUIPES

La peur de perdre son emploi demeure un frein. Les entreprises doivent être transparentes : l'IA ne remplace pas, elle redéfinit les rôles. En automatisant certaines tâches, elle permet de se concentrer sur des activités à plus forte valeur. Le leadership est clé : expliquer, rassurer et impliquer les équipes.

CIBLER LES BONS USAGES POUR MAXIMISER L'IMPACT

L'IA crée de la valeur lorsqu'elle est bien appliquée. Les entreprises doivent prioriser les fonctions où les gains sont réels, tout en préparant leurs équipes. Les outils d'IA intégrés aux environnements de travail — capables de rédiger, analyser ou automatiser — répondent aux enjeux de surcharge. Tout comme l'approche de Microsoft qui vise une intégration au flux de travail. Leur efficacité dépend toutefois de la formation.

TRANSFORMER UNE CONTRAINTE EN AVANTAGE

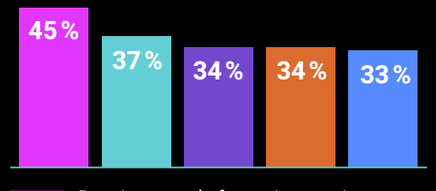
Dans un contexte de ressources limitées, l'IA représente une opportunité stratégique. Mais ce levier repose sur une approche humaine. Les organisations qui adopteront une posture de leadership — en investissant dans les talents, en structurant l'apprentissage et en intégrant l'IA de façon responsable — ne suivront pas le marché : elles en définiront les standards.

Microsoft

TABLEAU DE BORD

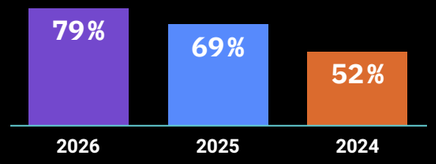
91 % **des entreprises** affirment être aux prises avec au moins un problème lié aux ressources humaines dans le domaine des TI

Les cinq principales préoccupations en matière de ressources humaines dans le domaine des TI :



79 % **des entreprises** collaborent avec une société de TI externe, une augmentation considérable par rapport aux années précédentes

Pourcentage d'entreprises collaborant avec une société de TI externe :



Les entreprises perçoivent leur partenaire TI externe comme un :

72 % **des entreprises** ont eu recours à au moins un service de ressources externes en TI au cours de la dernière année

Les cinq principales raisons de recourir à un service de ressources externes en TI :

Accélération des projets stratégiques ou critiques	33 %
Manque de compétences spécialisées à l'interne	31 %
Besoin de flexibilité ou de capacités temporaires	28 %
Manque de ressources disponibles à l'interne	23 %
Contraintes budgétaires ou optimisation des coûts	17 %

72 % **des entreprises** prévoient investir dans le renforcement des compétences des équipes de TI internes au cours des 12 à 24 prochains mois

« Dans le contexte actuel, le véritable défi du secteur des TI n'est pas seulement technique, mais aussi humain : les entreprises doivent attirer, former et fidéliser des talents capables de suivre le rythme toujours plus rapide de l'innovation, tout en comblant le déficit de compétences qui freine leur transformation. L'objectif principal est de mettre en place un écosystème intégré où la formation, l'engagement et le rendement vont de pair. »

Martin Larivière, *Vice-président des ressources humaines, NOVIPRO*

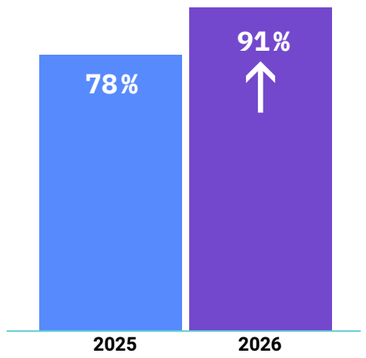
Interprétation des données

Lorsque l'on cherche à évaluer la situation des ressources humaines dans le domaine des TI en 2026, une donnée se démarque nettement : **91 % des répondants affirment être aux prises avec au moins un problème de ressources humaines au sein de leur service TI,** une augmentation considérable par rapport à l'année dernière.

L'instabilité de la main-d'œuvre dans le secteur des TI n'est plus une exception, mais bien la norme.

Le principal défi en matière de ressources humaines, signalé par 45 % des répondants, est « le besoin accru de formation continue ». Dans le paysage technologique actuel où tout évolue rapidement, les professionnels des TI doivent constamment rafraîchir leurs connaissances et leurs compétences. Faute de temps et d'argent, les entreprises ont du mal à financer les initiatives nécessaires pour maintenir leurs équipes internes à jour. Pour remédier à ce problème, 72 % des répondants prévoient de réaliser des investissements au cours des deux prochaines années afin de renforcer les compétences des équipes TI internes.

Le pourcentage de répondants aux prises avec au moins un problème lié aux ressources humaines des TI est passé de :



Bien qu'il s'agisse d'un investissement positif, les problèmes de ressources humaines sont largement répandus et profondément ancrés. Plus du tiers des répondants font état de difficultés en matière de formation, de fidélisation, de surcharge de travail et de manque de compétences spécialisées.

Il n'est donc pas surprenant que 79 % des entreprises collaborent avec un partenaire TI externe et que 72 % d'entre elles aient eu recours à des services de ressources externes en TI au cours de la dernière année. Ces ressources externes peuvent être d'importants partenaires stratégiques; en effet, 22 % des répondants considèrent leur société de TI externe comme telle. Les raisons invoquées pour le recours à des services de ressources externes en TI (telles que l'accélération de projets critiques et le besoin de capacités temporaires) suggèrent toutefois une approche réactive plutôt que stratégique. **(Pour voir la donnée complète voir la page 64 du tableau de bord)**

Un cycle inquiétant

Pour briser ce cycle, il faut trouver un équilibre stratégique entre l'amélioration des compétences internes et le soutien externe, plutôt que de miser sur des solutions provisoires

- Les équipes surchargées et insuffisamment formées s'épuisent
- Les employés épuisés quittent l'entreprise
- Les départs sont comblés par des ressources externes
- Les capacités internes diminuent

Par ailleurs, 33 % des entreprises se disent préoccupées par leur « dépendance aux ressources externes », ce qui laisse penser que ces ressources sont utilisées comme une béquille plutôt que comme un moyen de renforcer les capacités existantes. La plupart des entreprises ne font pas appel à des partenaires externes pour des raisons stratégiques ou financières, mais parce qu'elles doivent combler des lacunes immédiates en matière de capacités ou de compétences.

COMBLER LE FOSSÉ : PERSPECTIVES TI VS NON-TI

La solidité d'une stratégie TI repose sur la capacité de l'organisation à former et à maintenir les équipes responsables de son exécution. Pourtant, de nombreuses entreprises sous-estiment l'impact des divergences de perspectives entre dirigeants TI et non-TI sur sa mise en œuvre.

Cette année, 21 % des dirigeants hors TI affirment ne pas connaître les défis en matière de RH auxquels leur service TI est confronté et 7 % d'entre eux estiment qu'il n'y a « aucun problème particulier » – un point de vue qu'aucun dirigeant TI ne partage.

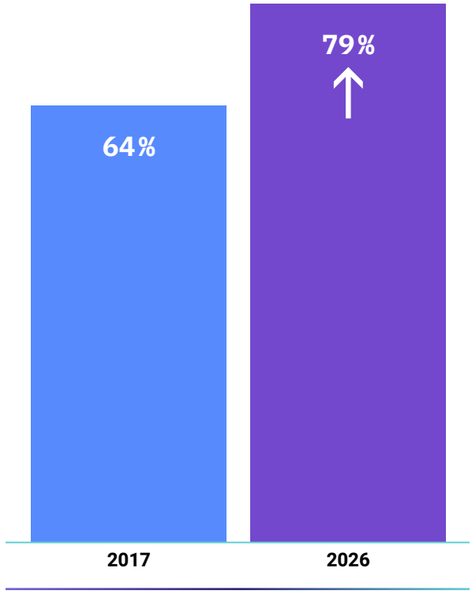
Ce décalage va au-delà d'un simple manque de visibilité; il a des conséquences directes sur les performances. Lorsque les contraintes en matière de personnel échappent à l'œil de la direction, les équipes TI se voient confier des initiatives complexes

« L'un des principaux défis auxquels nous faisons face est la pression disproportionnée qui pèse sur les services des TI, qui doivent souvent fonctionner avec des équipes beaucoup plus restreintes que ne l'exige la charge de travail. »

Paul Whitney, ***Directeur informatique, TST-CF Express***

Suivi des tendances

Le nombre d'entreprises collaborant avec une société de TI externe n'a cessé d'augmenter au fil des ans



sans disposer des ressources ou des compétences nécessaires pour les mener à bien, ce qui accroît les risques liés à la livraison, ralentit les progrès et contribue à l'épuisement professionnel.

Sans une compréhension claire des impacts de la pénurie de talents et de la charge de travail sur les échéanciers et les résultats, les dirigeants hors TI peinent à prendre des décisions d'investissement éclairées à long terme. Les enjeux RH en TI sont alors perçus comme des contraintes internes, plutôt que comme des risques critiques pour l'exécution des activités. Pour combler cet écart, il est essentiel d'instaurer un dialogue continu reliant explicitement les capacités des équipes, les priorités stratégiques et les engagements de livraison, afin d'intégrer pleinement la planification des talents TI à celle de l'entreprise. Sans cet alignement, même les stratégies les mieux définies risquent d'échouer — non par manque d'ambition, mais faute de capacités pour les concrétiser.

BRISER LE CYCLE

Au vu de l'écrasante majorité d'entreprises faisant état de défis liés aux ressources humaines, la pression exercée sur les services TI n'est pas seulement une tendance préoccupante, mais bien une crise cyclique et profondément ancrée. Toutefois, une fois ce schéma identifié, il devient possible de le briser.

Les organisations de toutes tailles doivent investir dans leur personnel et créer un environnement propice à l'apprentissage continu. Cela implique d'intégrer délibérément l'apprentissage dans les activités quotidiennes : consacrer du temps à la formation, encourager le transfert de connaissances, favoriser le mentorat, réduire la microgestion et instaurer une culture fondée sur la confiance. Cet investissement permettra de renforcer les connaissances et les capacités internes, et donc de réduire la dépendance aux ressources externes. Il favorisera également une compréhension approfondie des nouvelles technologies, qui est essentielle dans le paysage actuel en constante évolution. Une réussite durable repose sur l'étendue des connaissances, pas seulement sur la rapidité d'adoption.

Les organisations qui sortiront gagnantes ne sont pas celles qui échappent aux défis liés aux RH dans le domaine des TI, mais celles qui s'y attaquent de front en investissant judicieusement du temps et des ressources.

« Nous observons une transition notable chez les PME, qui délaissent les services gérés au profit de partenariats consultatifs. À mesure que les entreprises rapatrient la gestion des TI à l'interne, la demande en talents internes augmente, dans un contexte où le recrutement et la rétention de ces profils constituent déjà l'un des défis les plus pressants du secteur. »

Ian Christensen, ***Gestionnaire des partenaires infonuagiques, Arrow Electronics***

RISQUES

NORMALISATION DES DÉFIS LIÉS À LA MAIN-D'ŒUVRE EN TI

Comme la grande majorité des services TI sont aux prises avec des défis liés aux ressources humaines, les entreprises risquent de considérer cette situation comme la norme plutôt que de chercher à s'attaquer aux causes profondes du problème. Si les problèmes persistent, les employés se retrouveront constamment contraints à réagir à des défis à court terme, ce qui réduira leur rendement et les empêchera de se consacrer à la réalisation d'objectifs stratégiques à long terme.

MANQUE DE FORMATION ET ÉPUISEMENT PROFESSIONNEL

Plus du tiers des entreprises font état de difficultés en matière de formation, de fidélisation, de manque de compétences spécialisées et de surcharge de travail. Ces défis s'alimentent mutuellement, créant ainsi un cercle vicieux difficile à briser. Les entreprises prises dans ce cercle vicieux d'épuisement professionnel et de roulement de personnel seront confrontées à une perte de savoir-faire et de productivité, et se retrouveront distancées par leurs concurrents qui ont investi dans la formation continue et le mentorat de leurs employés.

DÉPENDANCE AUX ÉQUIPES EXTERNES

Face à des problèmes croissants, les services TI se tournent vers des ressources externes. Bien que ce soutien puisse permettre de faire avancer les projets, son utilisation comme solution provisoire plutôt que comme partenaire stratégique ne fait que fragiliser les capacités internes et gonfler les coûts. Les organisations peuvent se retrouver dépendantes d'un soutien externe permanent, ce qui ralentit la prise de décision et réduit leur capacité à innover et à se développer efficacement.

OPPORTUNITÉS

UN PLAN CLAIR POUR RÉPONDRE AUX PRÉOCCUPATIONS EN MATIÈRE DE RH

Plutôt que de normaliser les enjeux RH, votre organisation doit porter un regard lucide sur les problèmes structurels et définir un plan concret pour y remédier. En TI, ces enjeux influencent les capacités, les budgets et la performance. Prioriser la gestion des talents devient un levier stratégique : les entreprises qui s'y engagent gagnent en efficacité et renforcent leur capacité à innover, à croître et à rester compétitives dans un environnement technologique en constante évolution.

AMÉLIORATION CONTINUE DES COMPÉTENCES

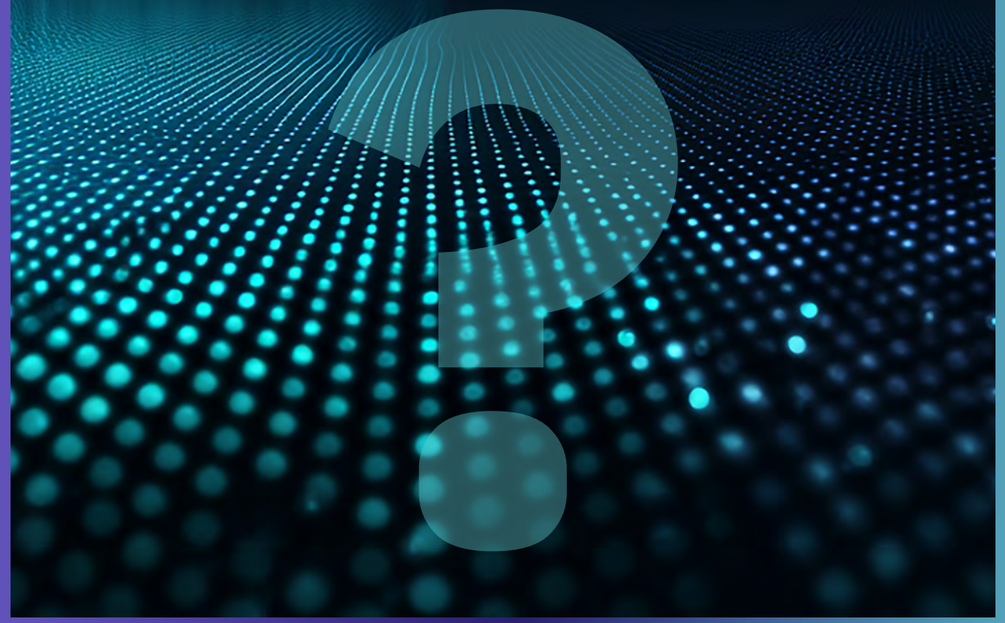
La technologie évolue rapidement; la formation ponctuelle ne suffit plus. Les organisations doivent faire du développement continu des compétences un pilier stratégique. Cet investissement soutient l'engagement, la motivation et la performance des équipes. À long terme, il permet de développer des talents à l'interne et de renforcer l'autonomie des entreprises canadiennes dans un contexte technologique mondial.

MODÈLES HYBRIDES DE DOTATION EN PERSONNEL

Un recours excessif à des ressources externes peut entraîner des coûts élevés, fragmenter la culture et limiter le transfert de connaissances. Plutôt que d'agir de façon réactive, les entreprises gagnent à adopter des modèles hybrides équilibrant talents internes et soutien externe. Cette approche améliore le contrôle des coûts, la flexibilité des ressources, la rapidité d'exécution et renforce une fonction TI plus résiliente et cohérente, capable de s'adapter aux besoins changeants.

La grande QUESTION

Votre entreprise dispose-t-elle des ressources et des compétences internes nécessaires pour mettre en œuvre votre stratégie de TI, ou est-elle freinée par des lacunes en matière de ressources humaines ? Quels membres de votre équipe doivent mieux comprendre vos défis et adopter une approche stratégique en matière de RH en lien avec les TI ?



07

PLEINS FEUX SUR LES SECTEURS D’ACTIVITÉ

Pleins feux sur les secteurs d’activité

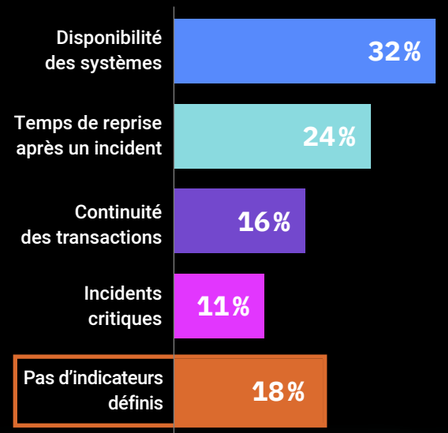
La technologie transforme tous les aspects de l’économie canadienne, mais son incidence est particulièrement visible dans les secteurs où la fiabilité, l’efficacité, l’intégrité des données et la sécurité sont essentielles.

Pour la 10e édition du Portrait TI, nous avons demandé pour la première fois aux décideurs des secteurs de la finance, manufacturier et des soins de santé d’examiner de plus près leurs pratiques TI. Les pages suivantes présentent les résultats de ces nouvelles questions, en soulignant comment les organisations canadiennes dans ces secteurs importants gèrent la modernisation et les risques, et ciblent les occasions de transformation.

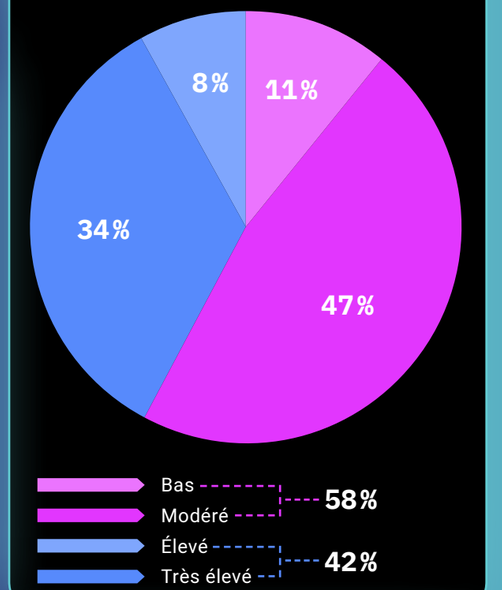
Chaque secteur connaît une évolution numérique rapide, façonnée par des systèmes hérités, des cybermenaces croissantes, des exigences changeantes en matière de main-d’œuvre et des attentes grandissantes envers les activités connectées et axées sur les données. Si l’adoption est inégale, la direction de la transformation est indubitable : la technologie devient un facteur déterminant de la résilience opérationnelle, de la compétitivité et de la croissance à long terme dans ces trois secteurs.

TABLEAU DE BORD

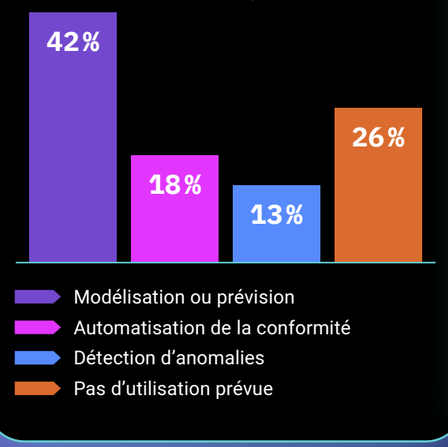
Indicateurs de résilience opérationnelle des systèmes critiques



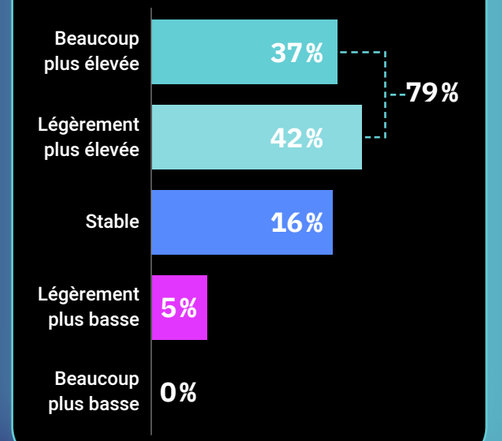
Niveau d'automatisation des processus transactionnels ou décisionnels



Utilisations actuelles ou prévues de l'IA / de l'analyse avancée des données pour la gestion des risques



Pression exercée par la cybersécurité sur les équipes TI : aujourd'hui vs il y a 2 ans



Interprétation des données : Finances

Le secteur financier canadien continue de se démarquer par la maturité de ses capacités informatiques. Les données de cette année montrent que les institutions financières sont plus susceptibles que celles des autres secteurs d'avoir mis en place des pratiques et des outils technologiques avancés. Toutefois, les nouvelles questions introduites cette année, spécifiques au secteur, révèlent une évolution inégale au sein des organisations financières.

Prenons l'exemple de l'automatisation : bien que certaines institutions aient adopté des processus hautement efficaces et axés sur la technologie, la majorité demeure à un niveau d'automatisation faible à modéré. Les organisations qui ont su se libérer des systèmes hérités et d'autres contraintes pour standardiser l'automatisation sont mieux positionnées pour renforcer leurs services numériques, réduire les risques opérationnels et répondre avec agilité aux pressions du marché. À l'inverse, celles qui n'ont pas encore effectué cette transition risquent de prendre un retard croissant, à mesure que les attentes des clients et la dynamique concurrentielle évoluent.

L'une de ces dynamiques concurrentielles est, et restera, la sécurité. La pression exercée sur les équipes TI en matière de cybersécurité s'est considérablement intensifiée au cours des deux dernières années. Les institutions financières protègent les moyens de subsistance des citoyens tout en faisant face à des menaces alimentées par l'IA, à l'instabilité géopolitique et à une dépendance croissante à l'infonuagique ainsi qu'à des écosystèmes tiers, qui élargissent la surface d'attaque. Le Bureau du surintendant des institutions financières (BSIF) ayant identifié la sécurité comme principal risque pour 2025, les institutions doivent répondre à des attentes toujours plus élevées en matière de renforcement des défenses, d'amélioration de la réponse aux incidents et de développement de capacités proactives en renseignement sur les menaces.

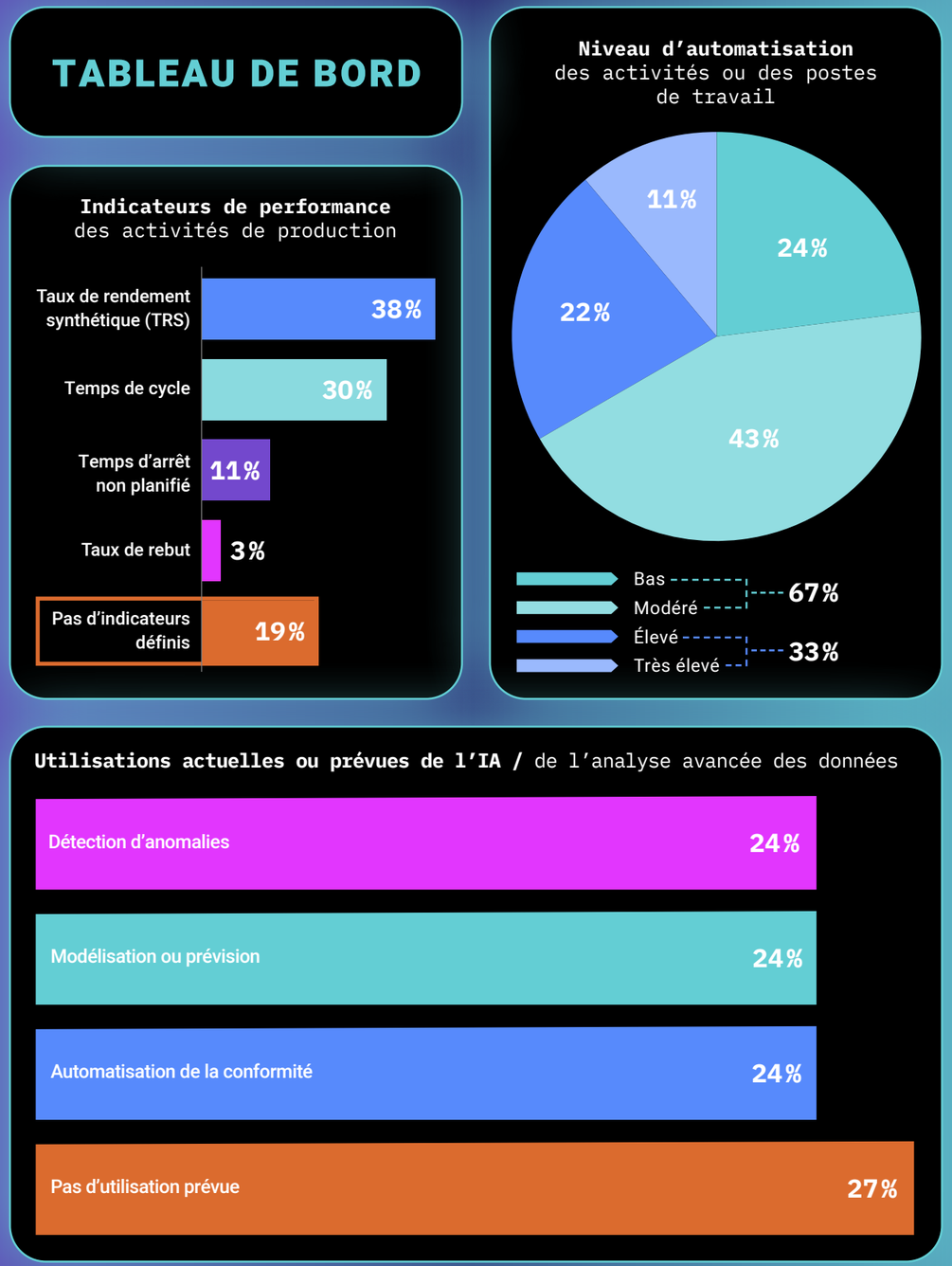
Compte tenu du niveau de menace actuel, il est préoccupant de constater que 18 % des institutions ne suivent aucun indicateur formel en matière de robustesse opérationnelle. Cette dimension demeure encore insuffisamment structurée dans le secteur. Or, étant donné le rôle systémique des services financiers, cette lacune ne relève pas d'un simple enjeu technique, mais constitue une vulnérabilité significative. Les organisations financières doivent impérativement définir des indicateurs clés et en assurer un suivi rigoureux et continu afin de renforcer leur capacité à faire face aux perturbations.

Alors que les analyses et les capacités de prévision avancées gagnent du terrain, une large part du secteur hésite encore à intégrer l'IA dans la gestion des risques, ou n'y est pas prête. Cette réticence pourrait accentuer les écarts de performance au fil du temps, d'autant plus que l'IA devient centrale pour la détection des fraudes, l'automatisation de la conformité et l'évaluation des risques en temps réel.

Les institutions doivent ainsi arbitrer entre les gains concurrentiels d'une adoption maîtrisée et les risques liés à une mise en œuvre fragmentée ou insuffisamment préparée. Déployer des solutions d'IA à grande échelle sans que les équipes en comprennent pleinement les mécanismes peut introduire de nouveaux risques. À l'inverse, ne pas recourir à l'IA pour contrer des menaces elles-mêmes alimentées par l'IA expose inévitablement les organisations à des vulnérabilités croissantes.

Pour dépasser ce paradoxe, les institutions financières devraient intégrer les capacités de détection et de prévention de la fraude basées sur l'IA dans des cadres de gouvernance solides, tout en les accompagnant d'une formation généralisée des employés à l'échelle de l'organisation.

Dans l'ensemble, ces tendances dépeignent un secteur technologiquement capable, mais inégalement transformé. Les organisations qui parviendront à combler ces écarts bénéficieront d'un avantage concurrentiel durable. La modernisation des systèmes hérités, la normalisation de l'automatisation, le déploiement de l'IA dans un cadre de gouvernance rigoureux et l'intégration d'une résilience mesurable dans les activités TI permettront non seulement de réduire les risques, mais aussi de renforcer significativement la qualité, la rapidité et la justesse des décisions à l'échelle de l'entreprise.



Interprétation des données : Manufacturier

Le secteur manufacturier canadien évolue dans un contexte marqué par une forte pression concurrentielle, des pénuries de main-d'œuvre et une volatilité persistante des chaînes d'approvisionnement mondiales, ce qui accélère le besoin de transformation numérique. Toutefois, les données révèlent que les pratiques de mesure, les niveaux d'automatisation et l'adoption de l'IA progressent de manière inégale selon les organisations.

La mesure de la performance illustre clairement cette maturité numérique inégale. Si de nombreuses organisations suivent des indicateurs de production clés, une part importante ne dispose toujours pas de métriques clairement définies. Cette absence est loin d'être anodine : sans visibilité cohérente sur la performance des équipements, les cycles de production ou la qualité, les fabricants peinent à identifier les goulots d'étranglement, à maîtriser leurs coûts ou à justifier leurs investissements de modernisation par un retour sur investissement clair. Dans un contexte où l'excellence opérationnelle devient essentielle pour rester compétitif à l'échelle mondiale, ce manque de structuration constitue une faiblesse stratégique majeure.

L'automatisation suit une dynamique similaire. Bien que la robotique avancée et les équipements connectés gagnent du terrain, la majorité des fabricants demeurent à un niveau d'automatisation faible à modéré. Cette réalité reflète les contraintes du secteur manufacturier canadien, où des équipements vieillissants, des limites d'investissement et des environnements de production fragmentés freinent la transition vers des usines pleinement intelligentes.

Pourtant, les opportunités ne manquent pas. Une automatisation ciblée — notamment sur les tâches répétitives, les goulots d'étranglement et le contrôle qualité — permet de réduire les temps d'arrêt, d'améliorer la productivité et d'atténuer les pénuries de main-d'œuvre. Les organisations qui agissent rapidement seront mieux positionnées pour stabiliser leurs opérations et gagner en agilité.

L'adoption de l'IA progresse elle aussi, mais pas encore au rythme nécessaire pour en exploiter tout le potentiel. Plusieurs manufacturiers explorent déjà la détection d'anomalies, la prévision et l'automatisation de la conformité, mais un quart d'entre eux ne prévoit toujours pas d'utiliser l'IA ou l'analyse avancée. Cette hésitation risque d'accentuer l'écart entre les adopteurs précoces et ceux qui s'en tiennent à des approches traditionnelles et réactives. Plutôt que de viser des déploiements massifs, les fabricants les plus avancés privilégient des cas d'usage ciblés, comme la maintenance prédictive, la prévision de la demande et la détection des anomalies — des domaines où l'IA génère des gains opérationnels tangibles et renforce la compétitivité.

Parallèlement, les organisations doivent composer avec un risque croissant en matière de cybersécurité, amplifié par la multiplication des environnements connectés et automatisés. Une transformation trop rapide, dictée par la pression concurrentielle, peut accroître l'exposition à des failles critiques.

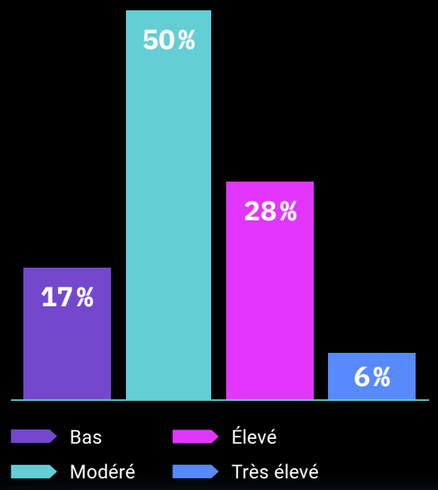
Dans l'ensemble, la tendance est claire : le secteur manufacturier canadien progresse sur le plan technologique, mais avec d'importantes disparités. Entre fragmentation des avancées et occasions manquées, se dessine néanmoins une trajectoire nette pour les organisations qui investissent dans leurs capacités numériques : davantage de résilience, de productivité et de compétitivité.

« Nous n'en sommes pas encore au point où l'on peut se fier aux résultats de l'IA sans vérification. Agir sur la base d'informations non vérifiées pourrait être très coûteux sur le plan financier, opérationnel ou réputationnel. Il existe une tension fondamentale à laquelle les organisations doivent faire face : la pression exercée pour que les systèmes continuent de fonctionner et que les modèles soient à jour, par opposition à la discipline requise pour vérifier ce que ces modèles produisent réellement. La confiance doit être gagnée progressivement, et non pas tenue pour acquise. »

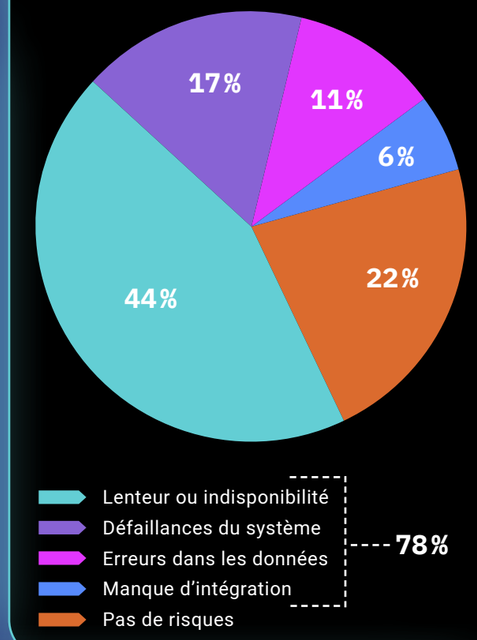
Don Bower, ***Chef d'équipe réseau, Vision Extrusions***

TABLEAU DE BORD

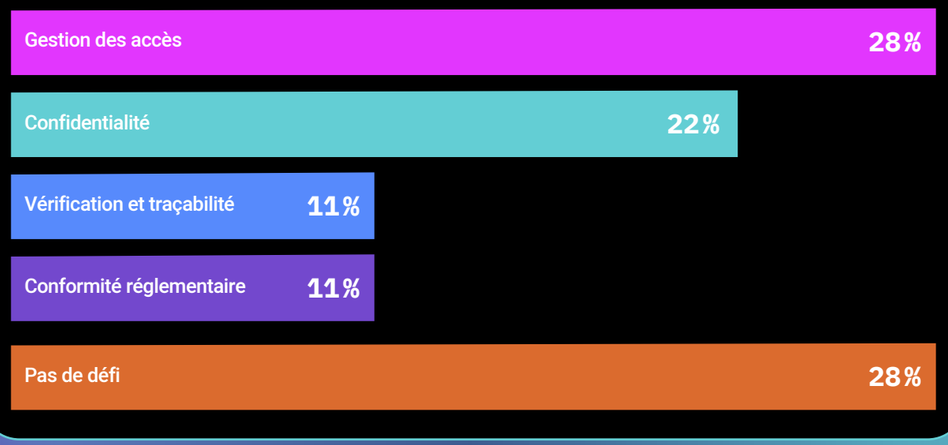
Niveau d'interopérabilité entre les systèmes cliniques et administratifs



Risques technologiques affectant le plus la qualité ou la continuité des soins



Défis liés à la protection des données des patients



Interprétation des données : Soins de la santé

Le secteur canadien des soins de santé traverse une période de pression numérique intense, où les menaces croissantes de cybersécurité, les systèmes fragmentés et les limites de l'infrastructure se combinent aux attentes croissantes pour des soins axés sur les données et centrés sur le patient. Les données mettent en évidence un secteur qui reconnaît ses vulnérabilités, mais qui n'a pas encore atteint le niveau de maturité numérique requis pour des activités harmonieuses et résilientes.

La protection des données des patients reste une préoccupation centrale. Une nette majorité des répondants font état d'au moins un problème lié à la protection des informations sensibles, ce qui souligne l'exposition du secteur aux cyberattaques et aux incidents de confidentialité. Le secteur des soins de santé est toujours l'un des plus ciblés au monde. Il est donc remarquable et préoccupant que plus d'un quart des personnes interrogées n'aient signalé aucun problème lié à la protection des données des patients. Cette déconnexion peut refléter des lacunes en matière de sensibilisation plutôt qu'une absence de risque, exposant les organisations à des interruptions potentielles de services, à des conséquences réglementaires et à une perte de confiance de la part des patients en cas d'incident de confidentialité.

Les problèmes d'interopérabilité compliquent encore le paysage numérique. Deux tiers des organisations décrivent leurs systèmes cliniques et administratifs comme étant faiblement ou modérément intégrés. Cette fragmentation limite le flux d'informations entre les différents environnements de soins, ce qui accroît la charge administrative, la duplication des efforts et réduit la capacité du système à fournir des soins coordonnés en temps opportun. Pour y remédier, il faut non seulement investir dans la technologie, mais aussi normaliser les pratiques en matière de données et renforcer la gouvernance au sein des établissements.

Les risques technologiques affectant la qualité des soins sont également largement reconnus. La plupart des personnes interrogées identifient au moins un risque : la lenteur ou l'indisponibilité du système apparaissant comme la préoccupation la plus fréquente. Dans un environnement clinique où les minutes comptent, les retards du système peuvent directement perturber les soins et avoir une incidence sur les résultats des patients. La fiabilité de l'infrastructure TI doit être considérée comme un élément clé de la performance clinique, et non comme un simple soutien opérationnel.

Dans l'ensemble, ces résultats décrivent un secteur des soins de santé qui progresse, mais de façon déséquilibréee. La fragmentation des systèmes, l'instabilité opérationnelle et les risques de cyberattaques sont importants, mais les occasions de progrès le sont tout autant. Les investissements dans l'interopérabilité, la cybersécurité et la modernisation des infrastructures peuvent permettre de mieux coordonner les soins, de réduire la charge de travail des cliniciens et d'améliorer les résultats pour les patients. Bien que l'échantillon soit de petite taille pour ces données et que ces dernières ne puissent indiquer qu'une direction, le message est clair : dans le secteur des soins de santé, la maturité des TI est essentielle pour les soins aux patients.

« En tant qu'ancien DSI d'hôpital, je sais à quel point il est essentiel de bien définir à qui s'adressent les différents investissements numériques. Les systèmes de back-office et les stratégies d'intégration jouent un rôle important dans la normalisation et la maîtrise des coûts, notamment pour les bailleurs de fonds et les gouvernements. En revanche, l'intégration entre les systèmes administratifs et cliniques doit être réfléchie et démontrer une valeur concrète pour les soins de première ligne; elle ne devrait pas être réalisée uniquement pour assurer une cohérence technique. »

Tyson J. Roffey, ***VP Santé numérique, Nova Networks***

Conclusion

La technologie n'est plus simplement une nouveauté que les organisations « adoptent ». C'est quelque chose qu'elles exploitent, qu'elles gèrent et avec laquelle elles vivent tous les jours. Les conclusions du rapport Portrait TI de cette année mettent en évidence une réalité simple, mais dérangeante : les occasions et les risques les plus importants liés aux technologies se situent aujourd'hui carrément en dehors du service informatique.

Les chefs d'entreprise approuvent des budgets plus importants, soutiennent des initiatives ambitieuses et font de la technologie une priorité stratégique. Mais en 2026, un schéma se répète : l'intention est là, mais les structures pour la concrétiser ne le sont souvent pas. L'infonuagique, l'IA, la cybersécurité et la gouvernance des données façonnent déjà l'exposition financière, le risque de conformité, la confiance des clients et la résilience opérationnelle. Pourtant, trop d'organisations traitent encore ces questions comme des questions techniques plutôt que comme des questions commerciales.

La prochaine phase de la transformation numérique appelle une évolution du rôle des dirigeants. Elle exige d'aller au-delà des orientations générales et de poser des questions plus exigeantes :

- **Comprenons-nous réellement les risques technologiques auxquels nous faisons face ?**
- **Les responsabilités sont-elles clairement établies en cas de problème ?**
- **Disposons-nous à l'interne des compétences nécessaires pour mettre en œuvre ce que nous approuvons ?**

Il s'agit également d'un moment important en matière de leadership. Les équipes informatiques sont soumises à une pression constante et doivent répondre à des attentes qui ne peuvent être satisfaites uniquement par des outils ou par l'externalisation. Sans un investissement réfléchi dans le personnel, la gouvernance et la coordination interfonctionnelle, la stratégie reste bloquée quelque part entre l'approbation et l'exécution.

Pour l'avenir, le message que les chefs d'entreprise doivent retenir est clair : les résultats technologiques sont désormais des résultats commerciaux. Les organisations qui réussiront seront celles dans lesquelles les dirigeants s'engagent tôt, se tiennent informés et traitent les décisions technologiques avec la même discipline que les décisions financières ou opérationnelles. La question n'est plus de savoir si la technologie a de l'importance, mais si les dirigeants sont prêts à s'occuper des changements qu'elle entraîne. Les organisations qui adoptent cette approche ne se contenteront pas d'atténuer les risques, mais elles bénéficieront également d'une plus grande souplesse et d'un avantage concurrentiel.

Étude menée par :

NOVIPRO Léger

En collaboration avec :

NOVA NETWORKS

Avec le support de nos partenaires :

Platine

IBM

Or

Microsoft

Argent

A10

Bronze

DATA SENTINEL