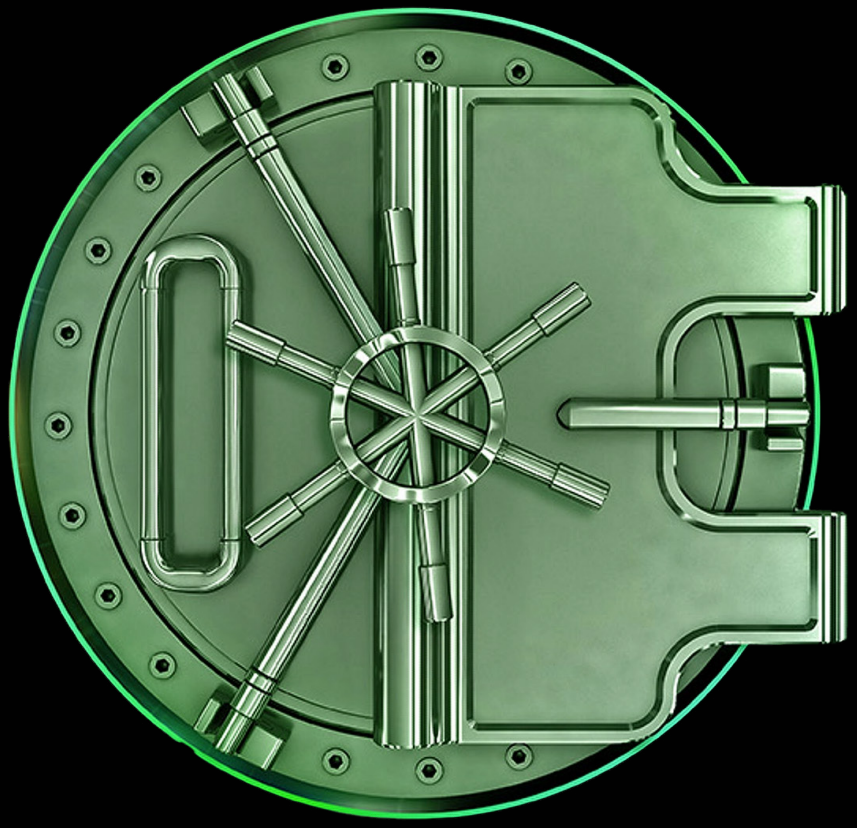
Deloitte.

CANADIAN INSIDER RISK MANAGEMENT CENTRE OF EXCELLENCE
CENTRE D'EXCELLENCE CANADIEN POUR LA GESTION DES RISQUES INTERNES



La gestion des risques internes au Canada

Résultats du sondage intersectoriel 2024-25 de Deloitte et du Centre d'excellence canadien pour la gestion des risques internes

Septembre 2025

À propos de ce rapport

Ce rapport présente en détail les résultats du premier sondage sur la gestion des risques internes mené par Deloitte Canada et le Centre d'excellence canadien pour la gestion des risques internes (CInRM CoE). Dans le cadre de ce sondage, des données ont été collectées auprès de professionnels canadiens en gestion des risques internes, portant sur leur perception des menaces internes ainsi que sur les mesures de contrôle mises en place au sein de leur organisation.

Les données de ce rapport sont fondées sur une enquête menée entre septembre 2024 et avril 2025. Le sondage a été complété par des cadres dirigeants issus des secteurs de la sécurité, de la lutte contre la fraude, de la cybersécurité, des technologies de l'information et des ressources humaines. Les répondants provenaient d’un échantillon représentatif d’industries canadiennes, incluant des filiales de sociétés étrangères, des organisations du secteur public, des organismes sans but lucratif ainsi que d’autres entreprises privées.

Les données présentées dans ce rapport sont enrichies par des entrevues menées auprès de dirigeants à travers le Canada, ainsi que par les perspectives d’experts de Deloitte, dont l’expertise s’étend tant au niveau national qu’international. Les citations incluses dans ce rapport ont été modifiées pour plus de lisibilité.

Sauf indication contraire, toutes les données numériques se réfèrent aux résultats des réponses à l'enquête. Ces résultats sont anonymes, et seules les réponses agrégées sont rapportées.

Merci à tous les participants au sondage pour votre soutien dans cet effort.

Avant-propos

Pierre Luc Pomerleau, Ph.D.
Associé
Deloitte Canada

Victor Munro
Directeur principal
Deloitte Canada
Directeur exécutif
Centre d'excellence canadien pour la gestion des risques internes

Dans un contexte où les environnements de risque deviennent de plus en plus complexes, les menaces internes demeurent l'un des enjeux les plus difficiles à maîtriser parmi l'ensemble des risques auxquels les entreprises sont confrontées. Cette publication, la première du genre au Canada et inspirée de l'initiative menée par Deloitte Australie, est le résultat d'une collaboration entre Deloitte Canada et le Centre d'excellence canadien pour la gestion des risques internes. Elle propose une perspective canadienne unique sur la manière dont les organisations, tous secteurs confondus, perçoivent et abordent ce défi.

Fondé sur les réponses à un sondage mené auprès de professionnels chevronnés des domaines de la sécurité, de la cybersécurité, des TI, de la fraude et des ressources humaines, ce rapport met en lumière l'évolution des risques internes, la façon dont les organisations canadiennes réagissent et les lacunes qui subsistent en matière de stratégie, de contrôles et de sensibilisation. Enrichi d'entretiens et de points de vue d'experts, le rapport examine également des approches concrètes et des considérations pratiques qui dépassent le cadre théorique.

Les données sont sans équivoque : la gestion des risques internes n'est plus un enjeu périphérique — elle est désormais essentielle pour préserver la résilience, la confiance et l'intégrité des organisations. Pourtant, malgré une prise de conscience croissante, nombreuses sont les organisations qui peinent encore à mesurer les progrès réalisés ou à justifier les investissements requis. Cette difficulté s'explique en grande partie par le caractère intangible des efforts de prévention et de réponse, par la complexité à confirmer des menaces internes passées, ainsi que par l'analyse prospective à long terme qu'exige la mise en place d'un programme robuste et efficace.

À mesure que le paysage réglementaire canadien évolue, guidé par les directives de Sécurité publique Canada, du Centre canadien pour la cybersécurité et du Bureau du surintendant des institutions financières, les organisations doivent passer de mesures réactives à des stratégies proactives à l'échelle de l'organisation. Ce rapport sert non seulement de référence pour la maturité de l'industrie, mais aussi de feuille de route canadienne pour renforcer une posture proactive, favoriser la collaboration interfonctionnelle et intégrer la gestion des risques internes comme discipline organisationnelle de base.

Nous espérons que cette édition inaugurale stimulera un dialogue critique à tous les niveaux de l'entreprise, y compris la haute direction, et qu'elle soutiendra les organisations dans l'élaboration des programmes nécessaires pour faire face aux risques internes d'aujourd'hui et de demain.

Au cours des 22 dernières années, j'ai travaillé à l'intersection de la sécurité nationale, de la sécurité publique et du risque d'entreprise, d'abord en tant que fonctionnaire fédéral canadien pendant 18 ans, et plus récemment en tant que conseiller principal dans le secteur privé. Au cours des sept dernières années, ma recherche doctorale s'est concentrée sur la surveillance et la détection des menaces internes, ce qui m'a permis d'observer de première main l'évolution des capacités et des mentalités organisationnelles à travers les secteurs et les domaines.

L'une des leçons les plus claires de ce parcours est que les menaces internes transcendent les frontières. Ils ne peuvent pas être pris en charge par un seul secteur d'activité, qu'il s'agisse de la sécurité, de la cybersécurité, de la fraude ou de la conformité. La gestion du risque interne nécessite une approche holistique et intégrée, qui inscrit la confiance, la responsabilisation et la transparence au cœur même du fonctionnement quotidien de l'organisation.

Ce rapport, qui s'appuie sur les points de vue de praticiens de partout au Canada, met en lumière le chemin que nous avons parcouru en tant qu'industrie et le chemin qu'il nous reste à parcourir. Les programmes les plus matures que nous avons observés dans notre enquête partageaient plusieurs caractéristiques clés :

- Une coordination interfonctionnelle robuste,
- Un engagement à accélérer l'élaboration et la mise en œuvre de politiques,
- Une surveillance continue à l'aide de l'analyse du comportement des utilisateurs et des entités (UEBA), et
- Une compréhension de la façon dont la culture organisationnelle et le comportement des employés façonnent à la fois les risques et les opportunités.

Nous avons également constaté que de nombreuses organisations canadiennes se trouvent maintenant à un point d'inflexion et qu'elles sont sur le point de faire passer la gestion des risques internes d'une activité cloisonnée à une priorité à l'échelle de l'entreprise. Ce rapport fournit un outil essentiel pour aider à faire avancer ces conversations avec la haute direction. Qu'il s'agisse de lancer un programme dédié ou de chercher à faire évoluer un programme existant, les informations fournies ici peuvent aider à combler le fossé entre la sensibilisation et l'action.

Il s'agit d'une période charnière pour la gestion des risques internes au Canada. Je suis fier de présenter ce rapport à la fois comme une référence nationale et un guide pratique pour les dirigeants qui s'engagent à bâtir des organisations plus résilientes.

Contenu

Résumé

Ce sondage intersectoriel 2024-25 révèle que même si les organisations canadiennes démontrent généralement une compréhension modérée du risque interne, celui-ci reste sous-estimé par rapport aux autres menaces d'entreprise. Malgré une reconnaissance croissante, la plupart des programmes de gestion des risques internes ne bénéficient pas d'un soutien suffisant de la part de la direction pour mener des actions proactives à l'échelle de l'entreprise. La visibilité continue des menaces internes a été soutenue par les nouvelles directives réglementaires, l'adoption des meilleures pratiques du secteur et les incidents très médiatisés dans tous les secteurs.

Le sondage anonyme mené par Deloitte auprès de praticiens canadiens offre un éclairage précieux sur la manière dont les organisations abordent la gestion des risques internes. Quatre enseignements clés s'en dégagent.

1

Les organisations canadiennes doivent renforcer la coordination interfonctionnelle

Il est nécessaire de renforcer la gouvernance interne de la gestion des risques en créant des groupes de travail dédiés et des comités transversaux impliquant les ressources humaines, la technologie de l'information (TI), l'éthique et la conformité, la sécurité, les services juridiques, les opérations commerciales et la finance.

2

L'élaboration et la mise en œuvre des politiques doivent être accélérées

Les politiques de gestion des risques internes doivent être élaborées et mises en œuvre plus rapidement. Des directives claires sur la façon de détecter, de traiter et de répondre aux menaces internes sont nécessaires pour renforcer l'engagement dans l'ensemble de l'organisation.

3

Assurer une surveillance continue et intégrer des outils tels que l'UEBA

L'absence de surveillance continue après l'embauche, avec peu de vérification continue de routine des employés, expose les organisations à des risques non détectés. Il est crucial d'intégrer des outils tels que l'analyse comportementale des utilisateurs et des entités (UEBA) pour identifier les comportements à risque tout au long du cycle de vie des employés.

4

Ne pas négliger les comportements en dehors des systèmes numériques

Les menaces internes résultent souvent de facteurs psychologiques et comportementaux complexes qui ne se manifestent pas uniquement sur les plateformes virtuelles. L'analyse des comportements non numériques, tels que les interactions en personne et les changements d'habitudes des employés, doit également être une priorité dans la gestion holistique des risques internes.

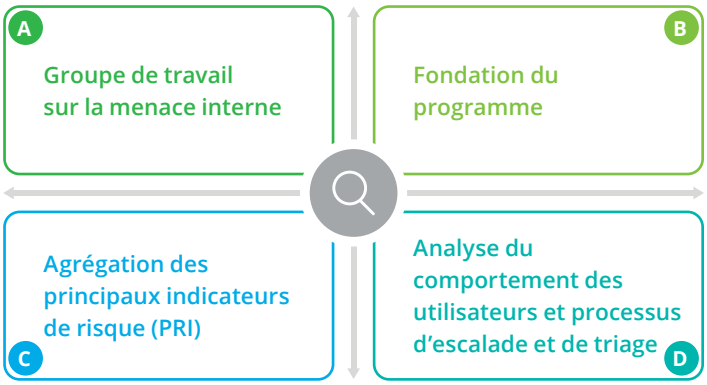
Introduction

Le paysage des menaces internes au Canada évolue rapidement. Alors que les entreprises des secteurs public et privé naviguent dans un environnement de risque accru marqué par la transformation numérique, le travail hybride et l'expansion des écosystèmes de données, la menace interne, qu'elle soit malveillante ou non, est devenue de plus en plus difficile à détecter et à atténuer. Alors que les programmes de sécurité traditionnels se sont concentrés sur les adversaires externes, les institutions commencent maintenant à reconnaître que les menaces internes, avec leur accès autorisé et leur connaissance contextuelle, présentent un risque plus complexe et persistant. Ce changement exige non seulement de nouvelles technologies, mais aussi de nouvelles façons de penser la confiance, la surveillance et la responsabilité organisationnelle.

Le Canada n'est pas étranger aux conséquences des menaces internes. Au cours des quinze dernières années, plusieurs violations très médiatisées, allant de la divulgation non autorisée d'informations gouvernementales sensibles à des employés de confiance exploitant l'accès au système à des fins personnelles ou criminelles, ont mis en évidence le besoin urgent de résilience. Ces événements nous rappellent brutalement que le risque interne n'est pas théorique ; Il est réel et a de profondes implications opérationnelles, réputationnelles et juridiques. À mesure que les menaces deviennent plus sophistiquées et que le coût de l'inaction augmente, les organisations canadiennes doivent prendre des mesures délibérées pour élaborer des programmes de gestion des risques internes matures fondés sur la collaboration interfonctionnelle, la sensibilisation culturelle et l'adaptation continue.

Enquête 2024-25 de Deloitte sur la gestion des risques internes

L'objectif de cette étude était d'évaluer l'état actuel des pratiques de gestion des risques internes dans les organisations canadiennes. L'équipe de recherche a réalisé une étude de réplication d'une enquête conduite par Deloitte Australie en 2023. Les participants ont été invités à répondre à 34 questions, pouvant être synthétisées en 10 questions clés, portant sur quatre domaines de contrôle, alignés avec le cadre suivant :



La menace interne fait référence à l'exploitation involontaire ou malveillante d'un accès privilégié à des actifs sensibles et essentiels à la mission d'une organisation, y compris à son personnel, entraînant des conséquences négatives.

À propos des organisations participantes

32

Organisations privées et publiques participantes

- **39 %** des organisations comptaient moins de 10 000 employés
- **26 %** des organisations comptaient moins de 1 000 employés

7

Industries représentées

- Aérospatiale et défense, Énergie et services publics, Gestion des installations, Services financiers, Agroalimentaire, Administration publique, Secteur manufacturier

Qualitatif et Quantitatif

Informations capturées

- Les citations incluses dans ce rapport sont présentées de manière anonyme et ont été modifiées pour plus de lisibilité
- Sauf indication contraire, toutes les données numériques se réfèrent aux résultats des réponses à l'enquête

Les participants à l'enquête ont été invités à estimer le nombre total de menaces internes subies par leur organisation au cours des 12 derniers mois.

Commençons par une statistique frappante : 73 % des organisations participantes ont connu au moins un incident de menace interne au cours de l'année écoulée. Ce chiffre met en lumière la portée bien réelle et omniprésente de ce risque, tant pour les entreprises du secteur privé que pour les organisations publiques au Canada.

Les organisations canadiennes évaluent leur niveau de sensibilisation aux menaces internes, la priorité accordée à ces risques et le soutien de la direction qu'elles reçoivent pour y faire face à une moyenne de 3,1 sur 5. Bien que le score reflète un certain degré de reconnaissance des menaces internes, il montre également qu'il reste encore du travail à faire pour intégrer pleinement ces enjeux dans la stratégie globale des organisations.

73%

Des participants ont subi un incident de menace interne au cours des 12 mois

3.1/5

Évaluation globale de la sensibilisation et de la compréhension

3.1/5

Évaluation de la priorité accordée aux menaces internes

3.1/5

Évaluation du soutien de la direction à la menace interne

Définition et suivi des menaces internes : types et résultats

Les organisations se doivent d'instaurer un suivi rigoureux des trois principales catégories de menaces internes (accidentelles, négligentes et malveillantes), chacune constituant une voie distincte susceptible d'engendrer des dommages graves, souvent assortis de conséquences qui se recoupent. Les actes accidentels ou négligents, tels que l'envoi de courriels à de mauvais destinataires ou le non-respect des protocoles de sécurité, peuvent entraîner des conséquences graves comme l'exfiltration de données ou l'interruption des opérations, même si leurs motivations diffèrent de celles généralement associées aux menaces internes malveillantes.

En l'absence d'une surveillance et d'une analyse systématiques, ces activités passent souvent inaperçues jusqu'à ce que les dommages soient irréversibles. Le suivi complet permet aux organisations d'identifier rapidement les indicateurs comportementaux et techniques, de corréler les incidents entre les unités commerciales et de mesurer les tendances au fil du temps, ce qui permet des interventions ciblées, renforce les contrôles et réduit le risque d'impacts en cascade qui pourraient miner à la fois la sécurité et la confiance.

Types

Accidentelle

Actions non intentionnelles d'un employé qui entraînent un préjudice ou un risque accru pour l'organisation, souvent en raison d'une erreur humaine, d'un manque de sensibilisation ou d'une erreur de jugement. Par exemple, l'envoi d'informations sensibles au mauvais destinataire ou la mauvaise configuration d'un système sans se rendre compte des implications en matière de sécurité.

Négligente

Le défaut d'un employé de suivre les politiques, les procédures ou les protocoles de sécurité établis, même s'il possède les connaissances ou la formation nécessaires pour le faire. Les actes de négligence sont évitables et découlent de l'indifférence, de l'imprudence ou de l'absence de diligence raisonnable, comme le non-respect des mises à jour de sécurité obligatoires ou le contournement des contrôles d'accès.

Malveillante

Actions intentionnelles d'un employé visant à causer un préjudice ou à obtenir un gain personnel, animées par des raisons telles que le gain financier, la vengeance, l'idéologie, la coercition ou la loyauté envers une entité extérieure. Cette catégorie comprend des activités telles que le vol de données, la fraude, le sabotage, la violence au travail ou la facilitation de l'ingérence étrangère.

Question : Votre organisation suit-elle les incidents liés aux menaces internes en fonction de l'intention sous-jacente ?	1-10	11-20	31+
Accidentelle	53%	0%	6%
Négligente	47%	6%	18%
Malveillante	29%	6%	6%

**Les pourcentages ne sont pas égaux à 100 et ne représentent que les incidents signalés par les organisations.*

Une observation notable concerne la nature des incidents signalés : les menaces internes liées à la négligence surpassent en fréquence celles résultant d'erreurs accidentelles ou d'actes malveillants. Cette tendance, qui n'est pas systématiquement rapportée dans les études du secteur, suggère que la négligence constitue une catégorie de menace interne potentiellement plus répandue que les menaces accidentelles.

Différents types de menaces internes peuvent entraîner les **résultats** suivants :

Exfiltration de données

Vol ou compromission de données sensibles développées/soutenues par une organisation (par exemple, propriété intellectuelle, données sur les marchés financiers, informations personnelles identifiables)

Fraude

Exploitation de la position ou de l'accès aux données pour induire délibérément en erreur l'organisation dans le but d'obtenir un gain personnel (par exemple, détournement de fonds, fraude dans les achats).

Sabotage

Actions mettant en péril les infrastructures critiques, incluant le sabotage d'actifs tels que l'introduction de logiciels malveillants, la manipulation de bases de données ou de sauvegardes, ainsi que la destruction physique.

Violence au travail

Actes d'intimidation, de harcèlement ou de violence, ou menace de tels actes, contre des employés par un collègue.

Ingérence étrangère

Collusion avec des États-nations étrangers visant à compromettre la sécurité nationale ou la souveraineté, notamment par le vol d'informations classifiées ou la promotion de technologies émergentes au profit de fournisseurs étrangers.

Extrémisme violent à motivation idéologique (EVCI)

L'EVCI peut découler de diverses sources, telles que l'extrémisme politique, la radicalisation religieuse ou des revendications sociales, et implique souvent des individus, groupes ou institutions perçus comme opposés à la vision du monde de l'extrémiste.

Une approche globale qui suit les activités de menaces internes tout au long du spectre, de l'accidentel à la négligence en passant par la malveillance, est essentielle pour plusieurs raisons.

En surveillant et en classifiant les incidents à travers l'ensemble du spectre, les organisations sont en mesure de détecter des tendances avant qu'elles ne s'aggravent. De nombreux comportements malveillants prennent racine dans des violations répétées aux règles ou des erreurs récurrentes. Identifier précocement ces signaux, tels que des antécédents de gestion négligente des données, permet de mettre en place des mesures correctives appropriées, comme des formations ciblées, un renforcement de la supervision ou des limitations d'accès, réduisant ainsi le risque d'une évolution vers des actes intentionnels préjudiciables..

Le suivi de toutes les catégories fournit une vue complète du profil de risque humain de l'organisation. Se concentrer uniquement sur les actes malveillants ne tient pas compte de l'impact significatif des incidents accidentels et négligents, qui causent souvent autant de dommages opérationnels et de réputation. Une approche basée sur le spectre garantit que la direction comprend l'interconnexion de l'erreur humaine, de la négligence et de l'inconduite intentionnelle.

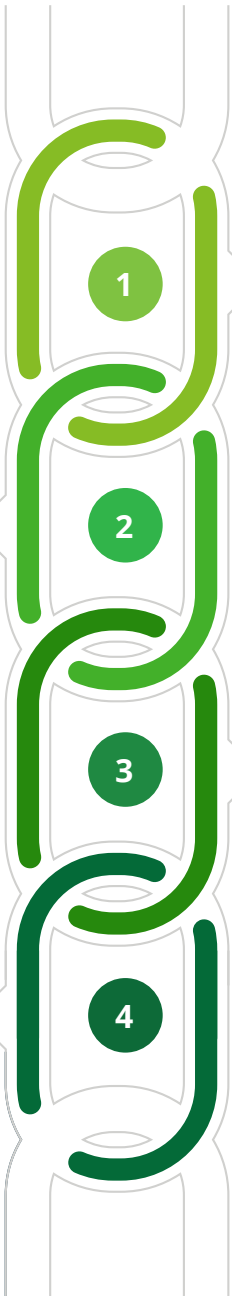
Enfin, différents types de menaces nécessitent des réponses différentes. La gestion efficace des incidents accidentels repose sur des campagnes de sensibilisation et l'optimisation des processus. Pour réduire la négligence, il convient de mettre en place des mécanismes de responsabilisation et de renforcer les contrôles. Quant aux comportements malveillants, ils nécessitent des enquêtes approfondies et des mesures disciplinaires appropriées. Une approche structurée de suivi permet ainsi à l'organisation d'adapter précisément les contre-mesures à chaque type de risque interne.

En comprenant l'éventail des risques internes, les organisations peuvent intégrer des contrôles culturels, procéduraux et techniques qui protègent à la fois les actifs et les personnes. Cette approche à plusieurs niveaux réduit non seulement la vulnérabilité aux menaces internes, mais renforce également la confiance entre les employés et la direction, en créant une culture consciente de la sécurité qui dissuade naturellement les comportements nuisibles.

Avez-vous constaté ce qui suit :	Oui	Non/refus de répondre	Inconnu
Vol d'informations personnelles (exfiltration de données)	76%	6%	18%
Vol de propriété intellectuelle	59%	18%	23%
Fraude	53%	35%	12%
Sabotage	35%	47%	18%
Violence au travail	35%	41%	24%
Ingérence étrangère	24%	47%	29%
Extrémisme violent à motivation idéologique	12%	65%	24%

Les résultats montrent tout de même la grande variété de menaces internes auxquelles les organisations sont confrontées, allant du vol de données à des problèmes beaucoup plus sérieux liés à la sécurité nationale et même à la radicalisation. Au total, 76 % des organisations ont signalé au moins un incident lié au vol de renseignements personnels, tandis que 59 % des organisations ont signalé un incident lié au vol de propriété intellectuelle. Ces cas d'exfiltration de données impliquent fréquemment un accès non autorisé à des informations sensibles concernant des clients ou des employés, ainsi que le vol de designs exclusifs, de secrets commerciaux ou de travaux de recherche. La fréquence et l'impact de ces incidents soulignent le besoin crucial de contrôles d'accès robustes, de surveillance continue et de programmes de sensibilisation des employés pour protéger les actifs personnels et de l'entreprise contre les menaces internes.

Il est vivement recommandé aux organisations de s'accorder sur une définition commune des menaces internes. Cela permet aux responsables des programmes de sécurité de mieux communiquer l'ampleur des risques à la direction, facilitant ainsi l'allocation de ressources et les investissements nécessaires à leur gestion. Une telle définition partagée constitue le fondement pour renforcer les capacités organisationnelles de détection et de réponse aux menaces internes.



UNE GOUVERNANCE ET DES PROCESSUS COMPLETS DE GESTION DES RISQUES AU NIVEAU DE L'ENTREPRISE

Gouvernance de toutes les lignes de défense de l'entreprise, établissant une « plaque tournante » opérationnelle pour les risques internes

COLLECTE CENTRALISÉE DES DONNÉES, ANALYSE PLURIDISCIPLINAIRE

Recherche comportementale, gestion du changement, cybersécurité, science des données, gestion des risques

CAS D'USAGE BASÉS SUR DES COMPROMISSIONS PASSÉES ET DES CADRES DE RÉFÉRENCE SECTORIELS

Identifier les principaux indicateurs de risque (PRI) pour l'organisation, prendre en compte les modèles de l'industrie (par exemple, MITRE Enterprise Attack)

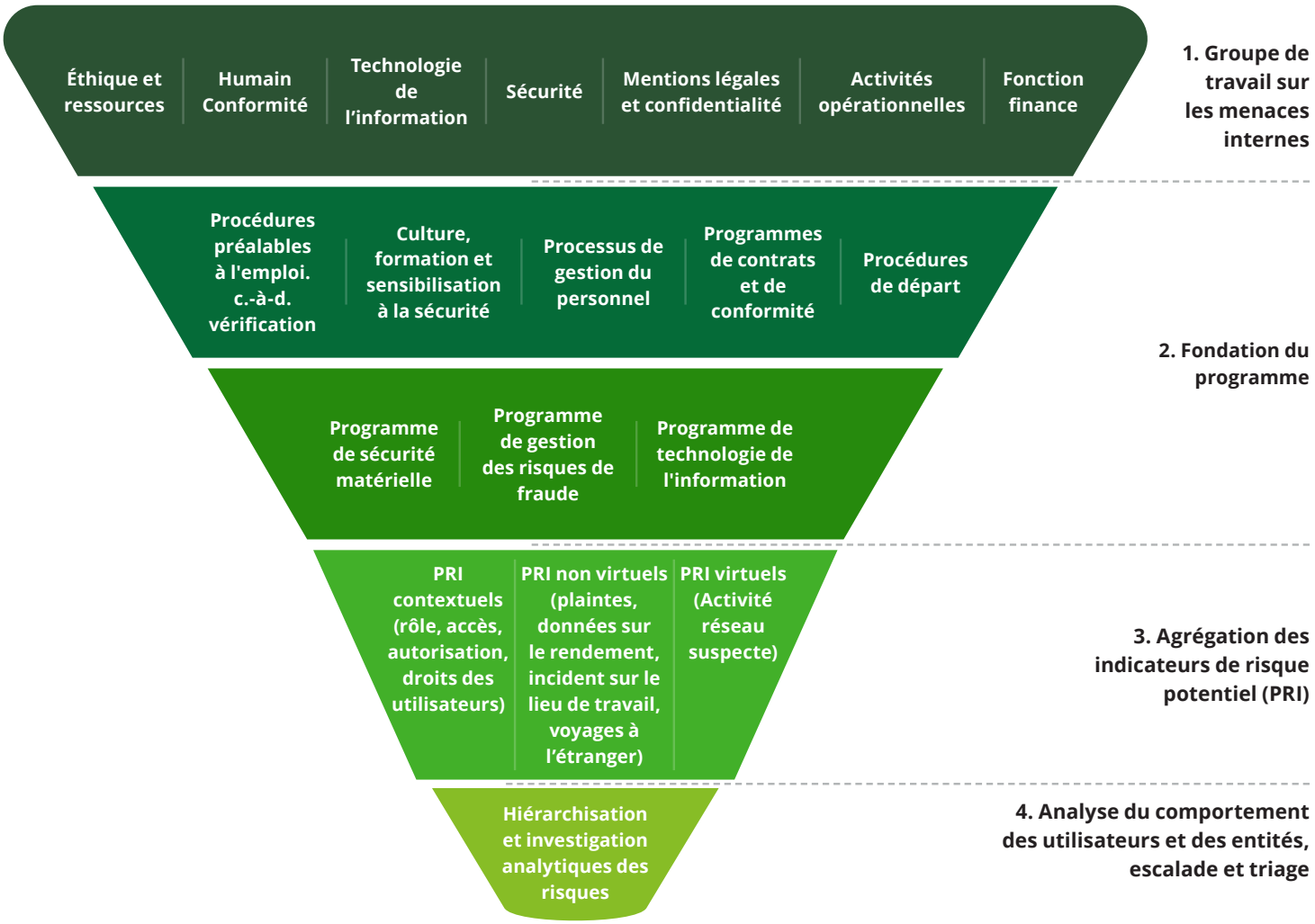
SENSIBILISATION ET FORMATION CONTINUES

Communiquer avec l'ensemble du personnel, renforcer les compétences techniques des praticiens de la sécurité et promouvoir les meilleures pratiques, les politiques et les enseignements tirés en cas de menace interne

Atténuer les menaces internes

L'atténuation des menaces internes, axée sur les personnes et leurs comportements, requiert une approche globale. Au quotidien, les collaborateurs interagissent avec l'organisation de multiples façons, physiquement et virtuellement, individuellement et en équipe. Il est donc essentiel de mettre en place des contrôles couvrant l'ensemble des environnements de travail et tout au long du cycle de vie des employés.

Le cadre ci-dessous présente les composantes fonctionnelles nécessaires à l'élaboration d'un programme de gestion des risques internes efficace, holistique et axé sur le risque. Cette structure englobe le cadre de gouvernance et de surveillance ainsi que les phases d'identification, de protection, de détection, d'intervention et de rétablissement. Elle s'appuie sur les capacités existantes tout en favorisant la coordination entre les différentes parties prenantes. Cette approche va au-delà de l'accent traditionnel mis sur la technologie et adopte une approche qui inclut les processus opérationnels, les politiques, la technologie et la formation.



Les quatre éléments clés d'un cadre de gestion des risques internes

1

Groupe de travail sur les menaces internes

Des parties prenantes interfonctionnelles, partageant une compréhension commune des menaces internes, définissent la culture du risque et pilotent l'orientation stratégique des programmes de gestion des menaces internes.

2

Fondation du programme

Des contrôles préventifs déployés tout au long du cycle de vie de l'employé, intégrant progressivement les domaines traditionnels de la sécurité physique et de la cybersécurité.

3

Agrégation des indicateurs de risque potentiel (PRI)

Identifier les indicateurs de risque potentiels (PRI), c'est-à-dire les comportements, actions, événements et conditions qui précèdent généralement un acte de menace interne. Comprendre comment ces PRI sont extraits des données, localiser les sources de ces données, et prendre en compte les enjeux juridiques et de confidentialité liés à leur collecte et agrégation.

4

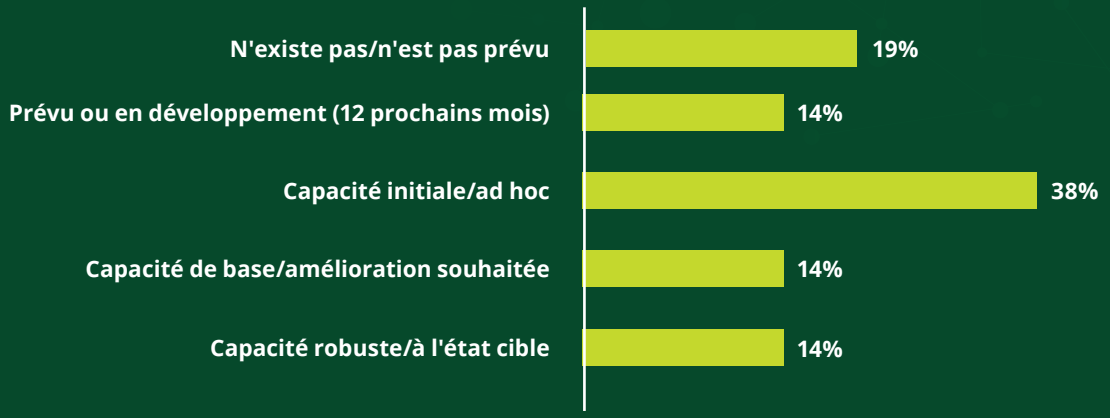
Analyse, escalade et triage du comportement des utilisateurs et des entités

En adoptant une approche axée sur les risques, collecter, corréler et visualiser les indicateurs de risque potentiels (PRI) issus de sources variées afin de détecter de manière proactive les menaces internes émergentes. Les individus présentant des scores de risque élevés doivent faire l'objet d'efforts d'atténuation ciblés, conformément à un processus d'escalade et de triage standardisé et cohérent.

Deloitte a demandé aux participants au sondage de répondre à dix questions axées sur le contrôle alignées sur ce cadre. Les réponses et les commentaires se trouvent dans les pages suivantes (pages 15-24).

Groupe de travail/comité directeur sur les menaces internes

Votre organisation dispose-t-elle d'un groupe de travail dédié aux menaces internes (ou d'un groupe interfonctionnel similaire) qui se réunit régulièrement pour discuter des risques, des tendances et des vulnérabilités organisationnelles, et pour guider la stratégie d'atténuation des menaces internes dans l'ensemble de votre organisation ?



Les pourcentages des réponses aux différentes questions de contrôle qui sont ensuite présentées sont basés sur les réponses obtenues (n = 21) ; 34 % des répondants n'ont pas répondu à ces questions.

> “Nous travaillons à l'établissement d'un programme officiel de gestion des risques internes. Au cours de notre processus initial, nous avons mis sur pied un groupe de travail spécial qui a pour but de cerner les principaux secteurs à risque et de jeter les bases d'un protocole d'intervention. Le groupe de travail permet également de discuter des lacunes immédiates, comme la vérification des employés, ainsi que les initiatives de sensibilisation et de renforcement des capacités. Nous sommes loin d'être là où nous espérons être à l'avenir, mais cela commence à gagner du terrain”

Une gouvernance coordonnée **de la gestion des risques internes**, par l'intermédiaire d'un groupe de travail spécialisé, est essentielle pour gérer efficacement les menaces internes. Seulement 14 % des organisations ont indiqué qu'elles avaient mis en place un groupe de travail interfonctionnel solide pour coordonner les efforts liés à la gestion des menaces internes. Cela signifie que même si de nombreuses organisations ont mis en place des contrôles et des mécanismes de sécurité, ceux-ci fonctionnent souvent de manière isolée, au sein de différents silos.

Un groupe de travail sur la gestion des risques internes est important, car il touche de nombreux secteurs différents d'une organisation et ne peut être géré efficacement par une seule fonction. Un groupe de travail interfonctionnel offre la structure et le cadre nécessaires pour coordonner les actions, partager les informations et aligner les priorités entre les différentes unités opérationnelles, notamment la sécurité, la cybersécurité, la fraude, les ressources humaines, le service juridique, la conformité, les communications, la protection de la vie privée et l'informatique.

Coordination interfonctionnelle

Les menaces internes couvrent souvent des domaines techniques, comportementaux et organisationnels. Un groupe de travail veille à ce que l'information circule entre les équipes chargées de la surveillance des systèmes, de la gestion du personnel et de l'application de la conformité. Cette coordination réduit les silos et augmente la capacité à détecter les risques à un stade précoce.

Stratégie de risque unifiée

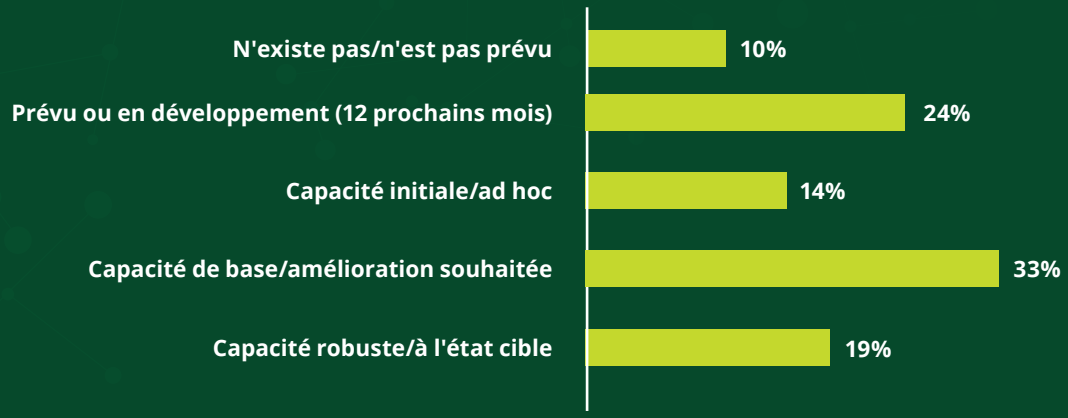
En réunissant les parties prenantes, le groupe de travail peut établir une définition cohérente du risque interne, s'entendre sur la propension à prendre des risques et assurer l'harmonisation avec le cadre plus large de gestion des risques d'entreprise de l'organisation. Cela permet d'éviter les réponses fragmentées et de soutenir le reporting exécutif.

Culture et communication

Le risque interne est autant une question de culture que de contrôle. Un groupe dédié peut travailler avec les communications et les RH pour socialiser le programme, promouvoir la sensibilisation des employés et s'assurer que les interventions sont équilibrées avec la confiance et le respect de la vie privée.

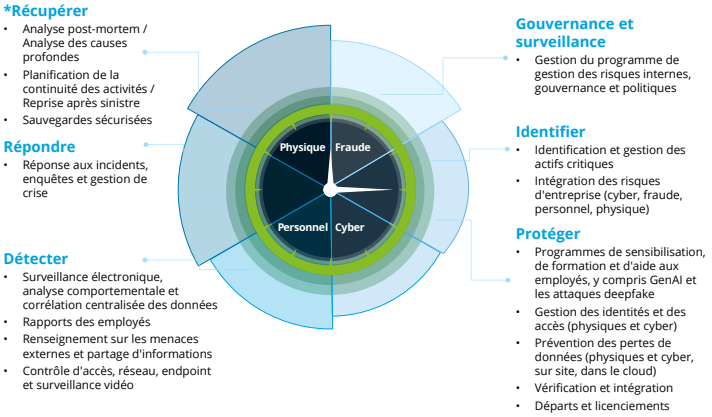
Politiques et cadres en matière de menaces internes

Votre organisation dispose-t-elle d'une politique ou d'un cadre interne qui traite spécifiquement des menaces internes, y compris des détails sur les propriétaires des risques, les voies d'escalade et les responsabilités en matière de gestion des incidents ?



Une **politique de gestion des risques internes**, accompagnée d'un **cadre de contrôle dédié**, est essentielle car elle établit les fondations, garantit la cohérence et instaure la responsabilité nécessaires pour traiter efficacement les menaces internes à l'échelle de l'organisation. En l'absence d'une politique clairement définie et d'un cadre structuré, les efforts visant à atténuer les risques internes peuvent devenir fragmentés, réactifs ou incohérents entre les unités opérationnelles.

Nos résultats montrent que plus de la moitié des organisations canadiennes ont des plans concrets pour renforcer leurs politiques et leurs cadres de gestion des risques internes au cours de la prochaine année. Un quart des organisations interrogées disposent déjà de politiques et de cadres dédiés à la gestion des risques internes, bien que ceux-ci soient encore en phase de planification ou de développement. Par ailleurs, un tiers des organisations considèrent qu'elles possèdent des capacités de base pour gérer les menaces internes, mais souhaitent renforcer et améliorer leurs programmes.



Éléments de contrôle communs du cadre de gestion des risques internes qui devraient être référencés dans une politique

Établir des attentes et une gouvernance claires

Une politique officielle énonce la position de l'organisation à l'égard du risque interne, clarifie les définitions et énonce les principes qui guident les comportements acceptables. Elle signale aux employés, aux sous-traitants et aux parties prenantes que les risques internes sont pris au sérieux et font l'objet d'une surveillance. Associée à un cadre de gouvernance, elle garantit la responsabilisation en attribuant les responsabilités et en définissant les procédures d'escalade à suivre lorsque des risques sont identifiés.

Soutenir la conformité et la résilience

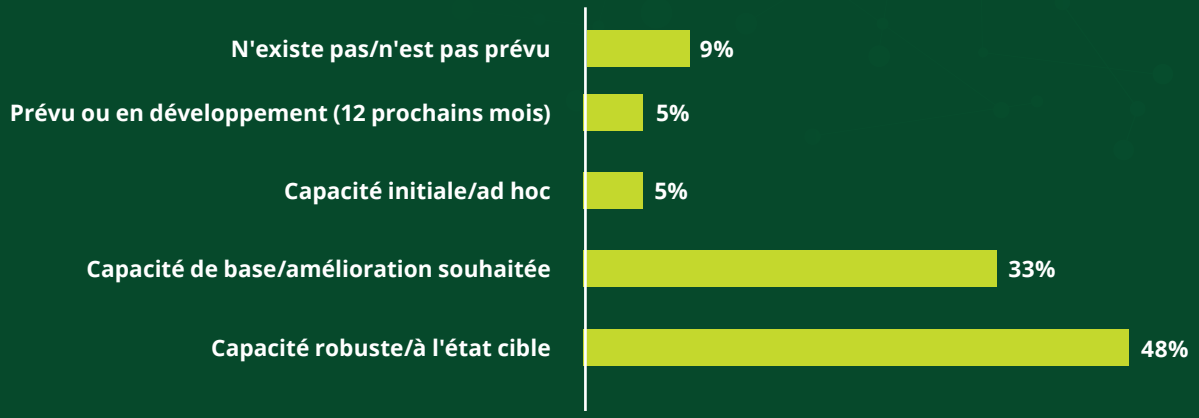
Au Canada, les directives réglementaires et sectorielles (Sécurité publique Canada, Centre canadien pour la cybersécurité et BSIF) mettent de plus en plus l'accent sur la gestion proactive des risques internes. Une politique et un cadre démontrent la conformité à ces attentes et fournissent des preuves défendables de diligence raisonnable en cas d'incident. Cela renforce la résilience non seulement contre les acteurs malveillants, mais aussi contre les menaces accidentelles et négligentes.

Normalisation des contrôles et des pratiques

Un cadre de contrôle opérationnalise la politique en la traduisant en mesures concrètes telles que les contrôles d'accès, la surveillance, l'analyse comportementale, la formation et les protocoles d'intervention. La standardisation permet de gérer les risques internes de manière cohérente, réduisant ainsi les zones d'ombre potentielles. Elle offre également une structure équilibrée entre surveillance et prévention, tout en respectant la vie privée et en préservant la confiance des employés.

Vérification préalable à l'emploi

Votre organisation effectue-t-elle des vérifications des antécédents dans le cadre du processus de pré-embauche, qui peut inclure des vérifications des antécédents criminels, des vérifications de crédit, des vérifications des médias sociaux et/ou d'autres vérifications spécialisées ?



> “Le secteur privé a besoin d'un moyen d'effectuer des vérifications plus approfondies des antécédents des entrepreneurs internationaux qui ont besoin d'un accès à distance aux réseaux et aux systèmes. Les vérifications standard du casier judiciaire par des fournisseurs tiers ne font qu'effleurer la surface. Nous devons être en mesure d'établir des liens avec la GRC, le SCRS ou Sécurité publique Canada afin de faciliter davantage de vérifications étrangères accrues dans le cadre de notre diligence raisonnable”

La vérification préalable à l'embauche est cruciale puisqu'elle constitue une première ligne de défense contre les menaces internes, en permettant aux organisations de prendre des décisions éclairées avant d'accorder aux individus l'accès à des systèmes, données, installations et personnel sensibles. Un répondant au sondage a souligné un point fondamental : la nécessité d'une meilleure collaboration entre le secteur privé et le gouvernement fédéral afin d'améliorer les processus de diligence raisonnable en matière d'embauche.

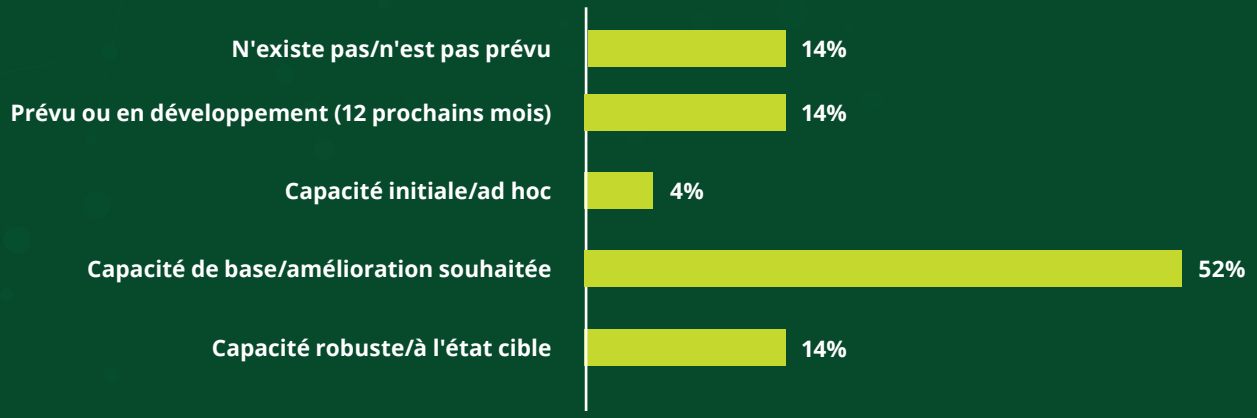
Il est important de noter que la vérification préalable à l'emploi est largement utilisée au sein des organisations canadiennes, mais qu'elle se limite souvent à la vérification des antécédents criminels. Un cadre de filtrage plus complet devrait inclure des vérifications des antécédents financiers et des examens du comportement passé dans des rôles similaires.

Types de vérifications préalables à l'embauche à prendre en compte :

- Vérification de l'identité
- Droit au travail
- Antécédents professionnels
- Vérification de l'éducation et des titres de compétences
- Vérification du casier judiciaire (national, provincial, municipal)
- Antécédents financiers/de crédit
- Dossiers de litiges civils
- Vérification des références
- Médias sociaux et sources ouvertes
- Divulgation des conflits d'intérêts
- Contrôle de l'influence et de l'ingérence étrangères
- Habilitation de sécurité (pour des rôles au sein du gouvernement ou d'infrastructures essentielles)

Évaluation continue/périodique

Votre organisation effectue-t-elle des vérifications continues ou périodiques tout au long du cycle de vie de l'employé, ce qui peut inclure des vérifications des antécédents criminels et des déclarations de conflits d'intérêts ?



Les résultats de l'enquête montrent que la majorité des répondants croient que des améliorations sont nécessaires dans la conduite de la **surveillance continue et des réévaluations périodiques** tout au long du cycle de vie de l'employé.

Il est important d'effectuer une évaluation continue et périodique des employés à la suite d'une vérification initiale préalable à l'emploi, car le risque n'est pas statique : la situation, les comportements et les niveaux d'accès d'une personne évoluent au fil du temps, tout comme son profil de risque potentiel. En effet, les circonstances peuvent changer : de nouveaux antécédents criminels, des difficultés financières et d'autres changements dans la situation personnelle peuvent modifier le comportement individuel et le niveau de risque pour l'organisation.

Cadre des facteurs de risque

- Intégrité et comportement personnel
- Activité en ligne, systèmes informatiques et sécurité des données
- Associations personnelles ou professionnelles
- Procédures pénales, statutaires et autres procédures judiciaires
- Finances
- Consommation de drogues et d'alcool
- Stabilité personnelle et comportement
- Loyauté envers l'employeur et l'activité/influence étrangère

Centre d'excellence canadien en gestion des risques internes – Fondements du dépistage et des facteurs de risque

Maintenir la sécurité et la confiance

Des évaluations régulières renforcent une culture de vigilance et de responsabilisation. Elles démontrent aux employés que la gestion des risques internes n'est pas seulement un exercice ponctuel lors de l'embauche, mais une priorité organisationnelle permanente. Lorsqu'elle est mise en œuvre dans la transparence et l'équité, cette pratique peut renforcer la confiance dans l'engagement de l'organisation à l'égard de la sécurité et de l'intégrité.

Détection des facteurs de risque émergents

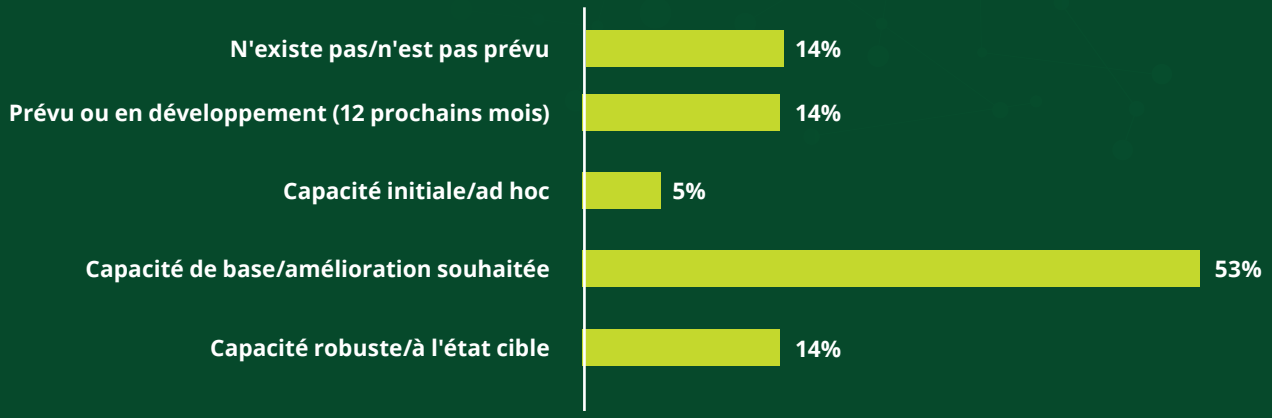
Un employé qui a réussi la présélection avant l'embauche peut éventuellement connaître des changements dans sa situation personnelle ou professionnelle, comme des difficultés financières, du stress, des griefs envers la direction ou des pressions externes, qui augmentent la probabilité d'un comportement négligent ou malveillant. Des évaluations périodiques permettent d'identifier ces signaux d'alarme émergents avant qu'ils ne se manifestent sous forme d'incidents de menace interne.

S'adapter à l'évolution des rôles et de l'accès

Les employés accèdent souvent à de nouveaux rôles, projets ou niveaux de responsabilité, obtenant parfois un accès plus élevé à des informations ou à des systèmes sensibles. Des examens périodiques permettent de s'assurer que l'accès demeure approprié et que les personnes occupant des postes de confiance continuent de respecter les normes de sécurité et de comportement de l'organisation.

Formation et sensibilisation aux menaces internes

Votre organisation dispose-t-elle de programmes internes de formation et de sensibilisation qui traitent spécifiquement des menaces internes et peuvent mettre en évidence les indicateurs et les canaux de signalement courants des menaces internes ?



En ce qui concerne la **formation** et la **sensibilisation**, la tendance au sein des entreprises canadiennes montre une adoption croissante de formations annuelles obligatoires axées sur la conformité et les risques internes. De nombreuses organisations offrent déjà ce type de formation dans le domaine de la cybersécurité, et il est à prévoir que des modules spécifiquement dédiés aux menaces internes continueront de se développer dans les prochaines années.

Les résultats de l'enquête suggèrent qu'il reste encore beaucoup à faire pour sensibiliser les organisations aux menaces internes. Il peut s'agir de la présentation d'études de cas, de séances de formation ou de dîners-conférences qui décrivent les conséquences réelles des menaces internes. Tout comme la sensibilisation à la cybersécurité est désormais monnaie courante et liée à la conformité, une formation dédiée aux menaces internes devrait également devenir la norme dans les organisations pour sensibiliser les employés à ces risques.

Considérations relatives à la formation du personnel

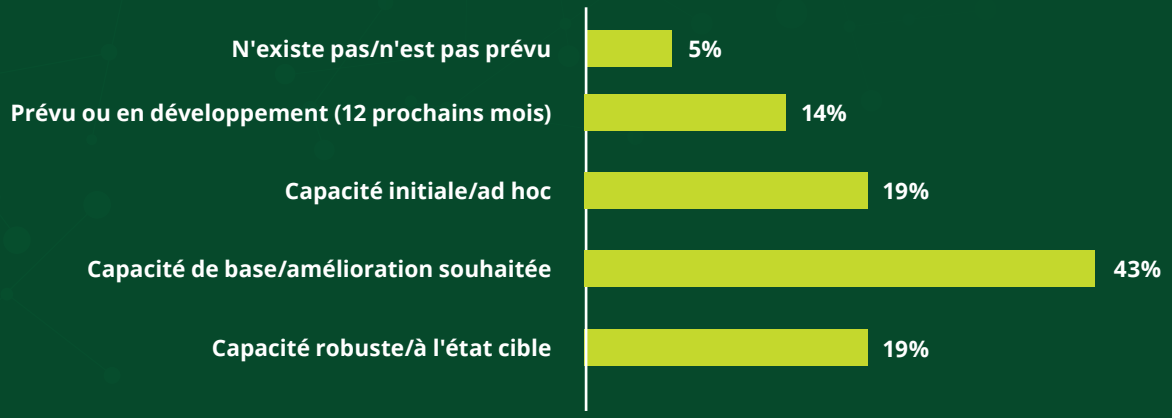
La formation sur les menaces internes doit viser à développer une culture de vigilance et de responsabilité à tous les niveaux de l'organisation. Elle doit permettre aux employés de comprendre ce qu'est une menace interne, qu'elle soit accidentelle, négligente ou malveillante, et les conséquences possibles, telles que la fuite de données, la fraude ou des atteintes à la sécurité. Elle doit inclure des mesures concrètes : protéger l'information sensible, reconnaître les comportements inhabituels, signaler les préoccupations par les canaux appropriés et suivre les protocoles de sécurité en place. Comme les employés représentent souvent la première ligne de défense, la formation devrait insister sur le fait que le risque interne n'est pas uniquement une question de sécurité ou de TI, mais une responsabilité collective.
Pour être efficace, cette formation doit rester accessible, utiliser un langage clair (non technique) et illustrer le contenu par des exemples concrets et réalistes, sans instaurer un climat de méfiance.

Considérations relatives à la formation des superviseurs

Exiger une formation plus avancée et ciblée qui va au-delà de la sensibilisation générale. Ils doivent être en mesure de cerner les comportements préoccupants, de reconnaître les indicateurs d'alerte précoce et de gérer les situations délicates avec discrétion et professionnalisme. La formation doit préparer les superviseurs à trouver l'équilibre entre la vie privée des employés et la sécurité organisationnelle, y compris la façon d'impliquer les fonctions RH, juridiques ou de sécurité lorsqu'une escalade est nécessaire.
Les superviseurs jouent un rôle crucial dans la promotion d'une culture de confiance, en veillant à ce que leurs équipes se sentent à l'aise pour signaler les incidents sans stigmatisation. Leur formation devrait porter sur les responsabilités réglementaires, l'importance de la documentation et la façon d'intégrer les considérations relatives aux risques internes dans la surveillance opérationnelle plus large. En positionnant les superviseurs à la fois comme des modèles et des premiers intervenants, les organisations s'assurent que les risques sont gérés de manière cohérente et proactive.

Procédures de départ

Votre organisation a-t-elle mis en place des procédures pour gérer spécifiquement le risque des employés sortants, telles qu'une surveillance renforcée, une liste de contrôle de départ et/ou un examen de l'accès physique et informatique ?



Le départ est un élément essentiel de la gestion des risques internes, car il représente le moment du cycle de vie de l'employé où le risque peut être le plus élevé s'il n'est pas correctement géré. Lorsque des personnes quittent une organisation, que ce soit volontairement ou involontairement, elles conservent souvent l'accès à des informations, des systèmes ou des réseaux sensibles qui, s'ils ne sont pas révoqués rapidement, pourraient être utilisés à mauvais escient intentionnellement ou accidentellement. Qu'ils soient volontaires ou involontaires, les employés qui se sentent sous-évalués ou insatisfaits peuvent tenter de voler des données sensibles ou d'exploiter des actifs à des fins personnelles.

Un grand pourcentage d'organisations ont mis en place des procédures de départ, 43 % des répondants déclarant qu'ils ont des procédures de base et 19 % déclarant qu'ils ont des procédures plus robustes.

Liste de contrôle de départ pour la gestion des risques internes

- Assurer la révocation des contrôles d'accès et du système
- Assurer la restitution et le recouvrement de tous les actifs de l'entreprise
- Effectuer une analyse de sortie des transferts de données inhabituels ou des transferts d'e-mails dans les semaines précédant le départ
- Mener une entrevue de départ structurée
- Informer les parties prenantes concernées du départ
- Conserver la documentation du processus de départ pour un examen juridique, un audit ou un examen réglementaire

Considérations clés sur l'importance du départ des employés

Atténuer les risques émotionnels ou liés aux griefs

Les départs peuvent être chargés d'émotion, en particulier en cas de licenciement, de restructuration ou de litige. Les employés dans ces situations peuvent ressentir du ressentiment ou un sentiment d'injustice, ce qui augmente la probabilité d'actions malveillantes telles que la fuite de données sensibles ou l'endommagement des systèmes. Les processus de départ qui incluent une communication respectueuse, des attentes claires et des transitions sécurisées contribuent à réduire ces risques.

Protection des actifs sensibles

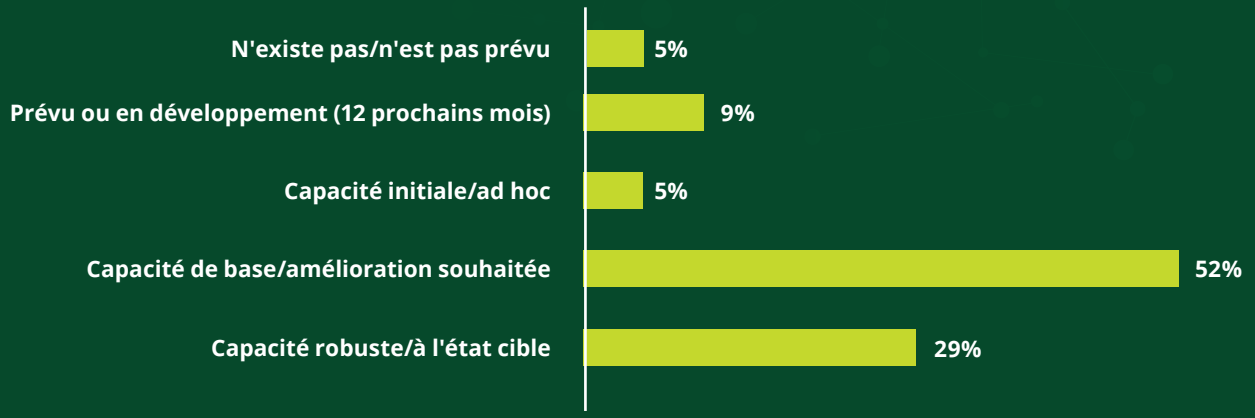
D'anciens employés, sous-traitants ou tiers peuvent toujours avoir accès à la propriété intellectuelle, aux données des clients ou à des systèmes propriétaires. Un processus de désintégration structurelle garantit la révocation rapide des droits d'accès, la récupération de l'équipement et la protection des informations confidentielles afin de réduire la probabilité de vol de données, de fraude ou de sabotage.

Culture et continuité

Lorsque le départ est géré de manière réfléchie, non seulement il minimise les risques de sécurité, mais il maintient également la confiance avec les employés restants en montrant que les départs sont gérés de manière professionnelle et respectueuse. Cela permet de préserver le moral, de réduire les commérages ou l'incertitude et de renforcer une culture de responsabilisation et de sensibilisation à la sécurité.

Gestion des accès physiques

Votre organisation maintient-elle des contrôles d'accès physiques pour gérer le risque que le personnel accède aux installations restreintes ou pour déceler les comportements irréguliers (c.-à-d. l'accès physique non requis pour les tâches ou en dehors des heures de travail habituelles) ?



Parmi les domaines évalués dans le cadre de ce sondage, la **gestion de l'accès physique** est l'un des principaux domaines où les organisations canadiennes ont déclaré avoir une capacité robuste à l'état cible. Parallèlement à la vérification préalable à l'emploi, les contrôles d'accès physique ont été constamment soulignés comme un élément bien développé des programmes de gestion des risques internes. Cela reflète l'accent mis depuis longtemps sur la protection des installations, des espaces de travail sensibles et des infrastructures critiques, où un accès physique non autorisé peut poser des risques opérationnels et de sécurité immédiats. Les résultats de l'enquête suggèrent que les organisations accordent la priorité aux aspects tangibles et visibles du risque interne, avec des contrôles structurés en place pour gérer les entrées, surveiller les mouvements et maintenir la responsabilité dans l'environnement physique.

La gestion de l'accès physique est importante car elle garantit que seules les personnes autorisées peuvent pénétrer dans des zones sensibles ou restreintes, ce qui réduit la probabilité de menaces internes et externes susceptibles de compromettre des personnes, des actifs ou des informations. Elle constitue une couche fondamentale de la gestion des risques internes qui complète les contrôles numériques et procéduraux.

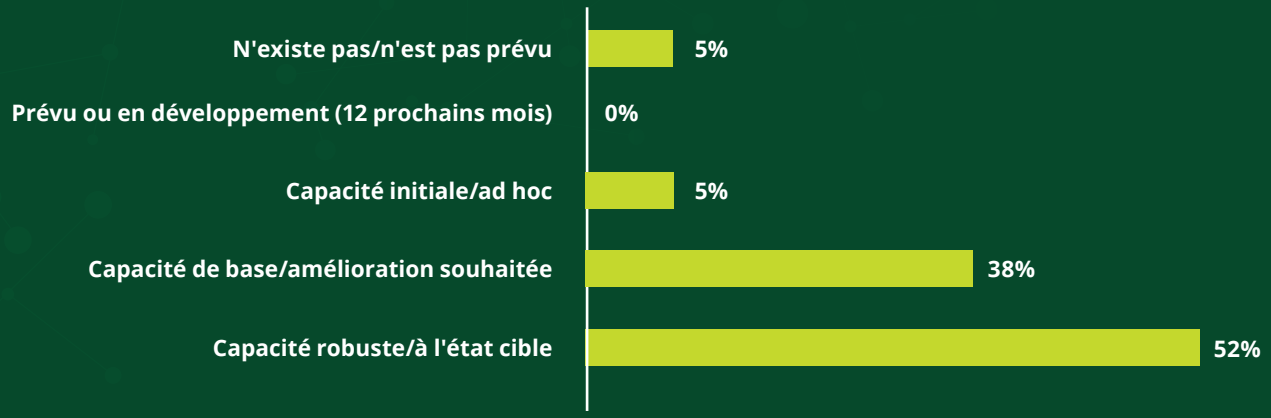
Dans l'environnement interconnecté d'aujourd'hui, les frontières entre les domaines physique et numérique sont de plus en plus floues, ce qui rend essentiel pour les organisations d'adopter une **approche cyber-physique de la gestion des accès**. Traiter l'accès physique et virtuel comme des silos distincts peut laisser des lacunes exploitables. Une approche unifiée renforce non seulement la résilience, mais reflète également la réalité selon laquelle les menaces internes modernes se déplacent souvent de manière transparente entre les espaces physiques et numériques.

Considérations

- **Protection des actifs critiques** - Le contrôle de l'accès physique empêche les personnes non autorisées d'atteindre les zones où sont stockés des données sensibles, des adresses IP, des actifs financiers ou des systèmes critiques. Même les mesures de cybersécurité les plus strictes peuvent être sapées si quelqu'un peut entrer dans une salle de serveurs ou dans des archives de documents sans surveillance appropriée.
- **Dissuasion et responsabilisation** – Lorsque les employés et les visiteurs savent que les entrées et les mouvements sont surveillés, par le biais de badges, d'une authentification biométrique ou de registres de visiteurs, cela dissuade les violations occasionnelles des politiques et les inconduites intentionnelles. Les pistes d'audit assurent également la responsabilisation, ce qui permet aux organisations de retracer qui a accédé à certaines zones et quand, ce qui est inestimable dans les enquêtes.
- **Intégration avec les programmes de gestion des risques internes** – Les données d'accès physique sont un indicateur de risque potentiel (PRI) précieux. Par exemple, un employé qui accède à plusieurs reprises à des zones en dehors de son travail ou qui entre dans des zones restreintes après les heures de travail peut signaler un risque élevé. Intégrés à l'UEBA ou à la surveillance de la sécurité, ces modèles peuvent aider à identifier les signes avant-coureurs de comportements accidentels, négligents ou malveillants.
- **Continuité des activités et confiance** – En empêchant le sabotage, le vol ou les dommages à l'infrastructure physique, la gestion des accès garantit la continuité des activités. Cela démontre également aux clients, aux régulateurs et aux employés que l'organisation prend la sécurité au sérieux, renforçant ainsi la confiance et la réputation.

Gestion des accès virtuels

Votre organisation applique-t-elle des mécanismes de contrôle pour encadrer l'accès aux systèmes, réseaux ou environnements numériques — par exemple, en s'appuyant sur le principe du moindre privilège ou la séparation des tâches ?



La gestion de l'accès virtuel a été identifiée comme l'une des capacités les plus solides signalées par les répondants, une proportion importante indiquant la maturité à l'état cible. Cette orientation illustre que les organisations reconnaissent l'importance cruciale du contrôle des accès numériques pour atténuer les menaces internes, particulièrement dans le contexte actuel de travail hybride, d'adoption croissante des technologies infonuagiques et de systèmes interconnectés. Une gestion robuste des accès virtuels garantit que les utilisateurs disposent du niveau d'accès minimum nécessaire pour remplir leurs rôles, tandis que les outils avancés de surveillance et de gestion des identités garantissent que les données et les systèmes sensibles restent protégés. Les pourcentages plus élevés du sondage dans ce domaine montrent que les organisations canadiennes harmonisent activement leurs stratégies d'accès numérique avec les pratiques exemplaires en matière de risque interne, ce qui renforce l'importance d'un accès sécurisé dans les domaines physique et virtuel.

Qu'est-ce que le Zero Trust ?

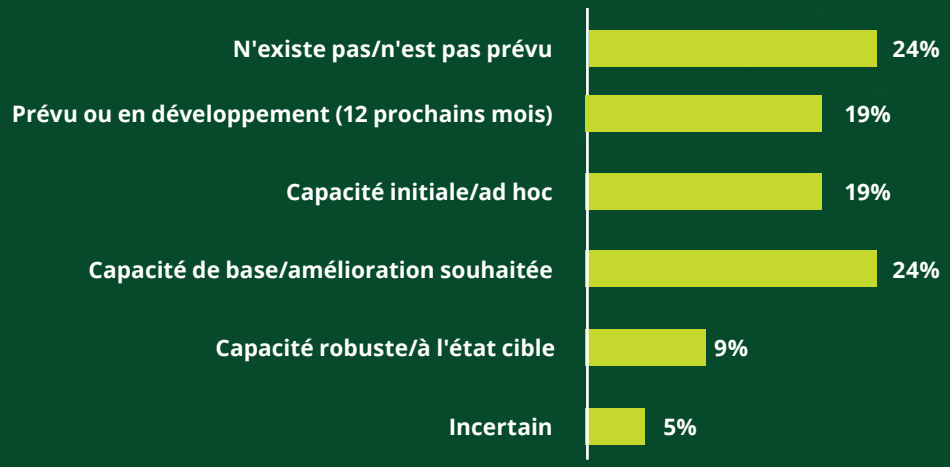
Le Zero Trust est une approche de sécurité moderne basée sur le principe « ne jamais faire confiance, toujours vérifier ». Au lieu de supposer qu'une personne au sein de l'organisation ou de son réseau peut être fiable par défaut, le Zero Trust exige une vérification continue de chaque personne, appareil et demande système, qu'elle soit physique (comme l'entrée dans une installation sécurisée) ou numérique (comme l'accès aux données sensibles). L'accès est toujours limité au moindre privilège nécessaire, surveillé en temps réel et révoqué lorsqu'il n'est plus nécessaire. En traitant chaque tentative d'accès comme potentiellement risquée, le Zero Trust aide les organisations à réduire les vulnérabilités, à détecter les menaces internes plus tôt et à renforcer la résilience dans les environnements physiques et cybernétiques.

Cyber-physique pour la gestion des accès *(objectif Zero Trust)*

- **Appliquez les principes du moindre privilège** – *Ne faites jamais confiance par défaut* – N'accordez l'accès physique et numérique qu'aux espaces, aux systèmes et aux données requis pour le rôle d'une personne ; examinez et ajustez régulièrement les autorisations.
- **Vérification continue** – *Vérifiez toujours* – Exigez la vérification de l'identité à chaque point d'accès, qu'il s'agisse d'entrer dans une zone physique restreinte ou de se connecter à un système virtuel, avec l'authentification multifacteur (MFA) comme référence.
- **Gestion unifiée des identités et des accès** – *Architecture Zero Trust* – Traitez les accès physiques et virtuels sous un modèle d'identité Zero Trust unique, où toutes les demandes d'accès sont authentifiées, autorisées et chiffrées.
- **Accès limité dans le temps et le contexte** – *Juste à temps et juste assez* – Mettez en œuvre des informations d'identification temporaires et révocables pour les visiteurs de l'installation et les utilisateurs informatiques tiers, réduisant ainsi les privilèges permanents.
- **Segmentez et micro-sécurisez** – *Microsegmentation* – Appliquez des protections d'accès en couches aux zones à forte valeur ajoutée (salles de serveurs, espaces de direction) et aux systèmes sensibles (bases de données financières ou de R&D), en limitant les mouvements latéraux en cas de violation.
- **Surveillance intégrée des risques** – Intégrez les données d'accès physiques et virtuelles dans les outils UEBA et SIEM, en corrélant les anomalies sur l'ensemble du spectre cyber-physique pour identifier les menaces internes potentielles.
- **Sensibilisation des employés à la culture Zero Trust** – Formez le personnel pour qu'il comprenne que la sécurité est la responsabilité de tous, en mettant l'accent sur des comportements tels que la prévention du talonnage, la protection des identifiants et le signalement des anomalies.

Analyse comportementale des utilisateurs et des entités

Votre organisation utilise-t-elle l'analyse du comportement des utilisateurs (ou une solution d'analyse similaire) pour renforcer ses capacités de détection en priorisant les comportements à risque au sein de l'organisation?



L'une des solutions les plus prometteuses en matière de gestion des risques internes est l'**analyse comportementale des utilisateurs et des entités (UEBA)**, qui sont des technologies capables de détecter les comportements anormaux qui pourraient indiquer des menaces internes avant qu'elles ne se matérialisent.

Malgré son potentiel, seulement 9 % des répondants à l'enquête ont indiqué que leur utilisation de l'UEBA était à un niveau optimal. Ce point est lié à la constatation que les organisations sont encore largement réactives plutôt que proactives dans leur approche.

À mesure que l'utilisation de l'analytique comportementale dans la gestion des risques internes augmente, on s'attend à ce que les organisations soient mieux outillées pour détecter les comportements suspects. Cela permettra également une meilleure modélisation des menaces et des risques et améliorera la posture globale de l'organisation face aux menaces internes.

Les systèmes UEBA établissent une base de référence de comportement « normal » pour les utilisateurs et les entités (tels que les comptes, les appareils ou les applications) dans l'ensemble de l'organisation. Ils surveillent ensuite en permanence les activités, telles que les connexions, l'accès aux données, les transferts de fichiers et les modèles de communication, afin de détecter les écarts par rapport à cette base de référence. Lorsque des anomalies se produisent, les outils UEBA les corrèlent avec des indicateurs de **risque potentiel techniques (PRI)** connus, tels que des téléchargements de données inhabituels, des tentatives de connexion infructueuses répétées, des accès en dehors des heures de travail ou des tentatives de contournement des contrôles de sécurité. Une approche à plusieurs niveaux combinant des PRI techniques, comportementaux observables et organisationnels/contextuels permet aux organisations de faire la distinction entre les irrégularités bénignes et les véritables menaces internes.

PRI communs

Faible tolérance au risque

- Licenciement en cours ou mesure disciplinaire liée au rendement
- Expressions de ressentiment dans les communications en milieu de travail
- Violations répétées des politiques malgré une prise de conscience antérieure
- Des schémas de connexion inhabituels
- Téléchargements excessifs de données ou transferts de fichiers
- Intérêt soudain pour des domaines sans rapport avec le rôle
- Tentatives de contournement des contrôles d'accès

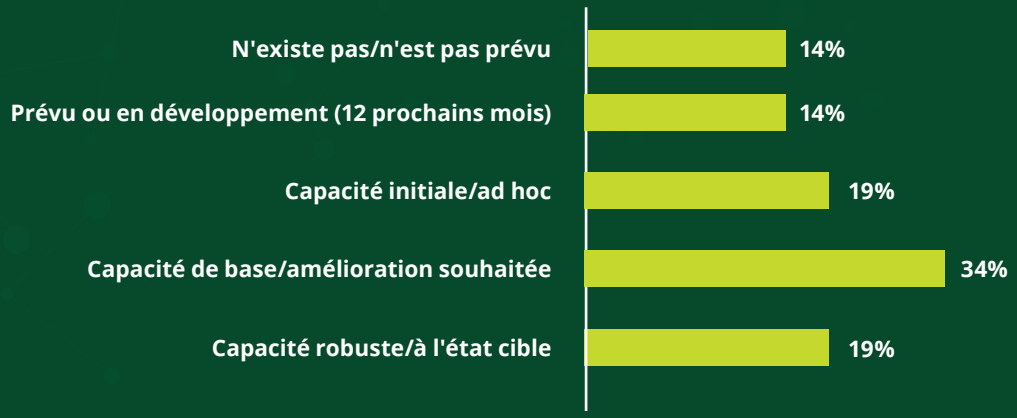
L'UEBA est-il adapté à mon organisation ?

- S'il y a un grand nombre d'utilisateurs, d'appareils et de flux de données, la surveillance traditionnelle peut avoir du mal à détecter les anomalies subtiles lorsque la complexité rend difficile l'utilisation de règles/alertes statiques.
- Si les menaces internes ont été identifiées comme un risque prioritaire dans votre organisation, l'UEBA peut fournir une détection avancée et un contexte technique à vos PRI existants.
- Demandez-vous si les outils actuels de gestion des informations et des événements de sécurité (SIEM), de prévention des pertes de données (DLP) et de gestion des identités et des accès (IAM) offrent une visibilité suffisante ou s'ils génèrent trop de faux positifs.

Contextuel Technique Comportementale

Réponse aux incidents de menace interne

Votre organisation maintient-elle des processus d'escalade et de triage pour gérer l'intervention en cas d'incident interne, qui peuvent inclure des rôles et des responsabilités définis et des protocoles de prise de décision ?



La réponse aux incidents est importante car elle permet aux organisations de passer rapidement et efficacement de la détection à l'action de réponse, en minimisant les dommages et en préservant la résilience lorsque les risques liés aux menaces internes se matérialisent. Contrairement à de nombreuses menaces externes, les incidents de menaces internes impliquent souvent des personnes qui disposent déjà d'un accès de confiance, ce qui rend la détection et la réponse particulièrement complexes. Une capacité de réponse claire et structurée aide les organisations à gérer ce défi de plusieurs manières clés.

En ce qui concerne la réponse aux incidents, seulement 19 % des organisations ont mis en place un processus de triage et d'escalade formel ou robuste pour répondre à un incident lié à une menace interne. Environ un tiers d'entre-elles disposent actuellement d'une capacité ad hoc et de ce tiers, il n'existe aucun plan supplémentaire pour faire évoluer les processus.

Le faible niveau de maturité est problématique, car les incidents liés aux menaces internes, qu'il s'agisse de fuites de données accidentelles, de violations de politiques par négligence ou d'actes malveillants tels que la fraude ou le sabotage, peuvent s'intensifier rapidement s'ils ne sont pas contenus. Un cadre de réponse aux incidents garantit que des mesures immédiates sont prises pour restreindre l'accès, sécuriser les systèmes critiques et protéger les données sensibles, réduisant ainsi l'étendue et la gravité de l'impact.

De plus, en l'absence d'un processus défini, les réponses aux incidents de menaces internes sont ponctuelles, fragmentées et retardées. Un plan formel de réponse aux menaces internes coordonne les efforts des RH, de l'informatique, du juridique, de la conformité, de la sécurité et de la direction, en veillant à ce que chaque fonction sache que son rôle et ses actions sont alignés. Cette consistance réduit la confusion et augmente l'efficacité dans des conditions urgentes.

Bien qu'une réponse efficace aux incidents soit essentielle, il importe de tenir compte des avantages d'une posture proactive pour la gestion des risques internes :

- Promouvoir la transparence par la communication et la sensibilisation à la nature du programme de gestion des risques internes de l'organisation.
- Améliore la collaboration entre les différentes fonctions de l'entreprise au sein de l'organisation.
- Centralise la gestion des risques internes pour gérer la complexité croissante dans un environnement de menaces en constante évolution.
- Démontre la nécessité pour l'organisation de quantifier les risques actuels et la valeur des investissements continus grâce à une visibilité accrue auprès des cadres supérieurs et de la direction.
- Améliore la détection et la réponse grâce à de multiples outils informatiques, à la collecte de données, à la centralisation et à la modélisation des risques.
- Définition et compréhension communes des risques internes, de l'impact, des contrôles et de la hiérarchisation des réponses sur la base de l'identification préalable des actifs critiques et des scénarios de menace.
- Des programmes de sensibilisation à la sécurité axés sur les menaces internes accidentelles et malveillantes sont régulièrement mis en œuvre, suivis de tests et de formations correctives pour les unités commerciales à haut risque.

Conclusion

Les participants à l'enquête ont été invités à évaluer l'état de préparation général de leur organisation à prévenir, détecter et répondre aux menaces internes.

Posture de prévention

2.7/5

Préparation à la prévention des menaces internes

Posture de détection

2.8/5

Préparation à la détection des menaces internes

Posture de réponse

3.2/5

Préparation à répondre aux menaces internes

Attitude proactive

2.6/5

Capacité à détecter et à réagir aux menaces internes avant qu'elles ne compromettent la sécurité

En matière de gestion des risques internes, près de la moitié des organisations canadiennes adoptent principalement une approche réactive face aux menaces internes. Cette posture pose un risque important, car elle conduit à intervenir surtout après la survenue d'incidents, plutôt que de renforcer les contrôles de détection proactive. En conséquence, ces organisations restent vulnérables à des menaces internes coûteuses, perturbatrices et évitables.

En ce qui concerne les capacités de gestion des incidents, 48 % des organisations évaluent leur aptitude à répondre à un niveau de 4 sur 5 ou plus, ce qui en fait l'une des forces majeures dans la gestion des menaces internes. En revanche, seulement 19 % des organisations jugent leur capacité de détection efficace, et 24 % considèrent que leurs mesures de prévention sont adéquates. Ces résultats soulignent un défi important pour le secteur : le besoin d'un changement de mentalité vers une détection proactive des menaces internes.

Les participants à l'enquête ont été invités à évaluer dans quelle mesure leur organisation est proactive dans la prévention, la détection et la réponse aux menaces internes.

Les résultats montrent que les organisations continuent principalement à réagir après la survenue d'incidents, plutôt que de mettre en œuvre des contrôles de détection et de réponse améliorés, ce qui les rend vulnérables à des menaces internes coûteuses, perturbatrices et évitables.

Bien que les résultats du sondage révèlent que les menaces internes constituent un enjeu accru dans les industries canadiennes par rapport à il y a dix ans, il est évident que les organisations doivent intensifier leurs efforts pour faire évoluer leurs contrôles. Par ailleurs, un renforcement des cadres législatifs et normatifs, notamment en comparaison avec les États-Unis et l'Australie, est nécessaire afin de garantir la promotion et l'harmonisation des bonnes pratiques de gestion des risques internes à l'échelle du gouvernement, des infrastructures essentielles et des secteurs privés.

Le gouvernement américain exige la mise en place de programmes dédiés à la gestion des risques internes dans chaque entité gouvernementale depuis la signature du décret présidentiel 13587 en 2011. Depuis 2024, le gouvernement australien exige la mise en œuvre de programmes dédiés dans toutes les entités gouvernementales qui gèrent les habilitations de sécurité dans le cadre de son cadre stratégique de sécurité préventive.

Perspectives pour les organisations canadiennes

- **Renforcer la coordination interfonctionnelle** : la gouvernance des menaces internes doit être renforcée par la création de groupes de travail dédiés et de comités interfonctionnels impliquant les ressources humaines, l'informatique, l'éthique et la conformité, la sécurité, le juridique et les opérations commerciales.
- **Accélérer l'élaboration et la mise en œuvre des politiques** : Des politiques de gestion des risques internes doivent être élaborées et mises en œuvre. Des directives claires sur la façon de détecter les menaces internes et d'y répondre sont nécessaires pour renforcer l'engagement à l'échelle de l'organisation.
- **Assurer une surveillance continue et intégrer des outils tels que l'UEBA** : L'absence de surveillance continue après l'embauche, avec peu de réévaluations périodiques des employés, expose les organisations à des risques non détectés. Il est crucial d'intégrer des outils tels que l'analyse comportementale des utilisateurs et des entités (UEBA) pour identifier les comportements à risque tout au long du cycle de vie des employés.
- **Ne négligez pas les comportements en dehors des systèmes numériques** : les menaces internes résultent souvent de facteurs psychologiques et comportementaux complexes qui ne se manifestent pas uniquement sur les plateformes virtuelles. L'analyse des comportements non numériques, tels que les interactions en personne et les changements d'habitudes des employés, doit également être une priorité.

Annexe A : Orientation et réglementation

Au Canada, la gestion des risques internes est de plus en plus reconnue comme un élément essentiel de la résilience organisationnelle. Bien qu'il ne soit pas régi par une réglementation unique et globale, le risque interne touche plusieurs domaines (sécurité, confidentialité, fraude et protection des infrastructures critiques) et est reflété dans les directives fédérales, les exigences sectorielles et les meilleures pratiques. Les organisations canadiennes doivent donc adopter une approche à plusieurs niveaux, en harmonisant leurs politiques internes avec les normes nationales et les attentes réglementaires.

Sécurité publique Canada **Résilience face au risque interne**	*S'applique à : Toutes les organisations, en mettant l'accent sur les propriétaires et les exploitants d'infrastructures essentielles* Décrit huit mesures de sécurité recommandées qui peuvent renforcer la résilience des actifs et des systèmes organisationnels.
Centre canadien pour la cybersécurité **Comment protéger votre organisation contre les menaces internes (ITSAP.10.003)**	*S'applique à : Toutes les organisations* Fournit plusieurs procédures de sécurité qui peuvent être mises en œuvre pour réduire les risques internes.
Bureau du surintendant des institutions financières **Ligne directrice B-13 : Gestion des risques technologiques et cybernétiques**	*Vise : Institutions financières canadiennes réglementées par le BSIF* L'objectif de la ligne directrice est d'aider les institutions financières à développer une plus grande résilience face aux cyber risques et aux risques internes.
Commissariat à la protection de la vie privée du Canada **Conclusions de la LPRPDE #2020-005**	*S'applique : Les leçons apprises et les recommandations s'appliquent à toutes les organisations en ce qui a trait à l'équilibre entre la surveillance et la protection de la vie privée des employés, afin de protéger les données* Fournit des recommandations sur l'équilibre entre la surveillance des employés et la protection de la vie privée en milieu de travail dans le contexte de la gestion des risques internes.
Innovation, Sciences et Développement économique Canada **Politique sur la recherche sur les technologies sensibles et les affiliations préoccupantes**	*S'applique à : Établissements d'enseignement supérieur/universités* Fournit des directives et des outils pour mettre en œuvre la sécurité de la recherche, y compris les meilleures pratiques d'atténuation des risques axées sur les menaces internes et le vol à des fins de recherche.

Contacts

Pierre-Luc Pomerleau, Ph.D.,
Associé
E : ppomerleau@deloitte.ca

Victor Munro
Directeur principal
E : vmunro@deloitte.ca
Directeur exécutif, CInRM CoE
E : victor.munro@cinrmcoe-cdecgrin.ca

Isabelle Fraser
Directrice
E : ifraser@deloitte.ca

Deloitte.

Designed by CoRe Creative Services. RITM2225986