2025

PORTRAIT.TI

9e édition

RAPPORT CANADIEN DES TI

DES DONNÉES POUR ORIENTER VOS DÉCISIONS STRATÉGIQUES EN TI

GROUPE NOVIPRO

Léger

IBM

NOTE SUR LA MÉTHODOLOGIE

Les données présentées dans ce rapport ont été recueillies dans le cadre d'un sondage en ligne mené par Léger, du 19 novembre au 2 décembre 2024, 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 303 décideurs spécialisés en TI, 77 gestionnaires non spécialisés en TI et 78 décideurs non spécialisés en TI qui ne sont pas gestionnaires. Il convient de noter qu'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 458 répondants (échantillon en ligne) aurait une marge d'erreur globale de ± 4,58 %, 19 fois sur 20. La marge d'erreur augmenterait toutefois pour les sous-groupes.

«Le Portrait TI 2025 est arrivé, exactement au moment où les entreprises canadiennes en ont le plus besoin. Notre rapport phare, qui en est à sa neuvième édition, offre un aperçu actuel des facteurs de transformation du paysage des TI au Canada et des choix stratégiques auxquels les dirigeants sont confrontés dans un environnement de plus en plus complexe.»

Chers lecteurs,

Le Portrait TI 2025 est arrivé, exactement au moment où les entreprises canadiennes en ont le plus besoin. Notre rapport phare, qui en est à sa neuvième édition, offre un aperçu actuel des facteurs de transformation du paysage des TI au Canada et des choix stratégiques auxquels les dirigeants sont confrontés dans un environnement de plus en plus complexe.

Cette année, le message est clair : la réussite des entreprises repose sur l'équilibre. En effet, les entreprises sont amenées à se moderniser rapidement, à adopter l'IA et à se protéger contre les cybermenaces grandissantes, tout en gérant les pressions budgétaires, les pénuries de ressources qualifiées et les tensions géopolitiques croissantes. Nos données montrent que les organisations canadiennes doivent trouver un juste équilibre entre l'innovation, la productivité et la sécurité.

Les conflits géopolitiques, les difficultés économiques et les incertitudes commerciales entre les États-Unis et le Canada indiquent clairement que les organisations doivent passer de la réactivité à la résilience. Avec la souveraineté de l'infonuagique, les données provenant de différents pays et la conformité transfrontalière mises en évidence, les entreprises canadiennes ne peuvent plus se permettre de prendre des décisions stratégiques en matière de TI sans comprendre pleinement les risques.

Notre rapport, qui s'appuie sur les observations de plus de 450 répondants de partout au Canada et de tous les secteurs d'activité, vise à guider concrètement les dirigeants d'entreprise afin qu'ils puissent composer avec ces exigences. Que vous souhaitiez élaborer une stratégie à long terme ou réagir à des risques à court terme, les résultats de cette année vous aideront à réajuster vos actions en toute confiance.

Je tiens à remercier sincèrement Léger, IBM et nos nombreux partenaires et contributeurs d'avoir participé à nouveau à cet effort collectif.

En cette année marquée par l'incertitude, le Portrait TI 2025 sera votre guide pour atteindre l'équilibre et renforcer votre résilience.

ALAIN CORMIER
Président-directeur général,
Groupe NOVIPRO

GROUPE NOVIPRO

« Chez IBM, nous pensons que les organisations doivent investir dans les stratégies technologiques appropriées, pas uniquement dans des outils, mais aussi dans des solutions infonuagiques et des modèles d'IA spécialisés, évolutifs et sécuritaires. »

DEB PIMENTEL
Présidente,
IBM Canada

Chers lecteurs,

IBM Canada est fière de soutenir les entreprises canadiennes alors qu'elles assistent à une évolution rapide des technologies. Dans tous les secteurs d'activité, les organisations doivent s'adapter, innover et rester compétitives au sein d'un environnement façonné par l'IA, la cybersécurité et la transformation infonuagique. Maintenant plus que jamais, les organisations canadiennes ont la possibilité de mettre en œuvre des technologies, en particulier l'IA, pour stimuler leur productivité, renforcer leur résilience et propulser leur croissance à long terme.

C'est pourquoi je suis ravie de vous présenter la dernière édition du rapport Portrait TI, une collaboration entre IBM Canada et le Groupe NOVIPRO. Ce rapport constitue une ressource stratégique offrant de l'information sur les nouveaux défis, les priorités d'investissement et le rôle de la technologie dans la création de l'avenir des entreprises canadiennes.

Chez IBM, nous pensons que les organisations doivent investir dans les stratégies technologiques appropriées, pas uniquement dans des outils, mais aussi dans des solutions infonuagiques et des modèles d'IA spécialisés, évolutifs et sécuritaires. L'IA a le potentiel de transformer le mode de fonctionnement des entreprises, mais pour en tirer pleinement parti, celles-ci doivent choisir les modèles qui répondront à leurs problèmes tout en établissant un équilibre entre la performance, les coûts et la fiabilité.

J'espère que ce rapport vous fournira de l'information précieuse qui vous aidera à réaliser des investissements stratégiques et judicieux dans les technologies, ainsi qu'à promouvoir l'innovation et la réussite.

Bonne lecture de l'édition 2025 du rapport Portrait TI!

Table des matières

À propos des résultats du rapport de 2025

La tendance nette qui se dégage du sondage de cette année mené auprès d'entreprises canadiennes est **l'équilibre**. Les entreprises canadiennes évoluent dans des environnements complexes et peinent à concilier les opportunités prometteuses offertes par les nouvelles technologies émergentes avec les contraintes liées aux coûts, aux ressources limitées et aux préoccupations en matière de cybersécurité.

Des cyberattaques marquées par une plus grande sophistication aux nouveaux modèles d'intelligence artificielle (IA) arrivant sur le marché (indépendamment de la taille, du secteur d'activité ou de l'emplacement géographique de l'entreprise), le sondage Portrait TI de cette année démontre clairement que la **cybersécurité, l'IA et la modernisation sont au cœur des préoccupations des services TI en général.**

PARMI LES CINQ PRÉOCCUPATIONS PRINCIPALES : la cybersécurité, l'IA et la modernisation figurent au premier plan			
	Défis de l'entreprise	**Investissements technologiques prévus**	**Secteurs prioritaires pour la modernisation**
1	**Sécurité**	**IA**	**Solutions de cybersécurité**
2	Budget	Infonuagique	Infrastructure et services infonuagiques
3	Mise à niveau/remplacement de solutions technologiques	**Solutions/services de sécurité**	**IA et apprentissage machine**
4	**Implantation de projets d'IA**	Solutions d'infrastructures	**Modernisation des systèmes existants**
5	**Modernisation des applications**	**Modernisation des applications**	Mises à niveau du réseau et de l'infrastructure

Les entreprises canadiennes savent qu'elles doivent investir dans les technologies pour demeurer efficaces, productives et rentables afin de continuer à prospérer. Les technologies qui étaient autrefois réservées aux grandes entreprises disposant de plus de ressources, comme l'infonuagique et l'analyse de données avancée, sont aujourd'hui considérées comme des éléments indispensables, et non plus comme des éléments non essentiels à la réussite. Cependant, les entreprises s'efforcent de concrétiser leurs hautes ambitions dans de nouveaux domaines tels que l'IA et de se protéger contre les cybermenaces croissantes, tout en gérant des ressources humaines (RH), des délais et des budgets limités. Le coût et la rétention des RH restent deux préoccupations majeures qui sont contraires aux attentes souvent élevées à l'égard des équipes TI.

Les statistiques, les analyses et les observations sur le terrain détaillées qui suivent vous aideront à mieux comprendre le paysage actuel des TI au Canada et à prendre vos propres décisions en matière de TI dans des périodes agitées.

01

IMPACT ET INFLUENCE DES TI

L'autonomie stratégique commence par une refonte des TI

Dans un monde de plus en plus marqué par l'incertitude, l'infrastructure numérique n'est plus une préoccupation d'arrière-plan : elle est un impératif de première ligne. Les entreprises repensent la manière de bâtir et de gérer leurs fondations numériques, non seulement pour améliorer leur efficacité, mais aussi pour garder le contrôle.

L'autonomie stratégique est devenue une réponse nécessaire à cette nouvelle réalité. Il faut s'adapter rapidement et protéger les actifs essentiels sans s'enfermer dans des systèmes rigides ou des relations de dépendance opaques.

L'infonuagique met ce défi bien en évidence. Le besoin urgent de modèles transparents, interopérables et flexibles n'a jamais été aussi évident. Qu'il s'agisse d'adopter des stratégies infonuagiques, d'affirmer la souveraineté des données ou de gérer les coûts de façon plus prévisible, les entreprises cherchent à mieux maîtriser leur environnement numérique.

Il est essentiel d'anticiper ces pressions. La sécurité, le contrôle des coûts et la modernisation des TI, qui constituent les principales préoccupations soulevées dans l'édition de cette année du Portrait TI, sont de plus en plus considérés comme interdépendants. Les entreprises dont l'infrastructure est encore qualifiée de « fonctionnelle » passent à des modèles plus évolutifs et sûrs. Lorsque les TI sont considérées comme un partenaire stratégique et qu'elles sont utilisées dès le début du processus décisionnel, les investissements dans l'infonuagique sont plus susceptibles de correspondre aux objectifs à long terme et d'apporter une valeur durable.

On constate actuellement une compréhension élargie du fait que la résilience à long terme dépend de l'autonomie stratégique. La diversification et l'ouverture ne sont plus de grands idéaux, mais des réponses pragmatiques à la complexité opérationnelle d'aujourd'hui.

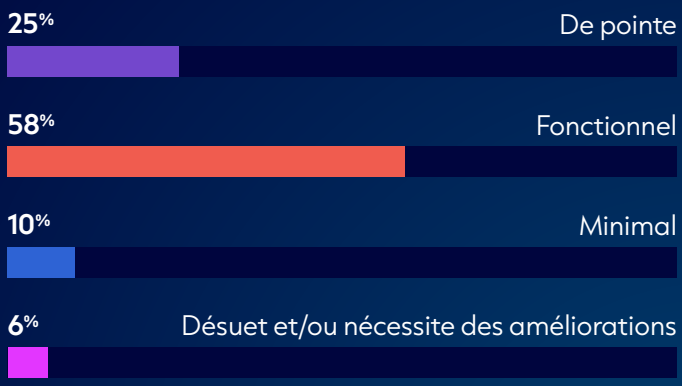
L'autonomie ne nécessite pas de réinvention, mais elle exige le courage de s'affranchir des dépendances technologiques, afin de préserver la liberté d'innover et de gérer les risques à long terme. Dans un récent sondage à l'échelle nationale, 64 % des répondants canadiens ont déclaré se sentir limités par les services de géants américains de l'infonuagique, citant le manque de flexibilité pour changer de fournisseur. Ce taux n'a probablement fait qu'augmenter depuis la publication du sondage. Le Canada doit profiter de ce moment charnière pour se tracer une nouvelle voie, qui concilie l'innovation et l'indépendance et qui établit une résilience durable grâce à des choix en TI effectués dans l'intérêt du pays.

ESTELLE AZEMARD
Vice-présidente Amériques
chez OVHcloud depuis 2020

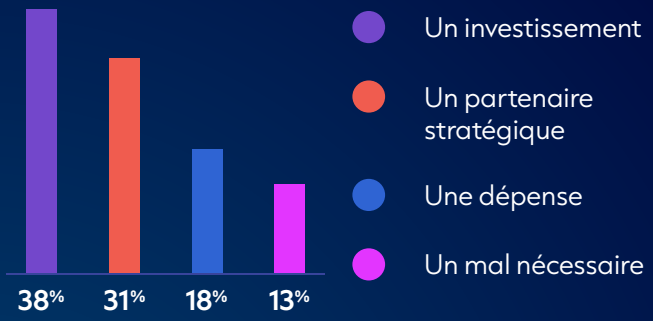
Estelle Azemard supervise les opérations au Canada et en Amérique latine. Titulaire d'un diplôme en droit et d'un MBA de l'HEC Montréal, elle est également conseillère du commerce extérieur de la France et membre du conseil d'administration de French Tech Toronto, où elle milite en faveur de la diversité et de l'égalité des chances dans l'industrie technologique.

TABLEAU DE BORD

25 % des entreprises canadiennes qualifient l'état de leur infrastructure technologique comme étant de pointe.

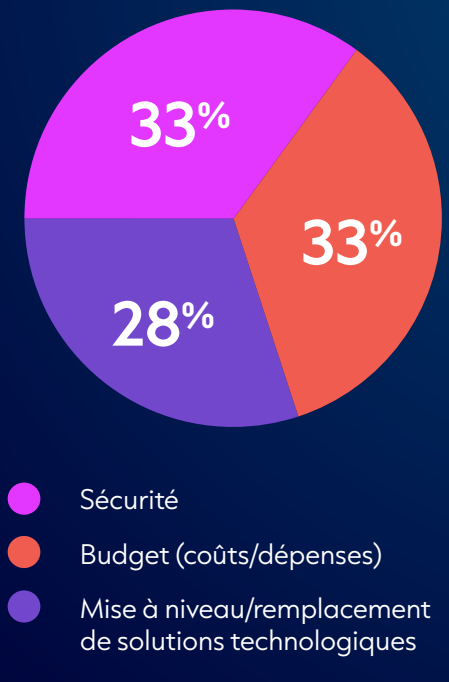


38 % des répondants interrogés perçoivent les TI comme « un investissement ».

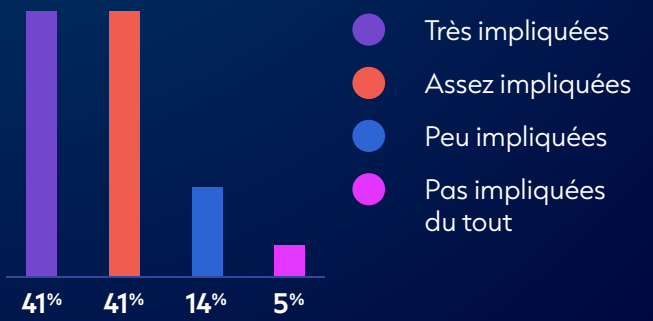


LES TROIS PRINCIPAUX

enjeux des entreprises canadiennes pour la prochaine année :



Jusqu'à quel point les **TI sont-elles impliquées** dans la définition des stratégies de votre entreprise ?



IMPACT ET INFLUENCE DES TI

INTERPRÉTATION DES DONNÉES

Imaginez une salle de conseil où un débat important fait rage autour de la prochaine percée technologique : les dirigeants non issus des TI demandent sans relâche pour des mises à niveau, tandis que les experts en TI chevronnés s'inquiètent que la sécurité est en déclin rapide. Le Portrait TI 2025 mené auprès d'entreprises canadiennes révèle ce fossé critique, mettant en lumière une tension bien réelle qui pourrait miner l'avantage concurrentiel de votre organisation.

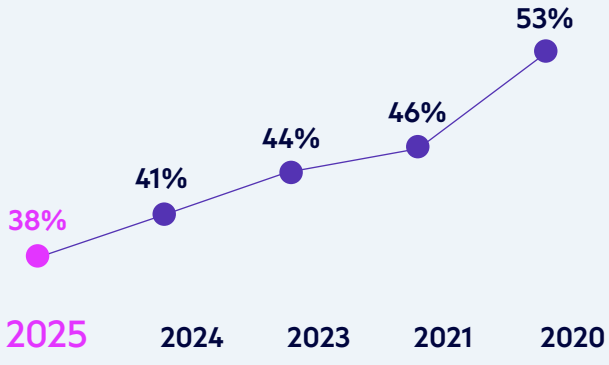
La sécurité au centre des préoccupations

Le rapport Portrait TI de 2025 révèle que **la sécurité a rejoint les contraintes budgétaires en tant que principaux défis pour les entreprises en 2025.**

Toutefois, un profond fossé s'est creusé entre les décideurs TI et les décideurs non TI. Alors que 34 % des dirigeants d'autres services considèrent la mise à niveau ou le remplacement de solutions technologiques comme leur principale préoccupation, 1 décideur TI sur 3 (33 %) considère la sécurité comme le défi technologique le plus pressant pour la prochaine année.

Cette division souligne **la grande divergence dans la façon dont les dirigeants TI et les dirigeants d'autres services perçoivent les défis technologiques.** Cette différence de point de vue est également évidente dans le fait que 33 % des dirigeants TI perçoivent leur infrastructure comme étant à l'« avant-garde », comparativement à seulement 13 % des dirigeants d'autres services. Ces chiffres reflètent bien plus que des opinions : ce sont des indicateurs d'un **défi concret** dans l'alignement des priorités stratégiques au sein d'une organisation.

PERCEPTION DES TI COMME UN INVESTISSEMENT :



« Certaines personnes peuvent constater les progrès technologiques et songer qu'elles n'ont pas atteint ce niveau. Elles peuvent poser des questions sur la « transformation numérique » sans vraiment comprendre de quoi il s'agit. Elles finissent donc par penser qu'elles sont en retard alors que ce n'est pas le cas.

Edward Iskander
Directeur des TI,
Red Apple Stores

La « transformation numérique » : un peu de clarté dans les mots à la mode

Le Portrait TI de cette année révèle que même si le nombre d'entreprises canadiennes qui perçoivent les TI comme un investissement continue de diminuer, le nombre d'entreprises qui les perçoivent comme un partenaire stratégique a augmenté pour atteindre 31 %, comparativement à 28 % en 2024. Cependant, les petites entreprises sont particulièrement susceptibles d'avoir une opinion négative des TI. En effet, 18 % d'entre elles considèrent leurs TI comme un « mal nécessaire », par rapport à 9 % pour les grandes entreprises.

Pour de nombreux cadres d'autres services, la « transformation numérique » est devenue une expression passe-partout, ou un impératif d'adopter chaque nouvelle technologie, que ses avantages soient clairement définis ou non. En revanche, les experts TI adoptent une approche plus mesurée. Dotés d'une expertise technique, les dirigeants TI comprennent que la transformation nécessite du temps et une planification stratégique. Cette disparité génère des tensions : les dirigeants non TI peuvent se sentir obligés d'agir rapidement pour suivre les tendances du marché, tandis que les équipes TI les préviennent que l'adoption précipitée de nouvelles solutions peut accroître les vulnérabilités, surtout dans des domaines comme l'IA, et que celles-ci peuvent avoir de graves conséquences pour la cybersécurité et la confidentialité des données.

CONSEILS POUR LES PETITES ENTREPRISES

Votre service TI constitue une ressource stratégique qui nécessite un investissement actif. Il est là pour protéger votre entreprise contre les cyberattaques et pour l'aider à être plus résiliente et plus concurrentielle.

« Les petites entreprises pourraient être plus agiles lorsqu'elles prennent des décisions fondées sur des données, mais elles ne disposent probablement pas de l'expertise interne et des ressources financières nécessaires pour en tirer parti de manière efficace. Il s'agit donc d'une excellente occasion pour elles de faire le premier pas.

Luvenn Alphonso
Directeur général,
Blair Technology Solutions

Implantation de l'IA : une nouvelle frontière

Pour complexifier davantage les enjeux en matière de TI, l'implantation de l'IA est apparue comme une nouvelle frontière, se classant au quatrième rang (22 %) des principaux enjeux à venir pour les entreprises canadiennes. Ce résultat suggère que de nombreuses entreprises se sentent pressées d'adopter des outils d'IA, même si elles n'ont pas encore pleinement compris les risques et les avantages que présentent ces technologies.

UN ÉCART GRANDISSANT

Alors que les décideurs non TI peuvent s'empresser de mettre en œuvre de nouvelles solutions d'IA sans disposer d'une feuille de route claire, les experts TI demeurent prudents et soulignent la nécessité de sécuriser et de gérer efficacement les données.

« Les entreprises doivent d'abord analyser leurs besoins en matière d'IA et savoir où sont stockées leurs données afin de bien comprendre quel service a le plus haut niveau de maturité et le plus grand besoin d'intégrer une solution d'IA. Cela garantira ensuite un meilleur retour sur investissement.

Martin Pelletier
Chef des initiatives stratégiques,
Groupe NOVIPRO

RISQUES ET OPPORTUNITÉS

Risques

Déconnexion croissante entre les dirigeants TI et les dirigeants non TI

Une communication inefficace entre les équipes TI et les autres services peut constituer un obstacle important, empêchant l'alignement des objectifs et des priorités, et entraînant des retards, des dépassements budgétaires et une gestion sous-optimale des ressources.

Succomber aux tendances du secteur

Les dirigeants non TI peuvent suivre les grandes tendances du secteur et se laisser facilement influencer par des exemples de réussite qui ne s'appliquent pas à leur secteur et à leur entreprise, investissant ainsi dans la technologie sans avoir de plan de match et d'objectif clair pour réussir leur intégration.

Sous-investir dans les TI

Un investissement insuffisant dans les TI se traduira par un positionnement concurrentiel statique. Des investissements plus importants dans les TI peuvent permettre d'étudier plus en profondeur la manière dont la technologie peut contribuer à la compétitivité.

Opportunités

Modifier la perception des TI

L'implication de votre service TI dès le début du processus stratégique permettra à votre entreprise de mieux comprendre comment la technologie peut produire de meilleurs résultats pour vos objectifs commerciaux, tout en normalisant et en améliorant la perception du service TI dans tous les autres d'activité.

Élaborer une feuille de route claire pour l'adoption de l'IA

Collaborez avec votre équipe TI et tous les services de votre organisation pour créer une stratégie claire et complète en matière d'IA, avec des indicateurs de performance clés mesurables et adaptés à votre entreprise et à votre secteur d'activité. Cette stratégie permettra à votre entreprise de maximiser les avantages de l'IA tout en gérant les risques qui y sont associés.

Obtenir un avantage concurrentiel grâce à l'intégration des TI

Une plus grande intégration des TI dans le processus décisionnel et stratégique se traduira par une incidence majeure sur votre entreprise, renforçant l'importance et l'influence des TI sur la compétitivité et le succès de votre organisation.

LA GRANDE QUESTION

Comment votre organisation peut-elle combler le fossé entre la direction TI et celle non TI pour s'assurer que les investissements technologiques favorisent à la fois l'innovation et une sécurité renforcée, tout en produisant des résultats clairs et mesurables dans le paysage numérique actuel en rapide évolution ?

02

ENVIRONNEMENT ÉCONOMIQUE

L'espoir n'est pas une stratégie : préparer les entreprises canadiennes pour l'avenir en 2025

Le Canada traverse un moment charnière de son histoire en 2025. Chaque semaine, en discutant avec des professionnels TI, des cadres et des dirigeants liés au secteur technologique partout au pays, une chose devient évidente : l'année 2025 s'annonce décisive pour les entreprises canadiennes. Nous évoluons dans un environnement numérique plus complexe, plus compétitif et plus impitoyable que jamais. Les décisions actuelles des dirigeants, notamment en matière d'investissement, d'adaptation et de protection, détermineront la réussite ou l'échec de leur entreprise dans les années à venir.

Les occasions sont bien réelles. Les entreprises canadiennes misent sérieusement sur des outils qui promettent de stimuler la productivité, de réduire les coûts et de moderniser les méthodes de travail. L'IA et l'automatisation sont au cœur de cette évolution. Et d'après ce que je constate, on ne parle plus de projets pilotes, mais d'investissements transformationnels qui propulsent des secteurs entiers vers l'avenir.

La course est lancée pour bâtir des entreprises plus intelligentes, plus efficaces et plus rapides. Mais toute transformation s'accompagne de défis. Par exemple, de nombreuses organisations peinent à améliorer les compétences de leurs employés. Par conséquent, on met de plus en plus l'accent sur la formation, pour permettre aux équipes d'adopter les technologies émergentes qui évoluent souvent plus vite que leur capacité à s'y adapter. La formation et la requalification ne sont plus un luxe, elles sont au centre de toute stratégie d'investissement.

Bienentendu,ilestimpossibledeparlerd'investissements informatiques sans aborder la question de la sécurité. En ce qui concerne les investissements technologiques prévus, les solutions de sécurité demeurent la priorité. Je travaille avec plusieurs entreprises de sécurité qui insistent toutes sur l'importance d'adopter de nouveaux moyens de protéger les entreprises, comme la cyberassurance. Après tout, nous savons que les cybermenaces sont en hausse et que l'IA contribue à les rendre encore plus sophistiquées. Comme me l'a récemment confié un expert en cybersécurité, les auteurs de ces attaques ne sont plus de simples individus en coton ouaté installés dans un garage, mais bien des groupes organisés et sophistiqués qui ciblent des entreprises vulnérables.

Malgré l'augmentation des risques, de nombreuses entreprises canadiennes n'investissent pas encore suffisamment dans l'atténuation des risques et la préparation en matière de sécurité. La cyberassurance devient un outil incontournable, mais son adoption reste inégale. Trop d'entreprises restent exposées et espèrent simplement ne pas faire les manchettes. Or, l'espoir n'est pas une stratégie. Si vous modernisez votre entreprise sans la renforcer, vous n'êtes pas du tout préparé pour l'avenir.

Autrement dit, en cette période charnière, il est indispensable d'investir dans la modernisation de votre infrastructure TI pour aller de l'avant et rester en sécurité. Les entreprises qui adoptent une attitude attentiste se verront dépasser par des concurrents plus agiles. Celles qui sortiront gagnantes en 2025 et au-delà seront celles qui auront su investir avec audace et sagesse, en agissant rapidement, en formant judicieusement leurs équipes et en intégrant la résilience à chaque couche de leur infrastructure technologique.

AMBER MAC
Présidente d'AmberMac Media, auteure à succès, podcasteuse primée et conférencière de premier plan dans le domaine des technologies

Nommée Femme de l'année 2024 par le DMZ, elle anime The AmberMac Show sur SiriusXM et apparaît régulièrement sur CNN, Bloomberg et Fast Company en tant qu'experte de confiance en technologies et innovation.

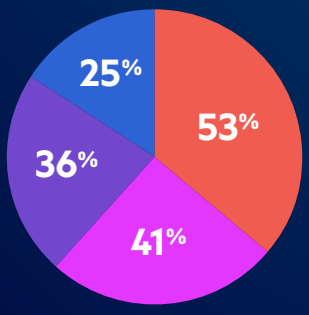
TABLEAU DE BORD

Plus de 50 % des entreprises canadiennes prévoient d'utiliser un service infonuagique et de s'appuyer sur leur équipe interne.

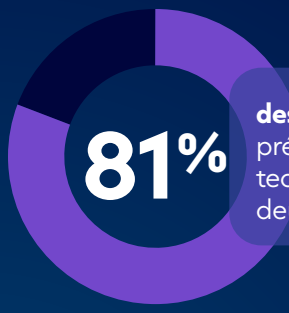
Au cours des deux prochaines années, pensez-vous être :	
Propriétaire des équipements	45 %
Utilisateur d'un service infonuagique	55 %
Dépendant d'une équipe interne pour la gestion de l'infrastructure	65 %
Dépendant d'une équipe externe pour la gestion de l'infrastructure	35 %

PLUS DE LA MOITIÉ DES ENTREPRISES QUI PRÉVOIENT D'INVESTIR DANS L'IA ET/OU L'AUTOMATISATION DES PROCESSUS LE FONT POUR STIMULER LA PRODUCTIVITÉ.

Les principaux objectifs des entreprises qui prévoient d'investir dans l'IA et/ou l'automatisation des processus au cours des deux prochaines années sont :



- Être plus productif
- Réduire les coûts
- Diminuer l'erreur humaine
- Pallier la pénurie de main-d'œuvre



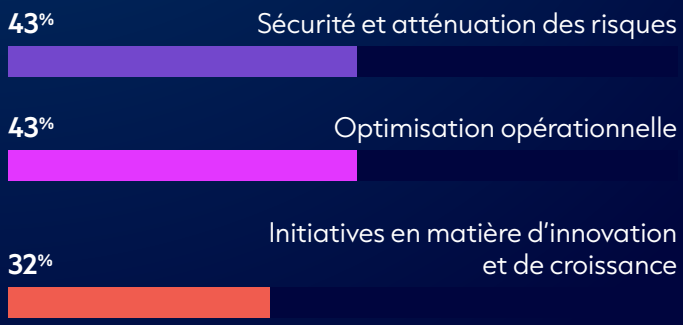
des entreprises canadiennes prévoient un investissement technologique majeur d'ici deux ans.

LES CINQ SECTEURS

clés pour les investissements technologiques d'ici deux ans :

Intelligence artificielle	30 %
Solutions infonuagiques	29 %
Solutions et/ou services de sécurité (par exemple, gouvernance, logiciels, formation et audits)	23 %
Solutions d'infrastructure (par exemple, matérielles et logicielles)	21 %
Solutions de modernisation d'applications (par exemple, automatisation, conteneurisation et orchestration)	19 %

LES TROIS grands objectifs des investissements technologiques :



ENVIRONNEMENT ÉCONOMIQUE

INTERPRÉTATION DES DONNÉES

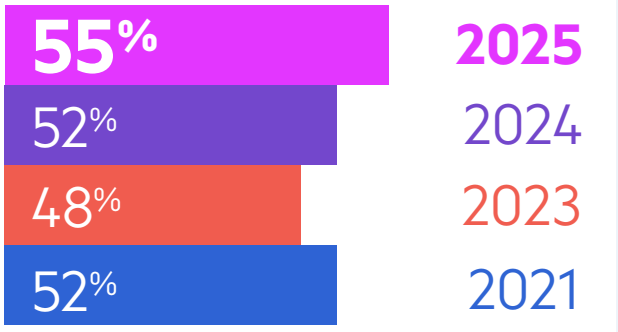
Dans le paysage technologique en constante évolution d'aujourd'hui, les entreprises repensent la manière dont elles investissent dans la technologie pour stimuler leur croissance et renforcer leur compétitivité. Les données de cette année dressent un tableau des priorités changeantes à travers le Canada, où des mesures audacieuses en faveur de l'IA transforment les stratégies d'entreprise, même si les préoccupations traditionnelles en matière de sécurité et de gestion des risques persistent.

Le Portrait TI de cette année révèle que 55 % des entreprises prévoient, au cours des deux prochaines années, de passer de solutions sur site à l'utilisation de logiciels infonuagiques, en s'appuyant sur des équipes internes pour la gestion de l'infrastructure. C'est une tendance en constante augmentation. Par exemple, de grands détaillants, comme de grandes chaînes de supermarchés ont migré leurs activités principales vers l'infonuagique pour rationaliser leurs chaînes d'approvisionnement. Ce changement réel souligne le rôle essentiel de l'infonuagique dans la gestion de vastes flux de données et dans le soutien à la prise de décision rapide.

DES PISTES DE RÉFLEXION

L'infonuagique n'est plus une option; il est maintenant temps d'évaluer sérieusement les risques de sécurité qui peuvent être associés aux solutions sur site ou hybrides.

AU COURS DES DEUX PROCHAINES ANNÉES, PENSEZ-VOUS QUE VOUS SEREZ UTILISATEUR D'UN SERVICE INFONUAGIQUE ?



« Nous sommes entièrement convaincus par les solutions infonuagiques et nous réapprenons continuellement à trouver la solution idéale pour optimiser nos activités.

Simon Bonanno
Directeur principal des TI,
BNC

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.

	2025	2024	2023	2021	2020	2019	2018	2017
Solutions de sécurité (ex : gouvernance, logiciels, formations, audits, etc.)	23%	29%	17%	25%	25%	42%	40%	N/A
Solutions infonuagiques	29%	28%	14%	34%	38%	N/A	N/A	N/A
Intelligence artificielle (ex : Apprentissage automatique, apprentissage profond, etc.)	30%	25%	13%	18%	N/A	N/A	N/A	N/A
Solutions d'affaires (ex : ERP 10%, CRM 17%, etc.)	27%	23%	16%	17%	25%	37%	36%	43%
Solutions d'infrastructures (ex : matérielles et logicielles)	21%	22%	19%	21%	28%	40%	43%	52%
Services professionnels (ex : consultation, implantation, etc.)	14%	19%	14%	15%	21%	34%	24%	39%
Analyse de données avancées (ex : Apprentissage automatique, apprentissage profond, etc..)	15%	17%	13%	18%	29%	36%	34%	23%
Solutions de modernisation d'applications (ex. : automatisation, conteneurisation, orchestration, etc.)	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.)	11%	15%	9%	N/A	N/A	N/A	N/A	N/A
Internet des objets (IoT)	11%	14%	7%	14%	20%	N/A	N/A	N/A
Technologie 5G	10%	14%	7%	12%	N/A	N/A	N/A	N/A
Commerce en ligne	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	12%	13%	14%	12%	8%	2%	6%	7%
Technologies propres (qui aident à réduire les impacts environnementaux)	7%	11%	7%	N/A	N/A	N/A	N/A	N/A
Technologie chaîne de blocs	6%	10%	4%	8%	11%	23%	22%	N/A
Réalité étendue (ex : Metavers, réalité augmentée, réalité virtuelle, etc.)	7%	7%	3%	N/A	N/A	N/A	N/A	N/A
Solutions de reconnaissance vocale et faciale	4%	6%	5%	5%	10%	N/A	N/A	N/A

L'IA sur le devant de la scène

Le marché mondial de l'IA poursuit son expansion fulgurante, avec des investissements dépassant 120 milliards de dollars en 2023 et des investissements projetés atteignant 900 milliards de dollars d'ici 2027. Plus de 75 % des entreprises figurant dans le classement « Fortune 500 » intègrent désormais activement l'IA dans leurs activités, tandis que l'adoption de grands modèles de langage (GML) a bondi de 300 % depuis 2022.

Le Canada n'échappe pas au boom de l'IA. Il n'est donc pas surprenant de constater que, pour la première fois, l'IA (30 %) a surpassé la sécurité (23 %) en tant que principal domaine où des investissements en TI sont prévus dans les deux prochaines années. Dans des secteurs tels que les technologies, les médias et les télécommunications, une proportion impressionnante de 92 % des entreprises prévoient d'investir dans l'IA, suivi de près par 88 % des entreprises spécialisées dans les TI qui suivent le mouvement. Plus de la moitié (53 %) de ces investissements sont motivés par un objectif clair : **stimuler la productivité (53 %)** et **réduire les coûts (41 %)**.

En 2023, plus de

120 milliards

de dollars ont été investis en IA

La projection pour 2027 à été estimé pour un total de

900 milliards

Automatisation : la productivité en tête des priorités d'investissement

	2025	2024	2023
Être plus productif	53 %	56 %	51 %
Réduire les coûts	41 %	48 %	41 %
Diminuer l'erreur humaine	36 %	36 %	38 %
Pallier la pénurie de main-d'œuvre	25 %	25 %	25 %

Les grandes entreprises, en particulier celles qui comptent plus de 100 employés (88 %) et les entreprises de l'Ontario (86 %), sont plus susceptibles d'avoir défini des objectifs clairs en matière d'IA. En revanche, les entreprises des secteurs de l'éducation, des services sociaux et des services personnels, ainsi que celles qui ont moins confiance dans leurs capacités informatiques, sont plus prudentes (respectivement 36 %, 29 % et 32 %) et n'ont pas l'intention d'investir dans l'automatisation dans l'immédiat.

Les principaux secteurs prévus pour les investissements technologiques

	2025	2024
Intelligence artificielle	30 %	25 %
Infonuagique	29 %	28 %
Sécurité	23 %	29 %

> L'IA est un outil et non une fin en soi. Il y a un besoin de formation, d'une définition commune de l'IA et d'une compréhension de la façon de l'utiliser pour mieux interpréter les données.
>
> **Isabelle Béguin**
> VP des TI,
> InTgral

Trouver l'équilibre : sécurité, risques et optimisation opérationnelle

Si l'IA est le premier domaine (30 %) dans lequel les entreprises prévoient d'investir au cours des deux prochaines années, l'objectif le plus recherché de leurs investissements planifiés (43 %) est la sécurité et l'atténuation des risques, ainsi que l'optimisation opérationnelle. **Bien que l'accent mis sur la sécurité ait diminué de 6 % par rapport à l'année dernière**, les entreprises restent méfiantes quant aux risques posés par les outils d'IA de tiers et les vulnérabilités des données. Ces deux objectifs reflètent la nécessité de moderniser les actifs essentiels tout en les protégeant, une question d'équilibre qui est au cœur de la stratégie d'investissement TI actuelle.

Les entreprises qui arrivent à atteindre cet équilibre pourront non seulement se positionner en tête du marché d'aujourd'hui, mais elles consolideront également leur avantage concurrentiel dans le futur.

RISQUES ET OPPORTUNITÉS

Risques

Mauvais alignement des stratégies d'investissement dans l'IA

Si une entreprise ne dispose pas des ressources financières nécessaires pour suivre l'évolution rapide de l'IA, elle risque de prendre un retard considérable par rapport à ses concurrents.

Absence de mesures solides de protection des données

Sans politiques de sécurité et de protection des données appropriées en place, l'adoption rapide de solutions d'IA, en particulier par le biais d'outils de tiers, peut exposer les entreprises à des risques importants quant à la confidentialité des données et la cybersécurité.

Compréhension insuffisante de la technologie

Les dirigeants non TI, qui peuvent ne pas avoir une compréhension approfondie de l'infonuagique, de l'IA et des technologies de modernisation, peuvent risquer de mettre en œuvre des changements selon des priorités différentes de celles des dirigeants TI et entraîner un retard de compétitivité.

Opportunités

Souveraineté des données

Dans un contexte de tensions et d'incertitudes commerciales entre les États-Unis et le Canada, les entreprises canadiennes ont une occasion unique de transformer les contraintes réglementaires en avantage stratégique. En évaluant et en choisissant correctement la stratégie infonuagique hybride appropriée - comme des solutions logicielles et infonuagiques hébergées localement - les entreprises peuvent veiller à la conformité en matière de souveraineté des données, protéger les informations sensibles, renforcer la confiance des clients et améliorer la résilience de l'organisation dans un paysage géopolitique changeant.

Augmentation de la productivité grâce à l'IA

Les investissements dans l'IA, associés à une compréhension précise des besoins et des cas d'utilisation, peuvent transformer les données brutes en informations exploitables, améliorant ainsi la productivité et la veille concurrentielle.

Alignement stratégique

Lorsque la direction TI et la haute direction travaillent en harmonie, les entreprises peuvent améliorer leur efficacité, réduire leurs coûts et assurer leur pérennité, et ce, grâce à l'intégration de technologies de pointe à des processus décisionnels plus intelligents et plus conscients des risques.

LA GRANDE QUESTION

Comment votre organisation parviendra-t-elle à trouver un équilibre entre la recherche d'innovations révolutionnaires comme l'IA et le besoin critique de sécuriser et d'optimiser vos actifs actuels, afin d'assurer une compétitivité à long terme dans un paysage numérique en rapide évolution ?

03

SOLUTIONS TECHNOLOGIQUES

De nombreuses organisations à travers le Canada mettent l'accent sur l'IA, l'analytique et l'infonuagique

Bien que l'expérimentation demeure très importante, de nombreuses entreprises mettent délibérément en œuvre de telles solutions pour atténuer les défis internes et externes. De par mon expérience dans différents secteurs, je constate l'émergence de **trois grandes tendances cette année.**

Premièrement, **l'utilisation accrue de l'IA pour automatiser les processus, améliorer la création et le partage de connaissances et renforcer l'engagement des clients.** L'objectif principal est l'amélioration de la productivité. Cela peut être accompli en automatisant les tâches répétitives, en réduisant les erreurs liées aux processus manuels, ou en mettant en évidence des informations clés pour favoriser des décisions éclairées par les données.

Deuxièmement, **la prise de décisions fondées sur les données devient la norme.** La plupart des organisations ont atteint un stade où l'analyse descriptive ainsi que les techniques et les outils traditionnels d'intelligence d'affaires (BI) font désormais partie des habitudes. Malheureusement, peu d'entreprises disposent des compétences internes ou des budgets nécessaires pour investir adéquatement dans l'analyse de données avancée et en tirer parti. J'espère que le marché des fournisseurs continuera de se développer afin d'offrir des solutions plus abordables et plus compétitives pour l'analyse prédictive, prescriptive et descriptive.

Troisièmement, le taux d'**adoption de l'infonuagique continue d'augmenter.** Les solutions infonuagiques offrent l'évolutivité et une infrastructure moderne mieux adaptée aux données complexes et aux besoins opérationnels d'aujourd'hui. D'autre part, les organisations doivent parfois renoncer à leur expertise interne au profit de services intégrés plus coûteux qui nécessitent une formation supplémentaire et l'acquisition de nouvelles compétences. C'est peut-être pour cette raison que nous constatons un intérêt soutenu envers les solutions à code source ouvert (open-source). Ces solutions sont souvent plus abordables et donnent aux entreprises la flexibilité nécessaire pour personnaliser leur infrastructure tout en évitant les coûts à long terme et les inefficacités associés à une technologie désuète ou restrictive.

Dans l'ensemble, les données de ce rapport correspondent à ce que j'entends dans mes entretiens de tous les jours : les organisations recherchent des solutions pratiques, évolutives, abordables et adaptées à leurs besoins uniques et complexes. **Lorsqu'elles sont mises en œuvre de manière réfléchie et en parfaite adéquation avec les objectifs organisationnels, les solutions technologiques peuvent offrir une valeur réelle et durable.**

George Firican
Fondateur de LightsOnData et fait partie du programme Top Voices de LinkedIn

George Firican est reconnu mondialement pour son travail en matière de gouvernance des données, de qualité des données et de veille stratégique. Grâce à son contenu, à ses programmes et à son balado, il aide les organisations à transformer les données en un véritable atout et à rendre les sujets complexes accessibles et exploitables.

TABLEAU DE BORD

PERCEPTION

LES TROIS principales sources de retour sur investissement prévues pour les solutions infonuagiques :

- **37%** Amélioration de l'efficacité opérationnelle et des processus d'entreprise
- **36%** Réduction des coûts liés à l'infrastructure matérielle
- **34%** Amélioration de la flexibilité et de l'agilité de l'entreprise

INVESTISSEMENT

LES TROIS grandes priorités d'investissement dans l'infonuagique :

- **63%** Sauvegarde des données
- **57%** Service de cybersécurité
- **41%** Mégadonnées

85%

des entreprises canadiennes utilisent une solution infonuagique.

ÉTAT ACTUEL

LES CINQ PRINCIPALES motivations des entreprises à adopter l'infonuagique :

- **36%** Réduction des coûts et optimisation
- **34%** Modernisation de l'infrastructure informatique
- **32%** Évolutivité et flexibilité
- **30%** Efficacité et automatisation
- **26%** Accessibilité à distance pour les travailleurs

ÉTAT ACTUEL

LES CINQ PRINCIPAUX usages de l'infonuagique en entreprise :

- **34%** Sauvegarde des données
- **32%** Site internet
- **31%** Courriel et collaboration
- **24%** Service de cybersécurité
- **23%** Intelligence artificielle

TABLEAU DE BORD

PERCEPTION

TOP 5

LES CINQ PRINCIPALES raisons **D 'ADOPTER L'INTELLIGENCE ARTIFICIELLE :**

- **20%** Augmenter la productivité
- **16%** Automatiser les tâches manuelles
- **12%** Réduire les coûts de fonctionnement
- **10%** Améliorer les processus internes
- **9%** Renforcer l'avantage concurrentiel

LES CINQ OBSTACLES majeurs à **L'INVESTISSEMENT** en **INTELLIGENCE ARTIFICIELLE** :

- **25%** Coûts
- **20%** J'ai déjà investi dans l'IA par le passé
- **17%** Préoccupations concernant la confidentialité et la sécurité des données
- **16%** Manque d'expertise à l'interne pour l'exécution
- **15%** Retour sur investissement

LES CINQ PRINCIPALES raisons **D'ADOPTER L'ANALYSE DE DONNÉES AVANCÉE** :

- **11%** Augmenter la productivité
- **9%** Renforcer la cybersécurité
- **9%** Réduire les coûts de fonctionnement
- **9%** Améliorer les processus internes
- **9%** Déchiffrer les tendances du marché

LES CINQ OBSTACLES majeurs à **L'INVESTISSEMENT** en **ANALYSE DE DONNÉES AVANCÉE :**

- **26%** Coûts
- **15%** Manque d'expertise à l'interne pour l'exécution
- **14%** Retour sur investissement
- **12%** Préoccupations concernant la confidentialité et la sécurité des données
- **12%** J'ai déjà investi dans l'analyse de données avancée par le passé

TABLEAU DE BORD

PERCEPTION

Le moment où **l'analyse de données avancée** deviendra un atout majeur pour **l'entreprise et son industrie.**

Le moment où l'**IA** deviendra un atout majeur pour **l'entreprise et son industrie.**

ENTREPRISE	INDUSTRIE		ENTREPRISE	INDUSTRIE
27%	32%	C'est déjà commencé	31%	34%
14%	12%	Oui, dans moins d'un an	17%	11%
17%	13%	Oui, d'ici 1 à 2 ans	15%	14%
10%	11%	Oui, d'ici 3 à 5 ans	10%	12%
3%	5%	Oui, d'ici 6 à 10 ans	3%	7%
14%	14%	Cela ne devrait pas l'affecter	13%	12%
15%	14%	Je ne sais pas	11%	10%

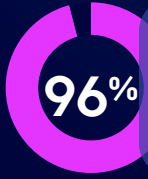
INVESTISSEMENT

LES CINQ principaux types **d'analyse de données avancée** que les entreprises envisagent de mettre en place :

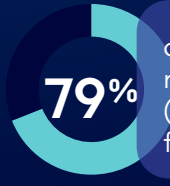
- **54%** Analyses statistiques avancées (par exemple, statistiques inférentielles, statistiques prédictives etc.)
- **42%** Analyses statistiques de base (par exemple, analyses descriptives et exploratoires)
- **41%** Visualisation de données (par exemple, graphiques et tableaux de bord)
- **33%** Analyse de type apprentissage machine (par exemple, segmentation et classification)
- **28%** Analyse de type apprentissage profond (par exemple, reconnaissance d'images et traitement du langage naturel [NLP])

LES CINQ principaux types de **solutions à code source ouvert** que les entreprises envisagent de mettre en place :

- **21%** Plateforme infonuagique (par exemple, OpenStack et CloudStack)
- **18%** Bases de données (par exemple, PostgreSQL, MySQL et MongoDB)
- **18%** Outils de sécurité (par exemple Graylog, Pfsense, Suricata et Kali)
- **17%** Plateforme de virtualisation (par exemple, KVM et VirtualBox)
- **17%** Développement de logiciels et outils DevOps (par exemple, Jenkins, Puppet et Chef)



des entreprises canadiennes prévoient de mettre en place au moins un type d'analyse de données avancée afin de soutenir leurs objectifs stratégiques.



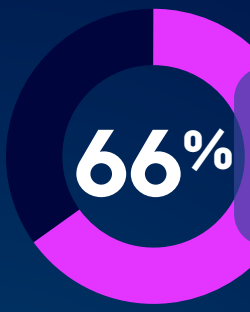
des entreprises prévoient d'adopter au moins une solution à code source ouvert (open-source) en production ou dans de futurs projets.

TABLEAU DE BORD

ÉTAT ACTUEL

Outils d'analyse de données avancée les plus utilisés par les entreprises :

Outils d'intelligence d'affaires (BI), de visualisation de données et de tableaux de bord	**44%**
Environnement et langages de développement à **code source ouvert (open-source)**	**29%**
Environnement de développement propriétaire, pouvant ou non utiliser des **codes sources ouverts**	**15%**
Je n'utilise pas d'outils d'analyse de données avancée	**27%**



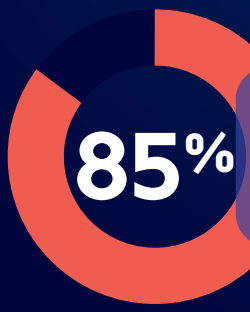
des entreprises utilisent actuellement au moins un type d'outil d'analyse de données avancée.

LES CINQ principaux usages des données dans la prise de décision :

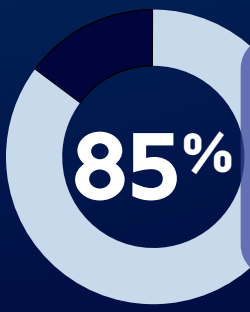
- **35%** Analyse des performances financières et budgétaires
- **34%** Gestion de la relation client et expérience client
- **32%** Optimisation des processus opérationnels
- **27%** Prévision des ventes et analyse du marché
- **26%** Prise de décision en matière de marketing et de publicité

LES CINQ solutions à code source ouvert (open-source) les plus utilisées en entreprise :

- **29%** Bases de données (par exemple, PostgreSQL, MySQL et MongoDB)
- **22%** Développement de logiciels et outils DevOps par exemple, Jenkins, Puppet et Chef)
- **21%** Plateforme infonuagique (par exemple, OpenStack et CloudStack)
- **18%** Plateforme de virtualisation (par exemple, KVM et VirtualBox)
- **17%** Outils de sécurité (par exemple Graylog, Pfsense, Suricata et Kali)



des entreprises canadiennes utilisent des données pour prendre des décisions commerciales.



des entreprises utilisent déjà au moins une solution à code source ouvert (open-source) dans leur environnement de production ou dans des projets à venir.

SOLUTIONS TECHNOLOGIQUES

INTERPRÉTATION DES DONNÉES

Exploiter l'avantage numérique

Les entreprises canadiennes sont à l'avant-garde de l'innovation numérique et investissent stratégiquement dans un éventail de technologies, telles que l'infonuagique, l'IA, l'analyse de données avancée et les solutions à code source ouvert (open-source), pour stimuler la productivité, gérer les coûts et se différencier sur les marchés concurrentiels.

L'infonuagique

Si 44 % des grandes entreprises utilisent l'infonuagique principalement pour moderniser leur infrastructure informatique, les petites entreprises considèrent toujours l'infonuagique comme un moyen de réduire les coûts. En effet, **35 % d'entre elles citent la réduction des coûts comme leur principale raison d'utiliser l'infonuagique.** Par ailleurs, 37 % citent l'amélioration de l'efficacité opérationnelle et des processus d'entreprise comme le principal avantage de l'investissement dans l'infonuagique. Plus du tiers (36 %) des répondants voient également dans l'infonuagique une occasion de réduire leurs coûts liés au matériel, afin de simplifier leurs opérations et de les rendre moins coûteuses et plus agiles.

« La réduction des coûts ne doit pas être l'objectif ultime. D'autres raisons doivent motiver la décision de passer à l'infonuagique. Il est tout aussi important de moderniser les infrastructures et d'allouer les ressources administratives ailleurs.

Martin Chagnon
Directeur des ventes - spécialiste de solutions,
NOVIPRO

Bien que de nombreuses entreprises canadiennes voient dans l'infonuagique une façon de mieux contrôler leurs coûts et d'optimiser leurs opérations, l'ampleur réelle des économies possibles demeure floue pour plusieurs. **Les entreprises qui souhaitent investir dans l'infonuagique ne doivent pas le faire dans une optique d'économie à court terme**, en pensant qu'investir dans l'infonuagique est moins dispendieux que d'acheter de nouveaux serveurs ou d'acquérir un environnement de test pour une utilisation ponctuelle. Si l'on considère le coût total d'acquisition, l'infonuagique n'est pas une option plus abordable qu'une solution sur site. **L'avantage de l'infonuagique réside plutôt dans l'amélioration de l'évolutivité, de la flexibilité et de la modernisation** de votre environnement technologique.

S'il est clair que l'infonuagique continue de remodeler le paysage des TI au Canada, on a encore l'impression que le transfert des données vers l'infonuagique entraîne un transfert des responsabilités en matière de sécurité, ce qui n'est pas le cas. Les entreprises doivent comprendre qu'elles sont toujours responsables de la sécurité de leurs données, où qu'elles se trouvent. Dans ce contexte, la souveraineté des données occupera une place de plus en plus centrale dans les choix d'investissement stratégique.

SOUVERAINETÉ DES DONNÉES ET RELATIONS ENTRE LES ÉTATS-UNIS ET LE CANADA

Envisagez de privilégier des fournisseurs de services infonuagiques canadiens, de varier entre l'infrastructure sur site et l'infrastructure infonuagique, ou d'utiliser plusieurs centres de données infonuagiques situés dans différents endroits.

« Nous constatons que de plus en plus d'entreprises s'inquiètent de savoir qui stocke leurs données et à quelles normes/lois le fournisseur d'hébergement est soumis. Est-il conforme à la loi 25 du Québec ou est-il soumis à la CLOUD Act ? Lorsqu'il est question de protection des données, l'emplacement n'entre malheureusement pas en ligne de compte, car même au Canada, vous êtes assujetti à la CLOUD Act si vous utilisez un fournisseur de services infonuagiques américain. C'est le genre de formation que nous voulons offrir aux entreprises canadiennes.

Rodolphe Rigault
Spécialiste services, solutions et infonuagique, NOVIPRO

> L'IA suscite d'énormes attentes, mais il n'existe pas encore d'application miracle. Les gens intègrent des outils d'IA générative comme ChatGPT, DeepSeek et Copilot. Tous ces outils sont utiles, mais les gens essaient encore de comprendre comment les mettre en œuvre le mieux possible pour leur entreprise. Il y a encore beaucoup de confusion.
>
> **Christopher Reynolds**
> Gestionnaire des comptes partenaires,
> OVHcloud

L'IA à la croisée des chemins : investissement stratégique, innovation dans le monde réel et enjeux élevés de la réussite

L'IA est officiellement passée de la marginalité à la normalité dans la stratégie d'entreprise et ce changement marque plus qu'une tendance passagère. Il signale une transformation plus large de la façon dont les entreprises perçoivent l'innovation, l'efficacité et l'avantage concurrentiel.

Quelles sont les principales raisons qui motivent ces investissements ? Augmenter la productivité (20 %), automatiser les tâches manuelles (16 %) et réduire les coûts opérationnels (12 %). Toutefois, les coûts (20 %) et les préoccupations concernant la confidentialité et la sécurité des données (17 %) restent des obstacles à une plus grande adoption.

Mais dans quels domaines ces entreprises investissent-elles précisément ?

Aujourd'hui, il n'y a pas qu'une seule façon d'adopter l'IA. Les entreprises explorent un large éventail de solutions, allant d'outils génératifs basés sur des tâches à des plateformes hautement spécialisées conçues pour des prises de décision complexes.

Ces technologies évoluent rapidement et ont déjà des répercussions dans plusieurs secteurs :

- Dans le domaine de la **création visuelle et multimédia**, *Midjourney* et *Stable Diffusion* élèvent les standards en génération d'images, tandis que *Sora* et *Runway Gen-2* ouvrent une nouvelle ère pour la conversion de texte en vidéo.
- Dans le domaine de l'**IA spécialisée**, *AlphaFold* révolutionne la recherche biologique en prédisant la structure des protéines, *Perplexity AI* redéfinit la manière dont nous recherchons et citons les informations, et *Character.AI* personnalise les expériences conversationnelles comme jamais auparavant.
- Dans le domaine des **services professionnels**, *Notion AI* et *Jasper* rationalisent la productivité et la création de contenu, Harvey transforme les flux de travail juridiques et *Synthesis* prend en charge l'analyse financière prédictive.
- Au **niveau de l'infrastructure**, des avancées telles que *Llama de Meta*, le moteur d'inférence ultrarapide de *Groq* et le traitement multimodal de *Gemini* repoussent les limites de ce que les modèles fondamentaux peuvent offrir en termes de rendement, d'envergure et de vitesse.

Cependant, malgré cette vague d'innovation, l'utilisation de **l'analyse de données avancée** a diminué depuis l'année dernière. Bien que la majorité des entreprises (85 %) utilisent des données pour prendre des décisions d'affaires, en particulier pour l'analyse des performances financières et budgétaires (35 %) et la gestion de la relation et de l'expérience client (34 %), **seulement 66 % des entreprises utilisent actuellement des outils d'analyse de données avancée**, soit une baisse de 19 % par rapport à 2024. Les deux principaux outils d'analyse de données avancée utilisés par les entreprises sont les outils d'intelligence d'affaires (BI), de visualisation de données et de tableaux de bord (44 %), ainsi que l'environnement et les langages de développement à code source ouvert (29 %).

Les entreprises connaissent la puissance des mégadonnées et sa capacité à faire émerger des informations exploitables, mais **27 % d'entre elles n'en profitent pas**, souvent en raison d'infrastructures désuètes (53 %) ou parce qu'elles opèrent dans des secteurs moins bien dotés en ressources, comme l'éducation et les services sociaux (50 %). Le coût reste un obstacle courant : **26 % des entreprises** citent les dépenses comme la plus grande barrière à l'adoption.

Et c'est là que l'engouement pour l'IA se heurte à la réalité :

85 % des entreprises utilisent des données pour prendre des décisions d'affaires

19 % de diminution dans l'utilisation d'outils d'analyse de données avancée

26 % des entreprises citent les coûts comme la plus grande barrière à l'adoption

PISTE DE RÉFLEXION

Alors que les entreprises s'efforcent d'exploiter les mégadonnées issues de l'IA et de l'analyse de données avancée, le principal défi n'est plus de savoir s'il faut investir, mais comment investir judicieusement.

L'écart entre l'expérimentation à l'aide d'outils génératifs (comme les outils d'IA fournissant des résumés de réunion ou rédigeant des courriels) et le déploiement de l'IA au niveau de l'entreprise (comme un modèle personnalisé pour une stratégie de tarification en temps réel) est important. Ces solutions varient considérablement en matière de coûts de mise en œuvre, de retour sur investissement, de complexité et d'exposition aux risques, en particulier dans des domaines tels que **la cybersécurité, la gouvernance des données et l'explicabilité des modèles.**

« L'IA doit être formée pour améliorer la prédictivité. Comme les données actuelles sont basées sur le passé (en remontant jusqu'à 2021 et 2022), les modèles d'IA doivent être alimentés en données sur l'avenir, ce qui nécessite une allocation budgétaire importante.

Stéphane Pincince
Directeur des TI,
Humania Assurance

Les solutions à code source ouvert (open-source) : favoriser l'innovation

Les technologies à code source ouvert ne sont plus des outils de niche, mais des outils courants. 85 % des entreprises canadiennes utilisent déjà au moins une solution à code source ouvert. Le taux d'adoption est encore plus élevé chez les experts TI (91 %), et chez les entreprises qui considèrent leur infrastructure technologique comme étant de pointe (91 %). Cette tendance reflète la reconnaissance croissante du fait que les plateformes à code source ouvert offrent une flexibilité inégalée, une innovation rapide et un bon rapport coût-efficacité.

RISQUES LIÉS AUX SOLUTIONS À CODE SOURCE OUVERT

Cybersécurité

L'accès libre au code augmente le risque de vulnérabilités non détectées et d'exploitation.

Soutien et maintenance

Le recours aux communautés bénévoles peut conduire à des mises à jour incohérentes et à une assistance technique limitée.

Conformité réglementaire

L'utilisation de solutions à code source ouvert dans les systèmes critiques peut entrer en conflit avec la souveraineté des données et les exigences de conformité.

Combler le fossé pour un avenir compétitif

Les données présentent un récit clair : l'infonuagique, l'IA, l'analyse de données avancée et les solutions à code source ouvert propulsent les investissements en TI planifiés et actuels dans l'ensemble du Canada. Toutefois, ce parcours comporte des défis. L'intégration de l'IA représente l'une des opportunités les plus prometteuses - mais aussi l'une des plus complexes - pour les entreprises modernes. Quel que soit le secteur d'activité ou la portée du projet, il est essentiel d'être bien accompagné lors de l'adoption de l'IA pour dégager une valeur à long terme tout en réduisant au minimum les conséquences imprévues. Dans cet environnement en rapide évolution, il faut privilégier une approche stratégique et indépendante, fondée sur des cas d'utilisation réels et des objectifs commerciaux. Il est donc nécessaire de poser les bonnes questions à propos du retour sur investissement, de l'intégration et de la viabilité à long terme avant d'autoriser toute implantation.

RISQUES ET OPPORTUNITÉS

Risques

Sécurité et vulnérabilité des données

S'appuyer sur des outils d'IA peut exposer l'entreprise à des risques considérables en matière de sécurité et d'intégrité des données. Le contrôle des données devient plus complexe lorsque l'information est accessible à des parties externes, en dépit des règles de gouvernance internes. Sans une gestion rigoureuse et des mécanismes de contrôle appropriés, l'entreprise risque de perdre le contrôle de ses données.

Adoption inéquitable

Les coûts élevés associés à la mise en œuvre de technologies de pointe en matière d'IA, d'analyse et de code source ouvert constituent des obstacles importants, en particulier pour les petites entreprises, ce qui risque de creuser le fossé concurrentiel. Il est également essentiel de disposer d'une équipe et d'une stratégie pour analyser, comprendre et exploiter la technologie.

Optimisme excessif quant aux économies associées à l'infonuagique

Le fait de croire que le passage à l'infonuagique se traduira inévitablement par des réductions de coûts peut s'avérer une erreur stratégique. Si l'infonuagique offre des avantages sur le plan de la flexibilité et de l'évolutivité, des coûts imprévus peuvent néanmoins survenir, notamment en raison de mauvaises configurations, de besoins de stockage accrus, de frais de transfert de données ou de services supplémentaires inattendus.

Opportunités

Amélioration de la productivité et réduction des coûts

L'IA permet de transformer des données brutes en renseignements stratégiques, ce qui améliore la prise de décisions et accroît l'efficacité. Si elle dispose des bons outils et d'une expertise interne, elle génère des indicateurs de performance clés plus rapidement et fournit des renseignements que l'analyse humaine pourrait ne pas détecter, ce qui permet d'optimiser les ressources et de réduire les coûts.

L'infonuagique pour accroître l'efficacité opérationnelle

L'augmentation constante de l'infonuagique démontre qu'elle rationalise les opérations en offrant des solutions évolutives et flexibles. Elle permet aux entreprises de s'adapter rapidement à l'évolution des exigences du marché, de renforcer la collaboration et d'améliorer la gestion des ressources, contribuant ainsi à accroître la souplesse opérationnelle.

Se distinguer de la concurrence grâce à l'analyse de données avancée

Tandis que 66 % des entreprises utilisent désormais l'analyse de données avancée, les entreprises les mieux à même d'utiliser cet outil ont la possibilité de découvrir des schémas cachés et d'acquérir un avantage stratégique. À mesure qu'une organisation gagne en maturité dans l'usage de ces technologies, elle peut enrichir ses décisions en s'appuyant sur un éventail plus large de données externes.

LA GRANDE QUESTION

De quelle manière votre organisation intégrera-t-elle l'IA, l'analyse de données avancée et l'infonuagique pour équilibrer les coûts, la sécurité et l'efficacité opérationnelle, afin de profiter d'un avantage solide et concurrentiel dans l'économie numérique d'aujourd'hui ?

04
CYBERSÉCURITÉ

Votre équipe TI ne peut pas y arriver seule : pourquoi la cybersécurité exige une nouvelle stratégie d'investissement

Les cyberattaques sont inévitables. Il suffit de jeter un coup d'œil à votre dossier de courriels indésirables pour vous rappeler que les pirates tentent constamment d'obtenir vos informations d'identification et de porter atteinte à l'intégrité de vos systèmes. Comme de plus en plus d'entreprises dépendent des TI, les récompenses pour les attaquants qui réussissent à compromettre un système ne font que croître. Il est peu probable que cette situation change. Elle reflète les crimes et les fraudes observés dans les systèmes non liés aux TI, mais à une plus grande échelle.

En même temps, les systèmes TI deviennent de plus en plus complexes et difficiles à protéger. Les petites entreprises sont particulièrement vulnérables à cette menace grandissante, car elles sont plus susceptibles de prioriser leur croissance et leur développement plutôt que leur infrastructure TI. Ce phénomène s'observe dans toutes les organisations, quelle que soit leur taille. Les équipes TI ont déjà fort à faire pour suivre les évolutions techniques, sans parler de la mise en œuvre des technologies, de la surveillance des cybermenaces et de la réaction face à des dernières. Ces défis peuvent être accentués par une réglementation qui diffère d'un territoire à l'autre et qui nécessite des contrôles personnalisés et également par la mondialisation croissante des entreprises et des plateformes TI qui transcende les champs de compétence. Même si la plupart des organisations font confiance aux compétences de leurs équipes TI en matière de sécurité, nous avons constaté une hausse du nombre de nouveaux programmes d'études supérieures dans les universités canadiennes visant à enseigner les bases de la cybersécurité aux professionnels, ce qui traduit le fait que la sécurité demeure un aspect peu approfondi dans la formation en TI.

L'un des rôles clés de la cybersécurité est un rôle opérationnel. Il ne suffit pas de déployer une technologie : il faut également la surveiller et y réagir. En règle générale, si 10 % du budget TI devait être consacré à la cybersécurité, une équipe de 10 professionnels TI ne comprendrait qu'une seule ressource de cybersécurité. Il est peu probable qu'une organisation disposant d'une seule ressource de sécurité opérationnelle soit en mesure de surveiller les cybermenaces et d'y réagir rapidement. Cela pourrait expliquer pourquoi les petites organisations ont plus tendance à affirmer qu'elles n'ont pas subi de cyberattaque, tandis que les grandes organisations sont plus susceptibles de reconnaître les attaques et les difficultés à les détecter. Pour savoir si vous avez été victime d'une attaque, il faut que vous soyez en mesure de la repérer !

La cybersécurité a évolué au-delà d'une simple approche basée sur les contrôles et s'inscrit maintenant dans un cycle de vie opérationnel complet. À lui seul, le pare-feu n'est pas suffisant : il faut aussi le surveiller et y réagir. À mon avis, toutes les organisations devraient s'assurer de mettre en place une authentification multifacteur sur chaque plateforme et chaque système qu'elles possèdent ou utilisent, et de déployer un logiciel de sécurité des points de terminaison sur l'ensemble de leurs actifs TI. Ces deux mesures permettent de prévenir et de contenir la majorité des attaques, mais nécessitent un investissement dans une équipe opérationnelle pour les surveiller (faire appel à un fournisseur de services de sécurité gérés (MSSP) peut être une bonne option). En combinant cette stratégie d'investissement à des sauvegardes indépendantes, à la formation des employés et à un programme de gouvernance qui effectue régulièrement un examen explicite des risques, les organisations peuvent établir une solide assise en matière de cybersécurité.

Marc Kneppers
Associé principal chez Goldenrod Consulting, spécialisé en cybersécurité

Ancien architecte en chef de la sécurité chez TELUS, il a dirigé des initiatives de protection des infrastructures à l'échelle nationale. Il conseille des organisations à l'international, y compris dans le domaine de la cybersécurité appliquée au secteur spatial.

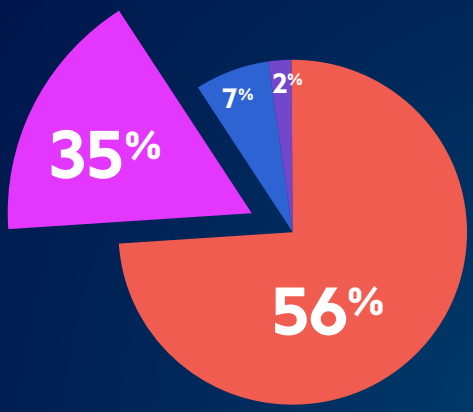
Marc est titulaire de diplômes de deuxième et troisième cycles en astrophysique et en science des données, et siège au comité consultatif du Consortium national en cybersécurité.

TABLEAU DE BORD

PERCEPTION

91%

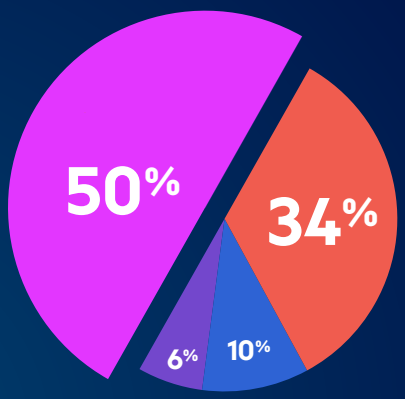
des entreprises déclarent faire confiance à leur équipe TI en matière de sécurité.



- Très confiant
- Assez confiant
- Peu confiant
- Pas du tout confiant

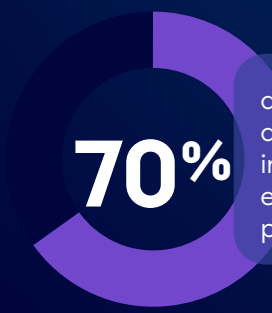
84%

des entreprises considèrent que la cybersécurité gagnera en importance comme avantage concurrentiel dans les années à venir.



- Oui, les clients privilégieront les entreprises dotées d'une sécurité renforcée
- Relativement, mais d'autres facteurs auront toujours plus d'importance
- Non, la cybersécurité sera une exigence standard, et non un facteur de différenciation
- Je ne sais pas

INVESTISSEMENT



des entreprises prévoient d'effectuer au moins un investissement supplémentaire en sécurité au cours des deux prochaines années.

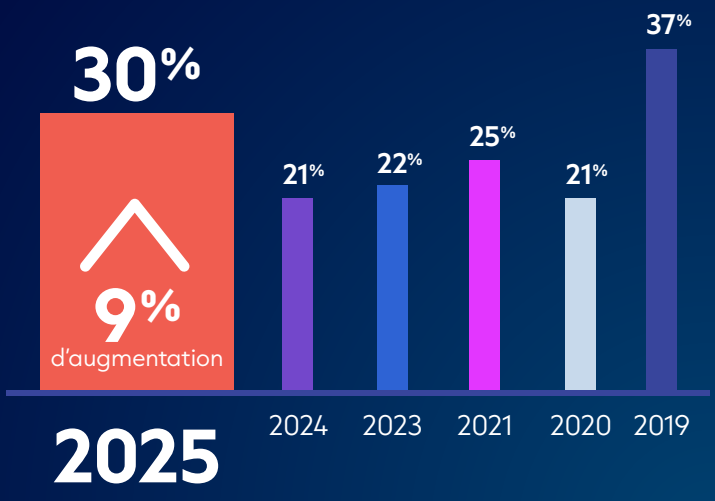
LES SIX principaux investissements prévus en cybersécurité :

Sensibilisation à la sécurité	**27%**
Prévention des pertes de données	**24%**
Détection des vulnérabilités	**19%**
Gouvernance des données	**19%**
Cyber-résilience	**19%**
Gestion des identités	**19%**

TABLEAU DE BORD

ÉTAT ACTUEL

Proportion d'entreprises ayant déclaré avoir été victimes d'une cyberattaque :

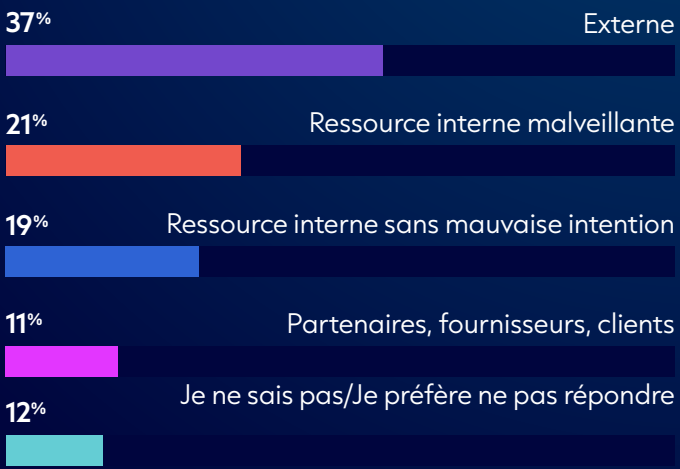


LES SIGNALEMENTS DE CYBERATTAQUES SONT À LEUR PLUS HAUT NIVEAU DEPUIS 2019.

LES ACTEURS EXTERNES CONSTITUENT LA PRINCIPALE SOURCE DE MENACES POUR LA CYBERSÉCURITÉ.

SEULEMENT **27 % DES RÉPONDANTS** ONT INDIQUÉ QUE LEUR ENTREPRISE **DÉTIENT UNE CYBERASSURANCE**. PARMI CEUX-CI, SEULEMENT 45 % DES POLICES COUVRENT À LA FOIS LES DONNÉES DES CLIENTS ET CELLES DES EMPLOYÉS.

Source de la dernière menace informatique :



Détenez-vous une cyberassurance ?

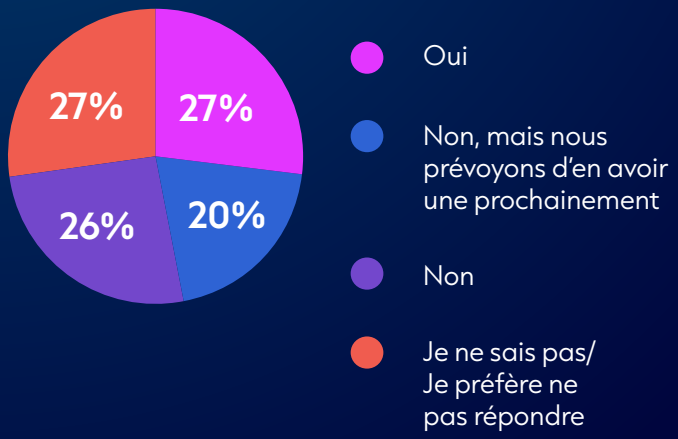


TABLEAU DE BORD

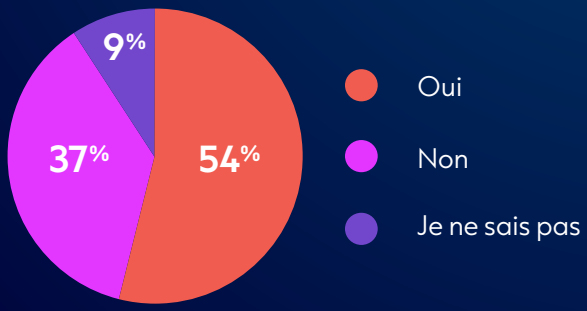
ÉTAT ACTUEL

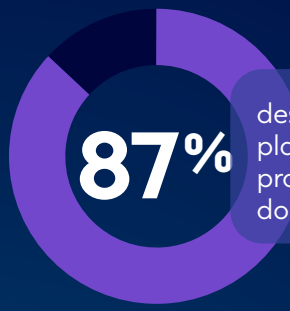
Malgré la généralisation des cyberattaques, **28 % des entreprises canadiennes n'ont pas offert de formation en cybersécurité** à leurs employés au cours de la dernière année.

Formation en cybersécurité offerte aux employés au cours de la dernière année :	
Oui, et je prévois d'en offrir une l'année prochaine	36 %
Oui, mais je ne sais pas si je vais en proposer une l'année prochaine	27 %
Non, mais je prévois d'en offrir une l'année prochaine	11 %
Non, et je ne prévois pas d'en offrir l'année prochaine	17 %
Je ne sais pas	9 %

MALGRÉ LES NOMBREUSES VIOLATIONS DE DONNÉES MÉDIATISÉES, **SEULEMENT 54% DES RÉPONDANTS ONT RÉÉVALUÉ LEURS PRATIQUES EN MATIÈRE DE SÉCURITÉ.**

Les violations de données relayées dans les médias ont-elles entraîné une révision de vos pratiques de sécurité ?





des entreprises ont mis en place au moins une mesure de protection contre la fuite de données.

LES CINQ mesures de protection les plus utilisées contre la fuite de données :

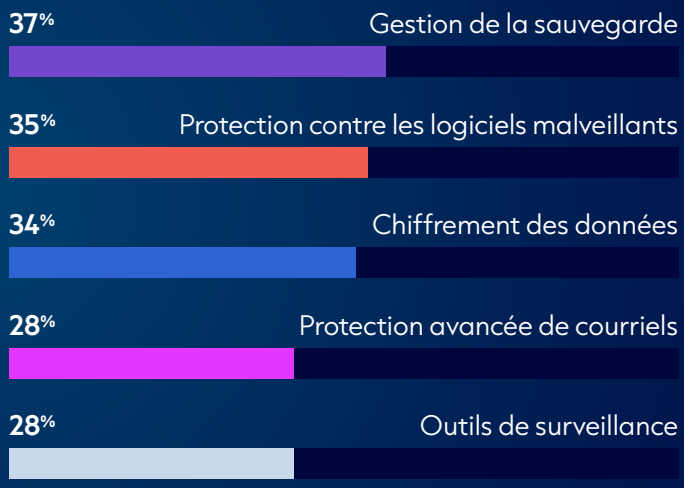


TABLEAU DE BORD

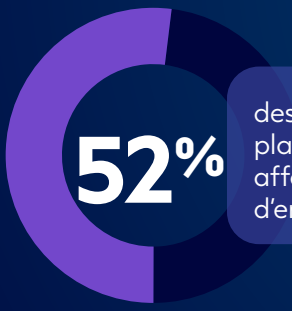
ÉTAT ACTUEL

LA LOI 25 DU QUÉBEC IMPOSE DES OBLIGATIONS PARTICULIÈRES AUX ENTREPRISES QUI GÈRENT DES DONNÉES PERSONNELLES CONCERNANT DES RÉSIDENTS DU QUÉBEC, QUEL QUE SOIT L'EMPLACEMENT DE L'ENTREPRISE. POURTANT, **33 % DES ENTREPRISES CANADIENNES NE CONNAISSENT PAS LA LOI, ET SEULEMENT 22 % SONT TOTALEMENT CONFORMES.**

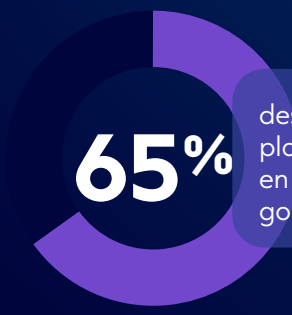
Respect des règles de confidentialité : quelle confiance les entreprises s'accordent-elles ?

Très confiant(e), nous adoptons une approche proactive	**30%**
Plutôt confiant(e), mais les changements réglementaires sont une source de préoccupation	**53%**
Peu confiant(e), nous avons du mal à les suivre	**10%**
Nous ne sommes pas certains de notre statut de conformité	**7%**

SEULEMENT 30 % DES ENTREPRISES ONT ADOPTÉ UNE APPROCHE PROACTIVE POUR RESTER CONFORMES À L'ÉVOLUTION DE LA RÉGLEMENTATION EN MATIÈRE DE PROTECTION DES DONNÉES.

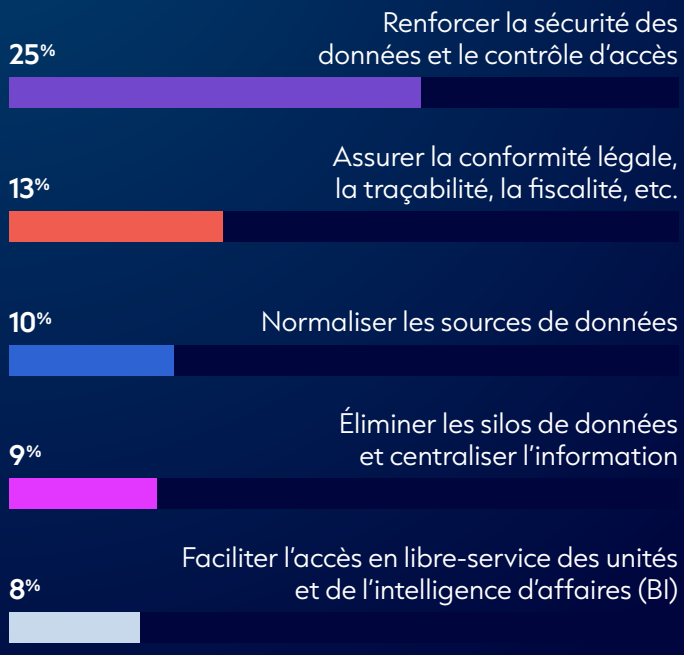


52% des entreprises ont mis en place un plan de continuité des affaires. Et près des trois quarts d'entre elles ont testé leur plan.



65% des entreprises ont mis en place ou envisagent de mettre en place un processus de gouvernance de données.

LES CINQ motivations clés de la gouvernance des données :



CYBERSÉCURITÉ

INTERPRÉTATION DES DONNÉES

Les menaces pour la cybersécurité ne sont pas près de disparaître

Dans le sondage de cette année, la sécurité et le budget se classent à égalité, en tête des défis auxquels font face les entreprises canadiennes. Par ailleurs, **la proportion d'entreprises ayant signalé avoir subi une menace de cybersécurité est passée de 21 % en 2024 à 30 % en 2025.** Malgré l'augmentation, cette proportion est probablement encore sous-estimée, étant donné que de nombreuses entreprises ne souhaitent pas révéler les cyberattaques dont elles ont été victimes, même dans le cadre d'un sondage anonyme.

Par conséquent, l'incidence réelle des attaques est à la hausse, mais comme les entreprises hésitent encore à signaler publiquement les cyberattaques dont elles sont victimes, cette proportion est certainement sous-estimée. Ainsi, le manque de préparation persiste malgré toutes les histoires de cyberattaques (grandes ou petites) que nous entendons chaque jour. En outre, comme le démontrait déjà notre rapport de 2024, **les entreprises canadiennes n'adoptent toujours pas les mesures appropriées pour se protéger des cybermenaces.**

MALGRÉ LA FRÉQUENCE ÉLEVÉE DES CYBERATTAQUES

28 % des entreprises canadiennes n'ont pas offert de formation en cybersécurité au cours de la dernière année. Parmi ces entreprises, 17 % ne prévoient pas d'en offrir l'année prochaine.

Seulement 27 % des répondants ont indiqué que leur entreprise détient une cyberassurance.

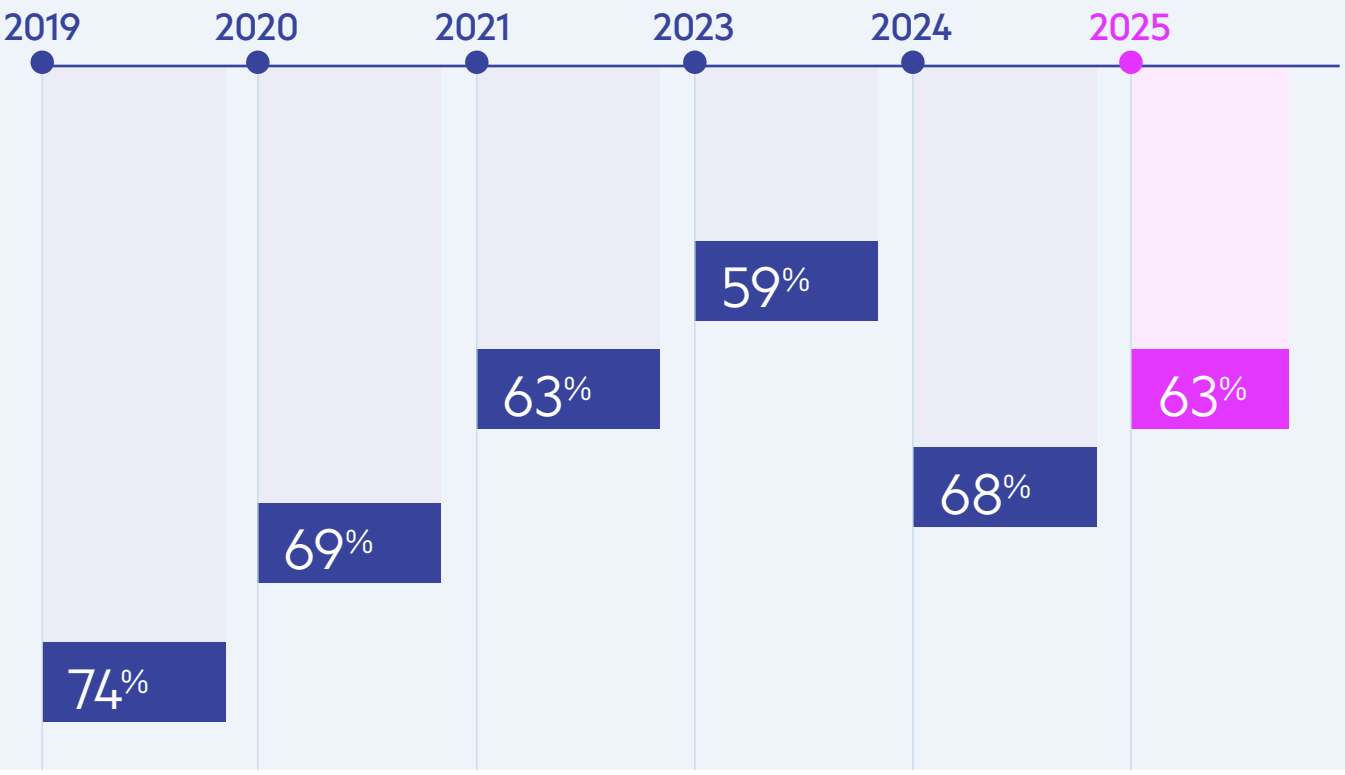
Les nouvelles sur des violations de données ont incité seulement **54 % des répondants à revoir leurs pratiques** en matière de sécurité des données, en baisse de 7 % par rapport à l'année dernière.

« Lorsqu'il s'agit d'évaluer et de gérer les risques à l'échelle de l'organisation, les solutions en silos et les infrastructures complexes nuisent à la visibilité nécessaire, compromettant ainsi la capacité à intervenir efficacement pour remédier aux menaces à grande échelle.

Jeff Sherman
VP Amériques, Intelligent Ops & BigFix, HCLSoftware

Nous constatons également une tendance constante d'une année à l'autre : les grandes entreprises, celles du secteur financier et celles qui ont déjà subi une attaque sont plus susceptibles d'avoir pris des mesures pour renforcer leur cybersécurité. Si cette tendance n'est pas surprenante, le décalage des petites entreprises demeure inquiétant, et reflète l'idée persistante que « cela ne m'arrivera pas »… jusqu'au moment où cela se produit.

AVEZ-VOUS OFFERT UNE FORMATION EN CYBERSÉCURITÉ À VOS EMPLOYÉS AU COURS DE LA DERNIÈRE ANNÉE ?



Une mauvaise compréhension de la menace

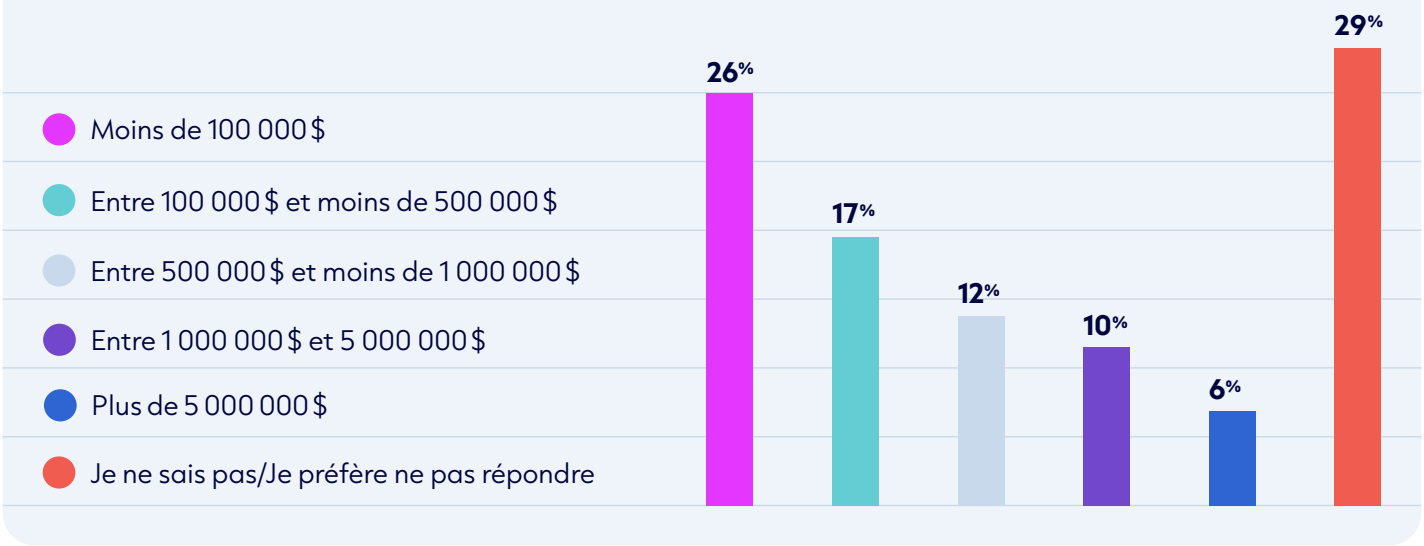
Ce manque de préparation peut s'expliquer par le fait que les décideurs ont mal compris l'ampleur de la menace.

De nombreuses entreprises hésitent encore à faire preuve de transparence à l'égard de leurs clients, de leurs pairs, du public ou même de leurs employés en ce qui concerne les attaques. Par exemple, 9 % des décideurs TI qui ont répondu au sondage de cette année ne savaient pas (ou ne voulaient peut-être pas divulguer) si leur entreprise avait déjà été victime d'une cyberattaque.

Interrogés sur le coût de leur plus récente cyberattaque, 29 % des répondants ont déclaré l'ignorer ou préférer ne pas répondre (une hausse considérable par rapport aux 14 % de 2024).

Ce manque de transparence laisse les décideurs dans l'ignorance quant à la probabilité réelle d'une cyberattaque et aux coûts qu'elle peut engendrer.

ESTIMATION DU COÛT D'UNE CYBERATTAQUE (COÛT DE LA RANÇON, DES RESSOURCES ADDITIONNELLES ET DES PERTES OCCASIONNÉES) :



La réponse la plus fréquente à la question du coût d'une cyberattaque est « moins de 100 000 $ » (26 %). Ce montant prévaut même pour les entreprises de plus de 500 employés. Compte tenu de l'éventail des coûts en jeu, il s'agit probablement d'une sous-estimation grossière. Outre le paiement d'une rançon, les cyberattaques entraînent également des coûts cachés, notamment les dommages collatéraux que constituent les frais juridiques, les interruptions de services, l'atteinte à la réputation, et bien plus encore.

DISPOSEZ-VOUS D'UN PLAN DE CONTINUITÉ DES AFFAIRES ?

Seulement 52 % des entreprises en ont un.

Pourquoi est-il nécessaire d'en avoir un ? Il est essentiel pour survivre à une crise, car il permet d'agir rapidement. De plus, il est souvent exigé dans le cadre d'une cyberassurance.

Posez-vous la question : Quels sont les services essentiels qui doivent demeurer en ligne pour que votre entreprise puisse continuer à fonctionner en cas de cyberattaque ?

En déterminant ces services, vous pourrez dissiper tout malentendu lors d'éventuelles cyberattaques.

« Chez IBM, nous avons constaté une augmentation constante du nombre d'entreprises victimes de cyberattaques, et les coûts de reprise ne cessent de grimper. Ces coûts peuvent être difficiles à mesurer, mais ils comprennent les frais juridiques, les frais de communication, les frais de réentraînement et, plus important encore, les dommages causés à votre marque.

Jay Badiani
Chef du marketing,
IBM Canada

Gouvernance des données : un enjeu souvent négligé

De pair avec la cybersécurité, la gouvernance des données est un domaine d'une importance capitale, mais encore largement sous-estimé par les entreprises canadiennes.

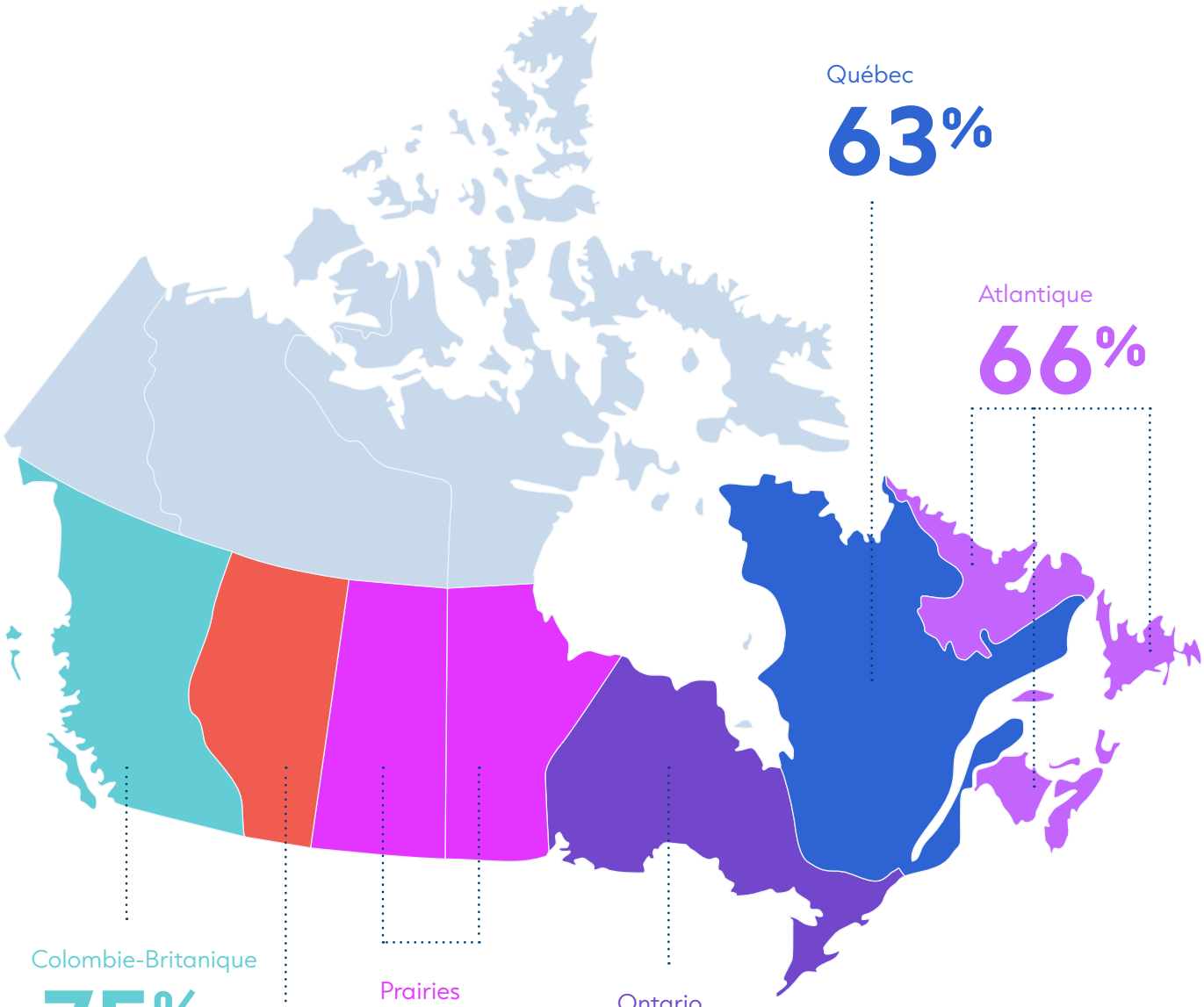
Par exemple, la loi 25 du Québec impose des obligations précises aux entreprises qui gèrent des données concernant des résidents du Québec, quel que soit l'emplacement de l'entreprise. Pourtant, **33 % des entreprises canadiennes et 19 % des entreprises québécoises ne connaissent pas encore cette loi.** En outre, seulement 22 % d'entre elles font état d'une conformité totale. Le gouvernement du Québec fournit de plus amples renseignements sur la manière de se conformer à la loi 25.

Seulement 30 % des entreprises déclarent adopter une approche proactive pour rester en conformité avec l'évolution des règlements en matière de protection des données. Les entreprises restantes (70 %) sont, d'une manière ou d'une autre, inquiètes, en difficulté ou incertaines de leur statut. À l'évidence, **une grande partie des entreprises canadiennes sont exposées non seulement à une gestion inappropriée de leurs données et aux cybermenaces qui en découlent, mais aussi aux conséquences juridiques d'un manque de conformité.**

POSEZ-VOUS LA QUESTION

Êtes-vous totalement conforme à la loi 25 du Québec, et êtes-vous prêt à assumer les conséquences financières d'une non-conformité ?

INTENTIONS D'INVESTISSEMENT EN CYBERSÉCURITÉ PAR PROVINCES EN 2025 :



RISQUES ET OPPORTUNITÉS

Risques

Absence de plan de continuité des affaires et de tests de sécurité

Les entreprises qui ne disposent pas d'un solide plan de continuité des affaires et qui ne testent pas régulièrement la résilience de leurs systèmes risquent de subir des conséquences catastrophiques dans l'éventualité d'une cyberattaque. Le processus d'élaboration d'un plan de continuité des affaires peut également aider les décideurs au sein de l'organisation à mieux comprendre les risques, notamment la perte potentielle de données critiques, les périodes d'indisponibilité prolongées et les atteintes à la réputation.

Formation insuffisante en cybersécurité

Les employés constituent la première ligne de défense contre les cyberattaques. Face à des attaques de plus en plus sophistiquées, l'absence de formation adéquate peut devenir une porte d'entrée pour les cybercriminels, mettant en péril la sécurité des données et des systèmes de l'entreprise.

Absence de cyberassurance

Même si le nombre de cyberattaques ne cesse d'augmenter, la majorité des entreprises ne détiennent pas de cyberassurance. Parmi celles qui en détiennent une, il est fréquent que la police ne couvre pas à la fois les données des employés et celles des clients. Une telle situation pourrait devenir très problématique dans l'éventualité d'une attaque.

Opportunités

Investissement stratégique

Effectuez une analyse d'impact sur les affaires, puis adaptez la feuille de route en matière d'investissements dans les TI de votre entreprise en conséquence. Les investissements qui renforcent la résilience de votre entreprise ouvriront la voie à d'autres opportunités d'investissement stratégique supplémentaires.

De petites mesures pour combler de grosses lacunes en matière de sécurité

Les décideurs peuvent être intimidés par l'ampleur des cybermenaces, mais de petits gestes comme la formation des employés, la gestion des accès par mots de passe et la réalisation de sauvegardes régulières peuvent renforcer considérablement la protection contre les attaques.

Règlements visant à orienter la gouvernance de données

Les règlements comme la loi 25 fournissent une orientation claire quant aux mesures que les entreprises doivent prendre pour protéger leurs propres données et celles de leurs clients. Passez en revue les règlements auxquels votre entreprise est soumise, ainsi que les mesures de sécurité de la chaîne d'approvisionnement exigées par vos clients, puis assurez-vous de sa conformité. Malgré son ampleur, ce processus peut protéger votre entreprise à la fois contre les cybermenaces et contre les conséquences juridiques d'une non-conformité.

LA GRANDE QUESTION

Avez-vous passé en revue vos pratiques en matière de formation, d'assurance et de conformité pour vous assurer que votre entreprise est aussi protégée que possible contre la menace inévitable des cyberattaques, y compris celles générées par l'IA ?

05
RESSOURCES HUMAINES

Anticiper l'avenir : remédier à la pénurie de talents en cybersécurité grâce à la collaboration

Au coeur de la cybersécurité : les humains, les processus et la technologie

Bien que la technologie et les processus soient des éléments essentiels de la cybersécurité, ce sont en réalité les personnes derrière ceux-ci qui constituent le véritable facteur de réussite.

Les professionnels qualifiés possèdent l'expertise nécessaire pour lutter contre les cybermenaces d'aujourd'hui, qui sont non seulement complexes, mais évoluent rapidement et deviennent de plus en plus sophistiquées.

Cependant, la main-d'œuvre mondiale en matière de cybersécurité est confrontée à un défi de taille : une pénurie de talents estimée à environ 2,8 millions, le secteur financier employant à lui seul 18 % de ces professionnels. Pour combler cette lacune, des efforts de collaboration concertés devront être déployés dans tous les secteurs.

Le pouvoir des partenariats : bâtir un avenir numérique plus sûr grâce à la collaboration

Ce défi ne peut être relevé de façon individuelle par une seule organisation ou un seul secteur d'activité. La solution repose sur des partenariats stratégiques réunissant des intervenants des milieux académiques, industriels et gouvernementaux qui travaillent de concert pour développer un écosystème de cybersécurité résilient. Cette collaboration permet de créer un solide bassin de talents, d'élaborer des solutions innovantes et de nous défendre efficacement contre les cybermenaces.

Grâce à des partenariats actifs, nous pouvons arrimer les programmes d'enseignement aux besoins de l'industrie, mettre en œuvre des programmes de formation pratique et faire connaître les carrières diverses et gratifiantes dans le domaine de la cybersécurité. Ces efforts collectifs sont essentiels à la formation d'une main-d'œuvre outillée pour faire face aux complexités des menaces informatiques dans le paysage actuel.

Combler les écarts de compétences par des stratégies collaboratives

L'un de nos plus grands défis consiste à nous assurer que les programmes d'enseignement répondent aux exigences de l'industrie. Nous devons collaborer avec les établissements d'enseignement pour moderniser les programmes et créer des possibilités d'apprentissage par l'expérience, comme des stages, des formations d'apprentis et des mentorats dans des contextes concrets.

Ces initiatives favorisent l'acquisition de compétences pratiques et permettent aux organisations de cibler rapidement les talents prometteurs. Les partenariats avec les milieux académiques pour évaluer et mettre à jour les programmes garantissent que les diplômés acquièrent des compétences pertinentes et recherchées.

Il est tout aussi important de faire connaître les carrières dans le domaine de la cybersécurité. En incitant les écoles primaires et secondaires à promouvoir les disciplines STIM et MATIS, on élargit le futur bassin de talents et on suscite un intérêt précoce pour les carrières dans le domaine de la cybersécurité. En invitant les étudiants universitaires, les diplômés et les anciens élèves à participer à des ateliers, à des conférences, à des programmes de diffusion et à des salons de l'emploi, on stimule la curiosité et on incite la nouvelle génération à poursuivre une carrière dans ce secteur vital.

La sensibilisation contribue grandement à corriger les idées fausses et à expliquer que la cybersécurité n'est pas uniquement technique. Il s'agit d'une discipline multidimensionnelle qui exige réflexion stratégique, communication, résolution de problèmes et leadership. La création d'un écosystème de cybersécurité complet nécessite la participation de rôles techniques et non techniques.

Investir dans la croissance et le développement continus

Pour conserver une longueur d'avance dans la gestion de la pénurie de talents, les organisations doivent prioriser le développement continu, tant pour les professionnels actuels que pour les débutants. La formation continue est essentielle pour s'adapter à l'évolution des technologies et des menaces. Afin de former une main-d'œuvre plus agile et mieux préparée, il faut investir dans des programmes comprenant des compétences fondamentales et avancées en matière de cybersécurité.

Des formations adaptées aux différents niveaux de compétences et basées sur des rôles précis permettent d'améliorer la capacité opérationnelle. Une formation en cybersécurité pour les cadres et les membres des conseils d'administration est également indispensable pour prendre des décisions éclairées. De plus, la création d'une culture de l'apprentissage continu améliore la rétention du personnel et la satisfaction au travail.

Collaborer avec le gouvernement pour contrer la pénurie de talents

Les organismes gouvernementaux jouent un rôle déterminant dans l'élaboration de politiques, le financement d'initiatives et la création de programmes destinés à attirer et à former des talents dans le domaine de la cybersécurité. Pour élargir son bassin de talents, il est essentiel de déployer des efforts conjoints afin de soutenir la formation, les stages et les campagnes de sensibilisation du public. Les partenariats avec le gouvernement permettent également d'influencer les normes et les politiques d'enseignement, assurant ainsi l'harmonisation avec les besoins de l'industrie et les priorités en matière de sécurité nationale.

Une vision commune pour la création d'un écosystème de cybersécurité résilient

La voie à suivre implique une collaboration et une action stratégique constantes. Ensemble, nous devons :

- Renforcer les partenariats intersectoriels pour développer des bassins de talents novateurs
- Aligner les normes d'enseignement aux exigences de l'industrie
- Élaborer des programmes de formation pratique, de mentorat et de stage
- Faire connaître les carrières dans le domaine de la cybersécurité afin d'attirer des talents variés
- Soutenir l'apprentissage continu pour garder une longueur d'avance sur les menaces émergentes

En travaillant ensemble, nous pouvons former une main-d'œuvre en cybersécurité qui soit résiliente, innovante et en mesure de relever les défis futurs.

Unité et objectif commun : le fondement de notre réussite collective

Tous les intervenants, qu'il s'agisse d'éducateurs, de chefs d'industries, de décideurs politiques ou de professionnels en devenir, jouent un rôle crucial dans la création d'un futur résilient en matière de cybersécurité. En travaillant en collaboration, nous pouvons transformer le défi de la pénurie de talents en occasions d'innovation, de croissance et de réalisation communes. La collaboration intersectorielle est essentielle pour bâtir un écosystème de cybersécurité solide et adaptable dont tout le monde peut tirer parti.

Notre engagement collectif à nouer des partenariats favorisera la création d'un environnement inclusif et dynamique, ancré dans la ténacité, la diversité et l'excellence. Ensemble, nous pouvons donner les moyens d'agir à la prochaine génération de dirigeants en cybersécurité, protéger notre infrastructure numérique et transmettre un héritage durable de résilience et d'innovation.

ELAINE HUM
Directrice des partenariats en cybersécurité, Scotiabank

Elaine Hum est une leader reconnue, forte de plus de 20 ans d'expérience dans divers secteurs. Elle pilote des stratégies de talents inclusives, développe des partenariats stratégiques et promeut l'innovation. Nommée Femme de l'année en cybersécurité (2023), elle accompagne activement et siège sur plusieurs conseils d'administration pour renforcer la communauté de la cybersécurité.

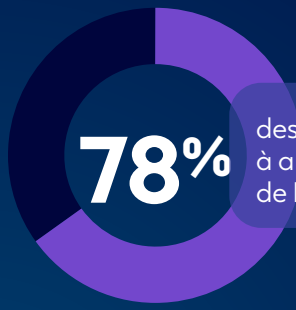
TABLEAU DE BORD

PERCEPTION

LES CINQ PRINCIPAUX

défis RH en TI :

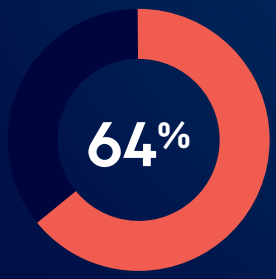
Rétention des ressources clés	**30%**
Manque de formation et de développement des compétences	**25%**
Difficulté d'attraction de ressources qualifiées	**23%**
Manque d'équilibre entre la vie personnelle et professionnelle	**22%**
Difficulté à mobiliser et motiver les ressources compétentes	**20%**



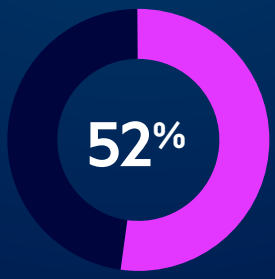
des services TI ont fait face à au moins un enjeu en matière de RH.

INVESTISSEMENT

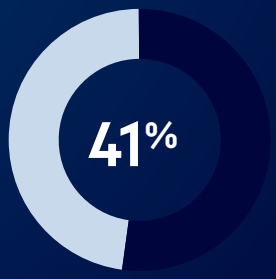
Investissements prévus en ressources humaines en TI :



La formation/le développement de compétences



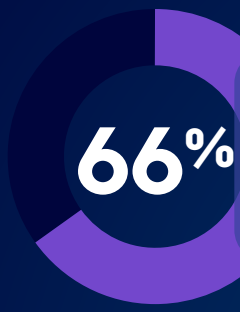
L'embauche de nouveaux employés



L'embauche de consultants externes

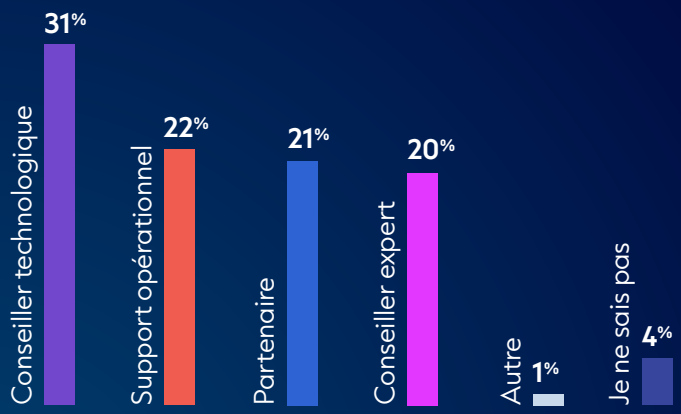
TABLEAU DE BORD

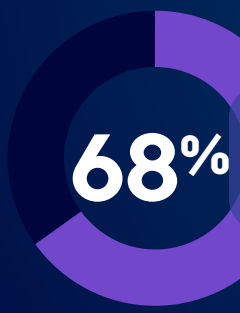
ÉTAT ACTUEL



66% des répondants déclarent collaborer avec une firme externe en TI en 2025, une proportion en baisse par rapport à 80 % en 2024.

Rôle de la firme externe en TI :





68% des répondants ont recours à des services de ressources TI temporaires.

Raisons de recourir à des ressources TI temporaires :

Manque de ressources disponibles	**25%**
Raisons financières/économie de coûts	**21%**
Mandat de courte durée ou ponctuel	**20%**
Manque d'expertise à l'interne	**17%**
Volonté d'externaliser les services TI	**17%**

RESSOURCES HUMAINES

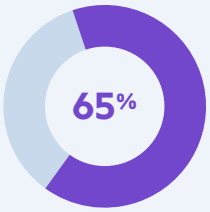
INTERPRÉTATION DES DONNÉES

Difficultés en matière de rétention des talents

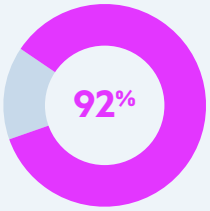
L'attraction, le développement, la fidélisation et l'engagement de talents qualifiés en TI représentent toujours des enjeux majeurs pour les services technologiques à travers le pays. Au total, **78 % des organisations ont rencontré au moins une difficulté liée aux ressources humaines dans ce secteur.** Ce sont les entreprises de taille moyenne qui ont le plus souvent rapporté de tels obstacles, probablement en raison de besoins organisationnels plus nuancés et de moyens plus limités que ceux des grandes entreprises.

Cette année, **la rétention des ressources clés** a dépassé le « manque de formation et de développement des compétences » comme enjeu principal des services TI.

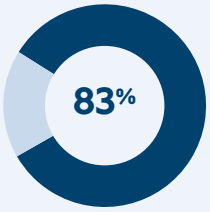
ENTREPRISES AYANT RENCONTRÉ AU MOINS UN DÉFI EN MATIÈRE DE RH EN TI :



Petites
(moins de 100 employés)



Moyennes
(de 100 à 499 employés)



Grandes
(au moins 500 employés)

« La rétention des talents en TI n'est pas seulement une question de salaires compétitifs; sur le marché actuel, qui est en constante évolution, nos experts TI choisissent leur employeur en fonction de l'ensemble des conditions de travail offertes. Nous devons créer un environnement où ils peuvent s'épanouir, se développer et se sentir réellement valorisés, car il ne s'agit pas seulement de pourvoir des postes, mais de bâtir des équipes qui attirent et maintiennent en poste les meilleurs candidats, dans un contexte de concurrence féroce entre les talents.

Martin Larivière
VP Ressources humaines,
Groupe NOVIPRO

Fait intéressant, bien que le maintien en poste figure souvent en tête de liste, les principaux défis des TI en matière de RH varient selon la taille de l'entreprise, son emplacement et le type de répondant. Les petites entreprises sont les moins susceptibles d'être confrontées à tout problème de RH relatives aux TI, probablement parce qu'elles n'ont pas la capacité d'engager du personnel spécialisé en TI. Les moyennes et grandes entreprises citent le maintien en poste comme leur principale préoccupation. La rétention du personnel interne des TI constitue le défi le plus courant dans l'ensemble du pays. Au Québec et en Alberta, **l'attraction** occupe plutôt le premier rang à ce chapitre. Enfin, dans les Prairies, l'équilibre entre le travail et la vie personnelle trône au sommet des préoccupations.

Le recrutement des meilleurs talents en TI au Québec est devenu de plus en plus difficile, plus particulièrement pour les entreprises qui insistent sur un modèle 100 % présentiel. De nombreux candidats exigent désormais la flexibilité du télétravail ou mode hybride pour mieux concilier travail et vie personnelle. Dans le contexte concurrentiel actuel, l'image de marque de l'employeur n'est plus un luxe, mais un levier essentiel pour attirer et fidéliser les meilleurs profils. Les organisations qui investissent dans une image forte et attrayante constatent généralement une réduction notable du coût par embauche, car les candidats évaluent avec soin l'ensemble de la proposition d'emploi.

Les décideurs TI et non TI ont des visions très différentes quant aux domaines où les investissements en ressources humaines sont les plus nécessaires. Ainsi, **71 % des décideurs TI** prévoient d'investir dans **la formation et le développement des compétences**, contre seulement **53 % des décideurs non TI**. L'écart est encore plus marqué en ce qui concerne le recrutement : **59 % des décideurs TI envisagent d'embaucher de nouveaux employés**, comparativement à **35 % des dirigeants non TI**. Sans surprise, les petites entreprises sont nettement moins enclines à investir dans les ressources humaines en TI que les entreprises de taille moyenne ou grande.

Malgré les nombreux défis rencontrés, bon nombre d'entreprises reconnaissent la nécessité d'allouer un budget stratégique à leur service TI. Ainsi, 52 % prévoient de consacrer des ressources financières à l'embauche de nouveaux talents, tandis que 64 % comptent investir dans la formation et le développement des compétences de leur personnel actuel. Si ces intentions témoignent d'une volonté d'amélioration, il demeure préoccupant que près d'une organisation sur deux n'envisage aucun investissement dans de nouvelles ressources TI, et que près de quatre sur dix ne prévoient pas de budget pour faire évoluer les compétences internes.

INVESTISSEMENTS PRÉVUS EN RESSOURCES HUMAINES LIÉES AUX TI :

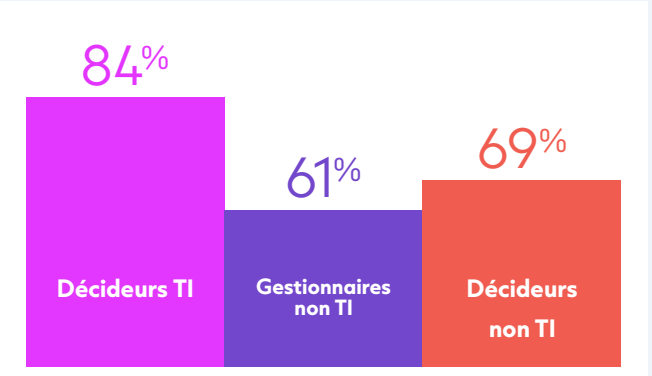
64 % Formation/ développement des compétences

52 % Embauche de nouveaux employés

41 % Embauche de consultants externes

LES DÉCIDEURS TI SONT BEAUCOUP PLUS SUSCEPTIBLES D'EXPRIMER LEURS PRÉOCCUPATIONS RELATIVES AUX RH EN TI QUE LES DÉCIDEURS NON TI.

Répondants signalant au moins un problème en ressources humaines dans le domaine des TI :



Soutien externe et temporaire

La majorité des entreprises canadiennes continue de collaborer avec des partenaires externes dans le domaine des TI (66 %), contre 80 % en 2024, ainsi qu'avec des ressources temporaires en TI (68 %). Ces statistiques révèlent une tendance à investir dans les employés permanents afin de préserver les connaissances organisationnelles à l'interne et de réduire la dépendance à long terme envers les firmes externes. Autrefois limitées à des fonctions d'expert-conseil, ces sociétés externes participent désormais de plus en plus au fonctionnement quotidien des organisations. Bien que l'on puisse penser que ces ressources externes servent de solution temporaire aux petites entreprises à capacité limitée en raison de leurs petites équipes ou même de leurs équipes inexistantes, les moyennes et grandes entreprises sont en réalité beaucoup plus susceptibles de recourir à des agences. Le secteur des services financiers, avec sa myriade de besoins en TI, est également le plus enclin à travailler avec des partenaires externes et des ressources temporaires.

Lors de l'utilisation de ressources externes ou temporaires, il est impératif de mettre en place des contrôles stratégiques et proactifs de gestion des risques et de l'accès. Bien que le recours à des ressources externes comporte des risques concernant la cybersécurité, les avantages d'un partenariat avec une société externe qui dispose de l'expertise spécialisée nécessaire au renforcement des contrôles, à la réduction des vulnérabilités et au soutien d'une position de cybersécurité alignée sur les priorités de l'entreprise peuvent valoir le faible risque.

AVANTAGES DE LA COLLABORATION AVEC UNE SOCIÉTÉ EXTERNE DANS LE DOMAINE DES TI

Les sociétés externes peuvent offrir une souplesse accrue, plus particulièrement pour les mandats ciblés qui nécessitent des compétences hautement spécialisées, de courtes durées ou des technologies de niche, pour lesquels le partenariat avec des experts externes peut offrir un avantage stratégique important.

Face à l'incertitude économique et à la complexité du contexte politique, de nombreuses entreprises canadiennes doivent examiner leur budget avec rigueur et faire des choix difficiles. Sous la pression croissante des coûts, plusieurs ont ajusté leurs effectifs en réduisant leur dépendance aux partenaires externes, y compris pour des mandats spécialisés ou des conseils de haut niveau. Dans bien des cas, les récentes initiatives en ressources humaines ou les efforts de restructuration interne exercent déjà une pression importante sur les équipes, poussant ainsi les organisations à internaliser davantage de responsabilités.

Si cette stratégie prudente peut générer des économies à court terme, elle comporte également des risques. En limitant l'apport d'expertises externes, les entreprises risquent de freiner leur capacité d'innovation, de perdre en agilité organisationnelle et d'accroître leur vulnérabilité face à des menaces émergentes - notamment en cybersécurité. Dans un environnement technologique en perpétuelle transformation, maintenir une ouverture vers l'extérieur demeure souvent essentiel pour rester compétitif.

« Les demandes directes de clients en matière de talents temporaires en TI ont diminué au cours des dernières années, mais notre équipe n'a jamais été aussi occupée en raison de l'augmentation du nombre de mandats confiés par des partenaires. Ce virage démontre que, malgré la diminution du nombre de demandes directes, le marché des ressources temporaires demeure solide.

Mélanie Gilbert
Directrice acquisition de talents,
NOVIPRO

RISQUES ET OPPORTUNITÉS

Risques

Retard dans le développement des compétences

Faute de miser régulièrement sur la formation continue des équipes TI, les entreprises s'exposent à un décalage technologique croissant, compromettant leur capacité à suivre le rythme de l'innovation.

Fidélisation des meilleurs talents

Attirer les meilleurs profils TI est une priorité pour les entreprises à travers tout le pays. Si votre organisation n'offre pas un bon équilibre travail-vie personnelle comparable à celui de vos concurrents, vous risquez de voir partir vos ressources clés vers d'autres employeurs.

Incertitude économique entraînant des compressions budgétaires

La prudence budgétaire peut contraindre les entreprises à sous-investir dans les RH, notamment en limitant le recours à des firmes externes, et accroître ainsi la pression et la charge de travail du personnel interne. La réduction de l'apport externe compromet également l'innovation et l'agilité opérationnelle, et elle complique du même coup la gestion des risques.

Opportunités

Collaboration avec des conseillers externes

Les partenaires externes sont de plus en plus sollicités à titre de conseillers technologiques. S'associer à une firme expérimentée permet de bénéficier d'une expertise essentielle pour protéger votre entreprise et garder une longueur d'avance.

Utilisation de ressources temporaires en TI

Travailler avec une ressource en TI temporaire peut répondre à des besoins à court terme ou compléter l'expertise en TI pour les entreprises manquant de capacité interne. Cela offre à votre entreprise une plus grande flexibilité pour gérer les charges de travail ponctuelles sans engagement à long terme.

Investir dans la formation

Un engagement constant envers la formation et le développement des compétences de votre équipe TI est essentiel pour garantir leur expertise face aux évolutions technologiques et aux défis à venir.

LA GRANDE QUESTION

Quelle est votre stratégie pour établir l'équilibre entre la rétention du personnel interne et les partenariats externes ? Avez-vous évalué les risques, les avantages et le coût de renonciation ?

06
MODERNISATION

L'IA entre attentes élevées et réalités du terrain

Les dernières données confirment ce que j'observe sur le terrain depuis plusieurs mois. Des échanges avec des professionnels, des créateurs de contenu et des directeurs marketing révèlent que si l'enthousiasme pour les outils alimentés par l'IA reste élevé, il est de plus en plus tempéré par le pragmatisme et l'accent mis sur l'application dans le monde réel.

Des développements récents ont mis en lumière ces tendances. Les déploiements successifs des plateformes d'IA générative de Google, de Microsoft et d'OpenAI ont manifestement suscité un vif intérêt temporaire. Chaque nouvelle fonctionnalité, qu'il s'agisse des résumés automatiques des courriels ou des assistants d'IA dans Word, a généré une courte vague d'adoption suivie d'un plateau. Les utilisateurs ne se contentent plus d'expérimenter, ils cherchent désormais à intégrer ces technologies dans leurs flux de travail quotidiens et à obtenir un retour sur investissement évident. Cependant, à mesure que l'effet de nouveauté s'estompe, l'engagement connaît une légère baisse ou une stagnation dans certains segments, marquant une évolution vers une adoption plus rationnelle et mesurée.

En même temps, la productivité fait l'objet d'une attention renouvelée. Au-delà de l'effet de nouveauté et de la génération de textes ou d'images, les organisations automatisent des tâches particulières telles que la rédaction de rapports, l'élaboration de présentations et le tri de courriels. Cette évolution est visible dans la montée en puissance d'outils tels que Notion AI et de modules intelligents au sein des systèmes de gestion de la relation client. Cependant, malgré l'essor des outils d'IA, ce qui m'a surpris, c'est que certains secteurs, en particulier les petites entreprises et le milieu de l'éducation, restent prudents. Est-ce dû à un manque de ressources, de formation ou de vision? Il est probable qu'il s'agisse d'un mélange des trois.

De plus, les discussions en cours sur l'éthique et la réglementation, attribuables aux annonces des gouvernements de l'Union européenne et de l'Amérique du Nord, ont incité certaines organisations à adopter une approche attentiste. Du côté des consommateurs, la couverture médiatique sensationnaliste des « risques liés à l'IA » et des « pertes d'emplois massives » a stimulé à la fois l'excitation et l'appréhension.

En bref, les données correspondent aux observations faites sur le terrain : la curiosité reste forte, mais elle s'accompagne désormais d'attentes plus élevées et d'une volonté de mise en œuvre efficace. L'IA fait désormais partie de la culture populaire et de la culture d'entreprise, marquant un moment charnière où les utilisateurs s'efforcent de trouver leur équilibre entre l'engouement médiatique et la productivité réelle.

BRUNO GUGLIELMINETTI
Consultant/producteur de podcast : MonCarnet.com

En tant qu'animateur de podcast et d'émission de radio, Bruno est également consultant en stratégie numérique. Par ailleurs, il donne des conférences, propose des formations et analyse les actualités dans les domaines des communications et des médias numériques. Fort de plus de 83 000 abonnés quotidiens sur Twitter et grâce à son podcast hebdomadaire MonCarnet.com, il présente les aspects essentiels de l'actualité numérique.

TABLEAU DE BORD

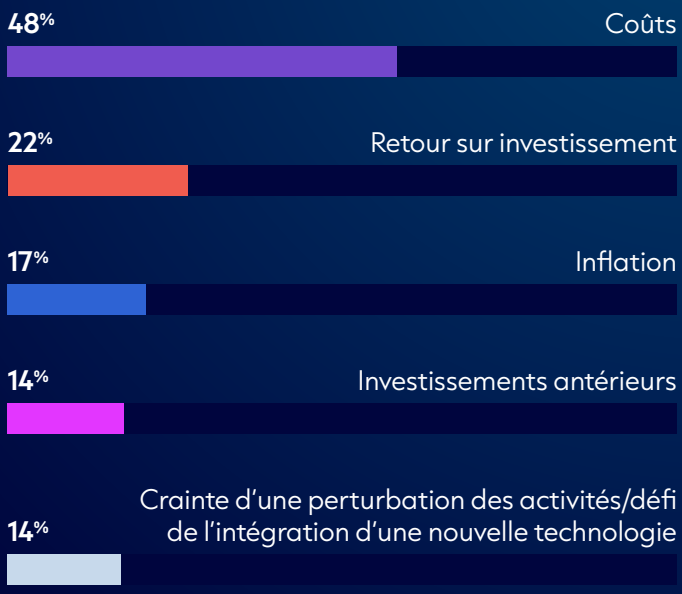
PERCEPTION

LES CINQ PRINCIPAUX

facteurs de sélection de technologies pour la modernisation :

Exigences en matière de sécurité et de conformité	**27%**
Retour sur investissement et rentabilité	**27%**
Compatibilité avec les systèmes et infrastructures existants	**26%**
Évolutivité et potentiel de croissance future	**24%**
Flexibilité pour la personnalisation et l'adaptabilité	**22%**

LES CINQ principaux obstacles à la modernisation des équipements TI :



ÉTAT ACTUEL

LA MAJORITÉ DES ENTREPRISES CANADIENNES A ATTEINT LE STADE DE LA MISE EN ŒUVRE DE SES EFFORTS DE MODERNISATION.

Stade des efforts de modernisation des applications :

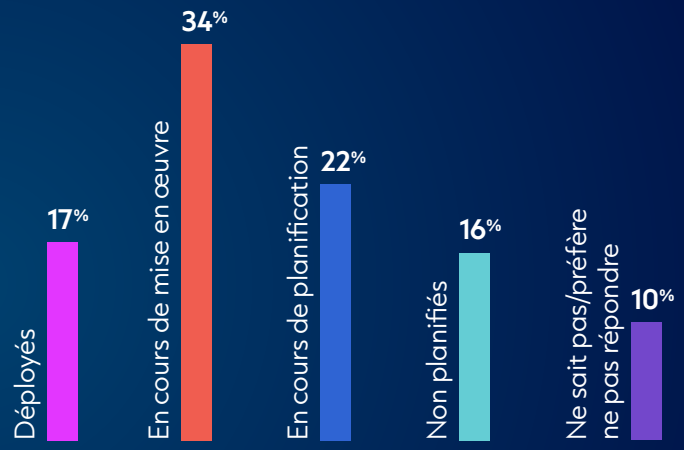
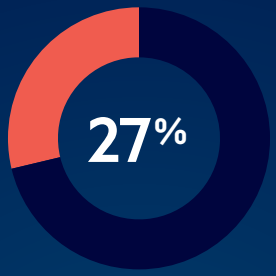


TABLEAU DE BORD

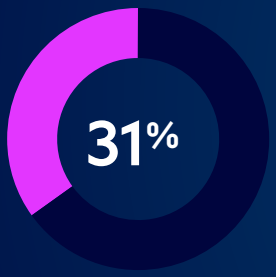
INVESTISSEMENT

LES CINQ PRINCIPAUX

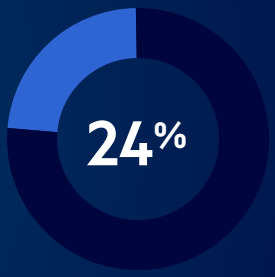
domaines dans lesquels des investissements de modernisation sont prévus :



Infrastructure et services infonuagiques



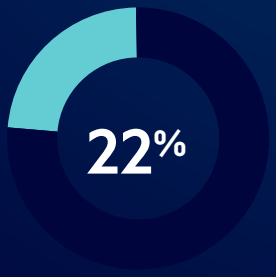
Solutions de cybersécurité



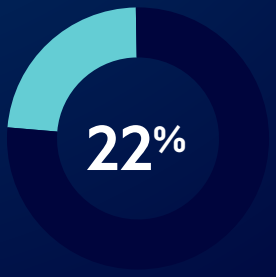
IA et apprentissage machine

80%

des entreprises prévoient investir dans la modernisation d'au moins un domaine des TI au cours de la prochaine année.



Modernisation des systèmes hérités



Mises à niveau du réseau et de l'infrastructure

MODERNISATION

INTERPRÉTATION DES DONNÉES

La volonté de modernisation

Le contexte technologique des TI évolue si rapidement que la modernisation des applications TI demeure un objectif important des services TI de l'ensemble du Canada. Le rapport de cette année révèle que huit entreprises canadiennes sur dix prévoient d'investir dans la modernisation d'au moins un domaine des TI au cours de la prochaine année.

La majorité (34 %) des entreprises canadiennes en sont à la phase de la mise en œuvre de ses efforts de modernisation. Entre 2023 et 2024, nous avons observé une modeste hausse (6 %) du nombre d'entreprises ayant atteint le stade du déploiement. Cette année, ce taux n'a augmenté que de 1%. Bien que de nombreuses raisons puissent expliquer cette baisse, il est clair qu'un retour sur investissement est essentiel à la prise de décisions sur la modernisation. De plus, comme la modernisation relève des décisions d'affaires, et non seulement des TI, et compte tenu de l'incertitude économique persistante actuelle et des tensions commerciales avec les États-Unis, les organisations scrutent leurs dépenses de plus près. Ainsi, bon nombre de ces dernières décident de faire une pause et de réévaluer les investissements.

Le coût demeure le principal obstacle à la modernisation, quels que soient la région, le secteur ou la taille de l'entreprise. Compte tenu de ces préoccupations, il n'est pas surprenant que les petites entreprises (moins de 100 employés) soient beaucoup moins susceptibles que les grandes d'avoir prévu des investissements dans la modernisation.

Bien que les progrès en matière de modernisation n'aient pas évolué de façon significative depuis 2024, des développements intéressants se sont produits dans les domaines où les entreprises concentrent leurs efforts de modernisation. Cette année, la cybersécurité a dépassé l'infrastructure infonuagique en tant que principal domaine d'investissement prévu. La modernisation des systèmes hérités et les mises à niveau du réseau/de l'infrastructure sont restées importantes, tandis que l'IA et l'apprentissage machine se sont hissés parmi les cinq principaux domaines d'intérêt.

La cybersécurité est le principal domaine d'investissement prévu aux fins de modernisation des entreprises de toutes tailles et dans la plupart des régions du pays. Fait intéressant, l'infrastructure et les services infonuagiques sont les principaux domaines dans lesquels les entreprises de la Colombie-Britannique et des Prairies prévoient d'investir, contrairement à la tendance nationale. Cette différence s'explique en grande partie par la présence croissante de géants des technologies : Microsoft a renforcé sa présence à Vancouver grâce à la mise en œuvre d'une zone Azure Edge, en 2021, tandis qu'Amazon Web Services a établi une nouvelle région infonuagique à Calgary, en 2024. Ces initiatives facilitent l'accès à une infrastructure de pointe et encouragent les entreprises locales, plus particulièrement dans les secteurs des technologies, de l'énergie et de l'agriculture, à moderniser leurs activités grâce à des solutions infonuagiques flexibles, évolutives et rentables.

La cybersécurité est le principal domaine d'investissement prévu aux fins de modernisation des entreprises de toutes tailles et dans la plupart des régions du pays.

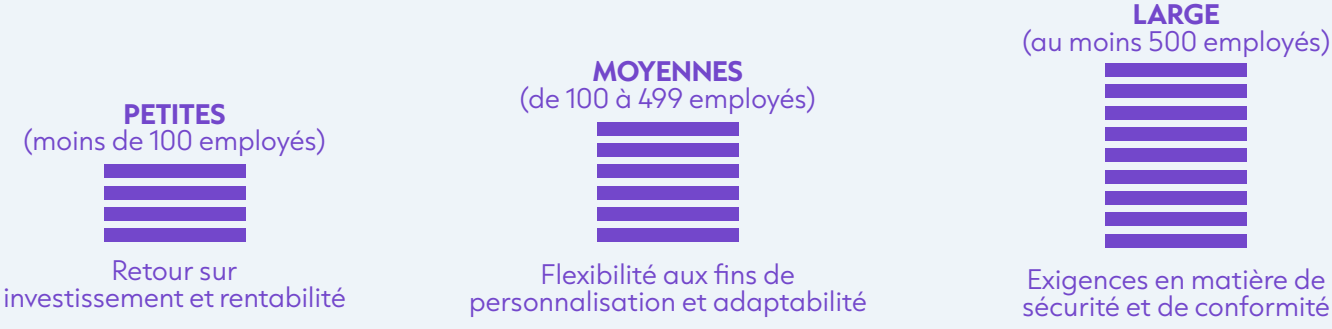
Pourquoi moderniser ?

Les critères déterminants dans le choix des technologies à moderniser sont demeurés constants depuis 2024. La sécurité, le retour sur investissement ainsi que la compatibilité avec les systèmes en place restent les principales préoccupations des entreprises.

Bien que les exigences en matière de sécurité et de conformité demeurent parmi les critères les plus importants, leur importance relative a diminué de façon notable depuis 2024. Cette année, seulement 27 % des répondants ont mentionné la sécurité comme facteur déterminant dans la sélection des technologies à moderniser, comparativement à 38 % l'année précédente. Cette année, la répartition plus équilibrée des priorités, témoigne de **la complexité croissante des enjeux auxquels les équipes TI sont confrontées lorsqu'elles doivent gérer des ressources limitées.**

PRINCIPAUX FACTEURS DE SÉLECTION DE TECHNOLOGIES POUR LA MODERNISATION

Selon la taille des entreprises :



« Bien que la sécurité soit essentielle et doit être prise en compte dans toute décision d'affaires, dans le contexte actuel, les entreprises doivent également composer avec la réalité économique et accorder la priorité au retour sur investissement. D'autres facteurs, tels que l'interopérabilité avec les systèmes existants, entrent également en ligne de compte. L'ensemble de ces pressions concurrentes pourrait expliquer le recul de la sécurité parmi les considérations principales, malgré son rôle crucial.

Alain Cormier
Président-directeur général,
Groupe NOVIPRO

RISQUES ET OPPORTUNITÉS

Risques

Gestion du changement

Les projets de modernisation nécessitent une planification minutieuse, un accord sur les avantages mesurables et le ralliement des parties concernées. Les décideurs et les employés de l'ensemble de l'entreprise doivent comprendre les avantages ultimes de la modernisation afin de s'adapter aux changements requis. Si ce processus n'est pas géré avec soin, la modernisation sera retardée et les systèmes désuets auront une incidence sur la rentabilité à long terme.

Pénurie de personnel qualifié

Sans une équipe spécialisée qui comprend parfaitement les avantages des nouvelles technologies et qui est en mesure de les optimiser, des retards, une qualité compromise et des coûts supplémentaires liés au recrutement ou à la formation risquent de nuire à vos efforts de modernisation. Il est essentiel de disposer de l'expertise interne appropriée pour gérer les activités en cours tout en exploitant les avancées technologiques.

Négligence du soutien externe intégré

Surcharger votre équipe interne avec des responsabilités de base et la charge de travail supplémentaire liée à l'intégration/à la migration de nouvelles technologies peut retarder la transformation et mettre en péril la stabilité opérationnelle. La mobilisation de partenaires externes, tels que des services gérés et des plateformes infonuagiques, ne constitue pas un luxe, mais un investissement essentiel pour assurer une intégration harmonieuse et des progrès soutenus.

Opportunités

La modernisation comme catalyseur d'activités

La modernisation permet de soutenir et d'accélérer la mise en œuvre de la feuille de route stratégique de l'entreprise. Les entreprises peuvent utiliser la modernisation pour harmoniser leurs capacités technologiques avec des objectifs à long terme, favorisant ainsi l'innovation et la compétitivité. Par conséquent, elles peuvent optimiser et automatiser les processus, tout en répondant plus efficacement aux besoins du marché.

Accent sur la sécurité

La sécurité demeure l'un des principaux domaines d'investissement dans la modernisation ainsi qu'un facteur à prendre en compte lors de l'examen des technologies aux fins de modernisation. En portant attention à cette vulnérabilité critique, vous pouvez protéger votre entreprise contre les cybermenaces, qui sont de plus en plus nombreuses. Tous les projets de modernisation doivent faire l'objet d'une évaluation complète des risques et de la gouvernance.

Moderniser pour stimuler la compétitivité

La modernisation permet aux entreprises de se différencier en intégrant des technologies avancées et en réduisant potentiellement les coûts, ce qui leur procure un avantage concurrentiel. En améliorant les systèmes et les processus, l'entreprise peut réagir plus rapidement aux changements du marché et offrir une meilleure expérience à ses clients, tout en restant plus agile face à la concurrence.

LA GRANDE QUESTION

La modernisation est un processus continu visant à soutenir l'atteinte des objectifs et la croissance de l'entreprise. Avec des ressources limitées, où concentrerez-vous vos efforts de modernisation ? Quelle combinaison de ressources internes et externes utiliserez-vous pour mener à bien ces efforts ?

Les résultats détaillés du Portrait TI 2025 permettent d'examiner de manière approfondie la façon dont les entreprises abordent et gèrent les grandes avancées technologiques et leurs préoccupations principales. Quelques grandes tendances se dégagent :

- Les décideurs à l'intérieur et à l'extérieur des services TI divergent souvent dans leur perception des risques, des opportunités et des priorités technologiques. Il s'agit là d'une tendance inquiétante qui peut limiter l'efficacité de la prise de décisions.
- Les entreprises sont impatientes d'intégrer l'IA, mais il est possible qu'elles aillent de l'avant sans avoir une compréhension claire des usages, des risques et des avantages des outils disponibles.
- Les solutions à code source ouvert (open-source) et l'analyse de données avancée sont des domaines à croissance rapide dans lesquels les entreprises investissent pour se moderniser, innover et obtenir un avantage concurrentiel.
- Les entreprises canadiennes sont préoccupées par la cybersécurité, mais seulement une minorité d'entre elles adoptent les mesures nécessaires pour se protéger.
- De nombreux domaines se disputent l'attention et les ressources des équipes TI, qui sont limitées par le budget, le temps et les RH.
- Les grandes entreprises, celles du secteur financier et celles situées en Ontario sont systématiquement plus enclines à intégrer leurs équipes TI dans le processus décisionnel et à mobiliser leurs (souvent plus vastes) ressources pour réaliser des investissements majeurs en technologies, notamment en cybersécurité et en modernisation.

Au début du présent rapport, nous avons mis en lumière le thème de **l'équilibre**. Ce dernier constitue un mot d'ordre nécessaire pour les entreprises qui analysent ces données et cherchent à prendre des décisions efficaces en matière de TI.

Qu'il s'agisse d'évaluer l'ambition et les ressources, l'innovation et le risque, les ressources externes et internes, ou les technologies établies et émergentes, trouver le juste équilibre adapté à votre réalité d'affaire vous permettra de tirer pleinement parti des TI pour soutenir la réussite de votre organisation.

L'avenir des TI : cinq grandes tendances qui façonneront l'avenir

La technologie évolue à la vitesse de l'éclair et change notre façon de travailler, d'interagir et de faire des affaires. L'IA, l'infonuagique et la cybersécurité sont au cœur de cette évolution, mais les entreprises cherchent encore comment exploiter ces outils pour en tirer de réels bénéfices. Le Portrait TI 2025 fait ressortir les principales opportunités et les défis à venir, en lien avec cinq tendances qui redéfinissent les TI.

La dette technique freine les entreprises

De nombreuses entreprises se sont précipitées dans la transformation numérique, en intégrant de nouvelles technologies à des systèmes obsolètes. Aujourd'hui, elles en paient le prix. Alors que 81 % des entreprises canadiennes prévoient d'importants investissements technologiques au cours des deux prochaines années, seulement 25 % d'entre elles estiment que leur infrastructure informatique est réellement prête à suivre le rythme. À l'avenir, les entreprises devront se moderniser plus intelligemment, en adoptant des architectures infonuagiques hybrides capables de soutenir les charges de travail évolutives de l'IA, tout en réduisant la complexité et les coûts.

L'IA ne remplacera pas les emplois, mais les transformera

Près d'un tiers des entreprises estiment que l'automatisation pilotée par l'IA est déjà un facteur de différenciation majeur pour leur entreprise et leur secteur d'activité. Or, l'IA ne se limite pas à l'automatisation des tâches : elle est appelée à modifier les méthodes de travail. Alors que 78 % des services TI sont confrontés à au moins un enjeu en matière de RH, il est essentiel que les entreprises investissent dans la requalification des travailleurs afin qu'ils puissent collaborer avec l'IA. L'essor de l'IA agentique, une forme d'IA qui agit de manière autonome, accélérera ce changement, faisant de l'IA non plus un simple outil, mais un décideur actif.

En outre, la cybersécurité joue un rôle de plus en plus important dans ce domaine. Alors que l'IA s'intègre de plus en plus aux flux de travail, la protection des systèmes automatisés et des données des employés devient essentielle. Il ne s'agit plus seulement de savoir qui fait le travail, mais à quel point ce travail est sécurisé.

La souveraineté des données est plus importante que jamais

L'emplacement où les entreprises stockent leurs données et la manière dont elles le font deviennent une décision stratégique, et non plus de simples enjeux de conformité. Alors que 83 % des dirigeants se disent confiants dans la capacité de leur entreprise à rester en conformité avec l'évolution de la réglementation en matière de protection des données, seulement 22 % des entreprises canadiennes sont en parfaite conformité avec des lois comme la loi 25 du Québec.

C'est là que l'infonuagique et la cybersécurité se rencontrent. Les organisations ont besoin d'environnements hybrides et multicloud qui leur permettent de respecter les règles locales sur la résidence des données, sans sacrifier le rendement et la flexibilité. Elles doivent également s'assurer que les données sont sécurisées, non seulement lorsqu'elles sont stockées, mais tout au long du cycle de vie de l'IA.

Les budgets consacrés à l'IA passent de l'expérimentation au retour sur investissement

Pendant des années, les entreprises ont considéré l'IA comme un terrain d'expérimentation - utile, mais pas nécessairement rentable. Cette perception évolue rapidement. La prochaine vague d'adoption misera sur l'IA autofinancée : des modèles propulsés par l'infonuagique qui génèreront de nouvelles sources de revenus, des analyses prédictives et une valeur client à grande échelle.

Mais tout cela repose sur la confiance. Les entreprises doivent associer l'IA à des cadres de sécurité robustes qui protègent à la fois les données et les résultats que l'IA contribue à générer.

Les modèles d'affaires doivent rattraper l'IA

Les produits et services alimentés par l'IA sont arrivés, mais de nombreuses entreprises sont encore figées dans d'anciennes façons de penser. Celles qui réussiront seront celles qui adopteront pleinement :

- **La personnalisation pilotée par l'IA :** adapter les services en temps réel
- **Les partenariats d'écosystème** : collaborer avec d'autres acteurs pour élargir la portée de l'IA
- **Une approche centrée sur l'IA pour l'engagement client :** interagir de manière intuitive plutôt qu'automatisée

En résumé

Le Portrait TI 2025 est clair : l'IA, l'infonuagique hybride et la sécurité ne relèvent plus seulement du service informatique. Ce sont désormais des enjeux stratégiques au cœur des décisions d'affaires.

Les véritables gagnants ne seront pas ceux qui adoptent simplement les dernières technologies, mais ceux qui repensent leur stratégie, revoient leur gestion des talents, et réinventent leur modèle d'affaires pour prospérer dans un monde axé sur l'IA.

C'est le moment de diriger avec détermination et de construire l'avenir.

Leanne Clarke
Directrice des ventes de l'écosystème,
IBM Canada

Une étude menée par :

GROUPE NOVIPRO

Leger

En collaboration avec :

NOVIPRO

BLAIR TECHNOLOGY SOLUTIONS

Avec le support de nos partenaires :

PARTENAIRE PLATINE

IBM

OR

OVHcloud

ARGENT

HCLSoftware

BRONZE

DATA SENTINEL

infor

OCCASIONEL

elastic

NUTANIX