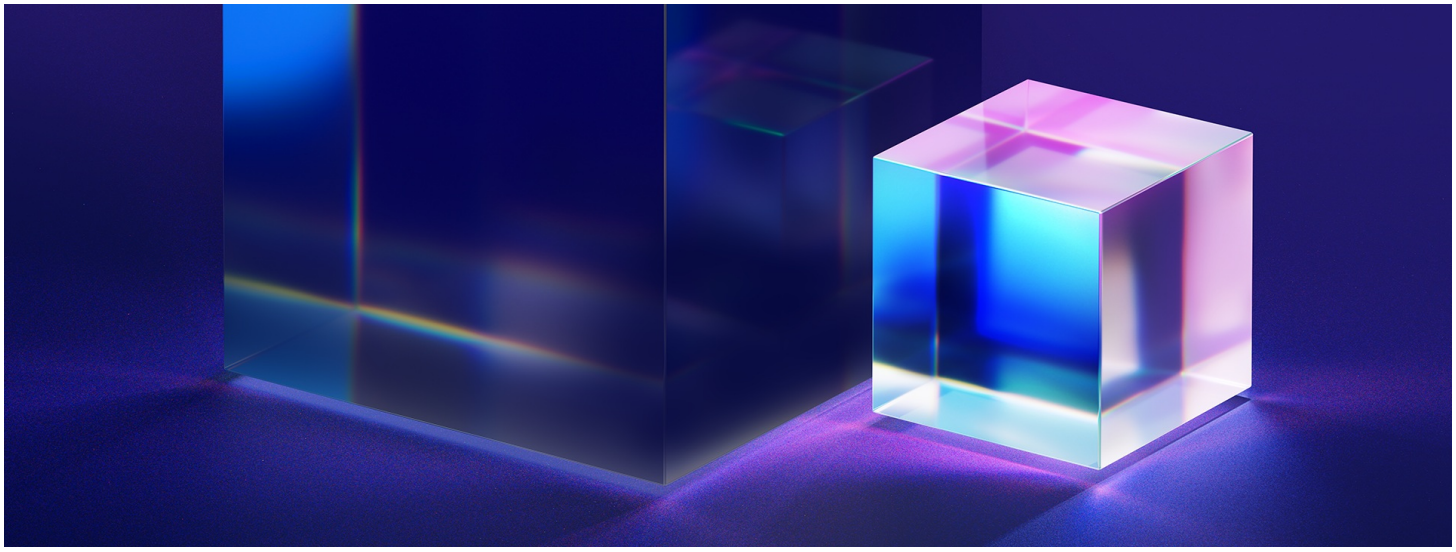
IBM Canada Newsroom

Rapport IBM : La sécurité des données des Canadiens est de plus en plus menacée, alors que les coûts des violations explosent



L'IA peut aider les entreprises à économiser des millions et à protéger les données des consommateurs

- Les entreprises canadiennes perdent en moyenne **6,98** millions **CA$** en raison de violations de données, avec des répercussions directes sur les consommateurs.
- L'IA fantôme augmente les risques, ajoutant **308 000 CA$ aux coûts moyens par violation** pour les entreprises canadiennes et augmentant la probabilité d'exposition de données sensibles.
- L'adoption de **l'IA de sécurité et de l'automatisation a considérablement réduit les coûts liés aux violations, qui** sont passés à 5,19 millions CA$ contre 8,53 millions CA$ pour les organisations qui n'utilisent pas ces technologies.

MARKHAM, ON, le 30 juill. 2025 /CNW/ - Les violations de données au Canada deviennent de plus en plus coûteuses et complexes. Selon le dernier rapport **IBM sur le coût des violations de données,** les organisations ont déboursé en moyenne **6,98** millions **CA$** par violation en 2025. Cela représente une **augmentation de 10.4 %** par rapport aux 6,32 millions CA$ de 2024, reflétant l'impact financier croissant des incidents de sécurité. Parmi les conclusions du rapport figure l'essor de l'IA non autorisée – connue sous le nom **d'IA fantôme** – qui amplifie les risques, fait grimper les coûts et expose les données sensibles des consommateurs. Souvent introduite par des employés utilisant des systèmes d'IA non approuvés, l'IA fantôme crée des vulnérabilités et des problèmes de conformité pour les entreprises.

Le rapport souligne le rôle essentiel de **l'IA de sécurité et de l'automatisation** dans la réduction des coûts de violation et l'amélioration de l'efficacité de la détection. Les organisations qui en font un usage intensif signalent des coûts de violation moyens de **5,19 millions CA$**, comparativement à **8,53 millions CA$** pour celles qui ne s'en servent pas. De plus, ces technologies ont aidé les organisations à accélérer la détection et le confinement, réduisant de **59 jours la durée moyenne des incidents pour les entreprises les utilisant de manière intensive**.

« La cybersécurité ne se limite pas à la protection des données : elle vise également à protéger la rentabilité et la réputation de votre entreprise », a déclaré Daina Proctor, chef de la prestation de services de sécurité chez IBM Canada. « Ce rapport montre que les organisations qui misent sur l'IA et l'automatisation économisent des millions et détectent les brèches beaucoup plus rapidement, mais les lacunes dans la sécurité et la gouvernance de l'IA, comme l'utilisation de l'IA fantôme, exposent les entreprises à des risques inutiles. En investissant dans des outils d'IA et en élaborant des politiques d'IA claires, les entreprises peuvent prendre le contrôle de leur sécurité et anticiper les menaces émergentes. »

Principales conclusions au Canada pour 2025

- **IA surexposée** : Une entreprise canadienne sur trois a déclaré ne pas disposer de contrôles d'accès aux systèmes d'IA, les positionnant ainsi comme des cibles faciles et de grande valeur.
- **Risques liés à l'IA fantôme :** L'utilisation de l'IA fantôme s'est également avérée être l'un des principaux facteurs de coût des violations pour les entreprises canadienne, augmentant les coûts de **308 000 CA$**.
- **Escroqueries par hameçonnage :** Le vecteur d'attaque initial le plus courant, l'escroquerie par hameçonnage, coûte aux organisations canadiennes en moyenne **7,91 millions CA$ par violation**, soit une **augmentation de 24 %** par rapport à 6,38 millions CA$ en 2024.
- **Impacts sur l'industrie :**
  - Le secteur financier est en tête des coûts de violation avec **9,97 millions CA$ en 2025**, soit une **augmentation de 7,4 %** par rapport à 9,28 millions CA$ en 2024, ce qui reflète la grande sensibilité et la valeur des données financières.
  - Les violations de la sécurité pharmaceutique coûtent **7,99 millions** CA$. Les incidents dans ce secteur ont le potentiel d'exposer la propriété intellectuelle et de retarder les traitements en raison de leur impact sur l'approvisionnement.
  - Les violations dans les secteurs industriels coûtent en moyenne **8,39 millions CA$**, car ces organisations ont une faible tolérance aux temps d'arrêt, ce qui en fait des cibles faciles pour les attaquants.

Comment l'IA transforme les opérations de cybersécurité

Le rapport souligne que les organisations **qui adoptent l'IA et l'automatisation** dans leur Centre d'opérations de sécurité (SOC) bénéficient d'avantages financiers importants. Les outils d'IA automatisent les tâches manuelles en cybersécurité, notamment la détection et la réponse aux menaces, permettant aux équipes de sécurité de se concentrer sur des priorités stratégiques.

L'automatisation de la sécurité permet d'accélérer les temps de réponse et de réduire l'impact des violations. Les organisations utilisant largement ces outils ont signalé une identification plus rapide des violations, avec un **temps moyen d'identification (MTTI)** réduit à **118 jours**, contre **162 jours** pour celles qui n'en font pas usage.

Ce que cela signifie pour les Canadiens

Les violations de données ne sont pas seulement un problème d'entreprise : elles touchent tout le monde. Lorsque des organisations perdent des millions à cause de cyberattaques, cela a des répercussions sur les Canadiens comme suit :

- **Coûts plus élevés des biens et services :** les coûts des violations sont souvent refilés aux consommateurs, par l'augmentation des prix des biens ou services.
- **Données personnelles volées :** les violations exposent fréquemment des renseignements personnels, notamment des coordonnées bancaires, des dossiers médicaux, etc.
- **Interruptions de service :** les violations peuvent entraîner des retards dans les expéditions, des rendez-vous annulés et des interruptions dans les services essentiels.

Recommandations pour les entreprises canadiennes

- **Gouverner et sécuriser les systèmes d'IA :** élaborer des politiques pour gérer l'utilisation de l'IA, prévenir l'IA fantôme et assurer le respect des lois sur la confidentialité.
- **Investir dans l'automatisation de la sécurité :** utiliser des outils d'IA pour détecter et contenir les violations plus rapidement.
- **Connecter la sécurité et la gouvernance IA :** investir dans des logiciels de sécurité et de gouvernance intégrés peut aider les organisations à découvrir et à gouverner automatiquement l'IA fantôme.
- **Renforcer la formation des employés :** renforcer les programmes de sensibilisation à la sécurité afin de minimiser les erreurs humaines.

Sources supplémentaires :

- Téléchargez une copie du rapport 2025 sur le coût des violations de données pour en savoir plus.
- Inscrivez-vous au webinaire IBM sur le coût des violations de données en 2025 le mercredi 13 août 2025 à 11 h HE.
- Consultez le blogue IBM pour en savoir plus sur les principales conclusions du rapport.

Contact média

Lorraine Baldwin
Communications IBM Canada
lorraine@ca.ibm.com

À l'intention des médias : B-Roll
