



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

MEMBER OF
IRPA
Insider Risk
Practitioner Alliance



20 26

DTEX

 **First Advantage**

Control Risks

EVERFOX

Deloitte.

 **EchoMark**

GARDAWORLD
SECURITY

SUMMARY OF INSIGHTS

Insider Risk
Management
Partnerships
Summit

Toronto, Ontario

21-22 September



OVERVIEW

The 2026 Insider Risk Management Partnerships Summit brought together Canadian and international practitioners from the public, private and academic sectors for two days of discussion on the evolving insider risk environment and the continued development of organizational insider risk management capabilities.

Discussions explored the changing threat environment; national security and foreign interference; governance and program maturity; employee reporting and organizational culture; screening and workforce assurance; behavioural and technical detection; artificial intelligence; high-risk roles; and international collaboration. These themes reflect the Summit's broader objectives of strengthening Canada's insider risk management community, advancing practitioner knowledge and sharing emerging practices across domestic and international partners.

ABOUT THIS REPORT

This report consolidates recurring themes and practitioner insights from the 2026 Summit. Consistent with the Chatham House Rule under which the Summit was conducted, observations are presented without attribution to individual participants or organizations.

The report captures areas of convergence, lessons learned and emerging considerations rather than providing a transcript of Summit proceedings.

BOTTOM LINE

Insider risk is increasingly an enterprise risk. Effective management requires accountable leadership, integrated governance, trusted reporting mechanisms, visibility across the workforce lifecycle, and the ability to adapt to rapidly changing technologies and threats.



SIX INSIGHTS DEFINING INSIDER RISK IN 2026

01 | GOVERNANCE COMES FIRST

02 | TRUST IS A SECURITY CONTROL

03 | INTERVENE BEFORE AN INCIDENT

04 | MANAGE THE ENTIRE WORKFORCE LIFECYCLE

05 | NO ORGANIZATION SEES THE WHOLE PICTURE

06 | AI IS CHANGING THE RISK LANDSCAPE



Governance Comes First

Technology cannot compensate for fragmented accountability. Mature insider risk management programs require an accountable executive, formal governance and sustained participation across security, cyber, HR, legal, privacy, risk and business functions.

INSIGHT 01



Trust is a Security Control

Employees are often the first to recognize concerning changes in behaviour. Their willingness to raise concerns depends on psychological safety, confidence in leadership, protection from retaliation and belief that reporting will lead to fair and appropriate action.

INSIGHT 02



Intervene Before an Incident

Insider risk management should operate before behaviour becomes an incident. Indicators should prompt assessment and proportionate intervention—not an automatic assumption of malicious intent. Effective mitigation can include employee support, access changes and other preventative measures.

INSIGHT 03



Manage the Entire Workforce Lifecycle

Strong pre-employment screening is not enough. Risk changes throughout employment, particularly during role changes, periods of stress, privileged access and departure. Contractors, temporary personnel and other third parties require comparable consideration.

INSIGHT 04



No Organization Sees the Whole Picture

Insider risk increasingly crosses organizational, sectoral and national boundaries. Foreign interference, supply chains, distributed workforces and common adversaries make trusted information sharing and practitioner collaboration essential.

INSIGHT 05



AI is Changing the Risk Landscape

AI is changing how people interact with organizational information and creating risks that existing controls were not designed to address. Organizations must also begin considering AI and other non-human agents within insider risk governance.

INSIGHT 06

01 | LEAD AND GOVERN

Name the owner before buying the tool.

Organizations should establish executive accountability and cross-functional governance before—or alongside—investments in advanced detection capabilities.



Insider risk must be managed as an enterprise risk.

Summit discussions repeatedly reinforced that mature programs begin with leadership, governance and accountability—not technology.



Executive ownership matters.

A clearly accountable senior leader is required to sustain organizational attention, resolve competing priorities and provide authority for cross-functional action.



Governance connects fragmented capabilities.

Many organizations already possess relevant controls across cyber, physical security, HR, legal, privacy, investigations and risk. The challenge is bringing these capabilities together under a common framework.



Programs should be risk-based, not tool-based.

Technology accelerates detection and analysis, but it does not determine organizational risk appetite, make intervention decisions or establish accountability.



Maturity requires institutionalization.

Working groups are valuable starting points, but mature programs require defined policies, procedures, roles, escalation pathways and executive oversight.

02 | KNOW AND SUPPORT YOUR WORKFORCE

Measure whether employees trust the system—not simply whether a reporting mechanism exists.

Successful intervention can protect both the organization and the individual. As discussions emphasized, insider risk management programs should not be understood simply as mechanisms for identifying and terminating employees; timely support and proportionate intervention can prevent escalation.



Trust and workforce awareness are fundamental to prevention.

Technology can identify unusual activity, but people often recognize behavioural change, workplace conflict and personal stressors before those signals appear in technical systems.



Create a culture where employees will speak up.

Employees need clear reporting channels and confidence that ambiguous concerns can be raised without retaliation or an expectation that they prove wrongdoing themselves.



Front-line managers matter.

Direct supervisors are particularly important because they are positioned to recognize changes in behaviour, performance and workplace relationships.



Perception can outweigh policy.

A reporting process may appear effective on paper but fail if employees believe reports will be ignored, mishandled or result in disproportionate consequences. Summit discussions identified lack of confidence that action would be taken as an important barrier to reporting.



Indicators are not proof.

Behavioural change or technical anomalies should trigger assessment—not an automatic conclusion that an individual represents a threat.

03 | DETECT, CONNECT AND ACT

Ask whether your organization can connect the dots before an incident—or only explain them afterwards.



The challenge is often not the absence of indicators—it is the failure to connect them.
Insider risk signals can exist across different organizational functions without any one function seeing enough information to recognize the broader pattern.



Establish a baseline.
Understanding normal workforce and system activity helps organizations distinguish meaningful deviations from routine behaviour.



Combine human and technical signals.
Behavioural analytics, access controls and monitoring should complement—not replace—observations from managers, coworkers, HR, physical security and other organizational functions.



Enable appropriate information sharing.
Legal, privacy and organizational requirements must be respected, but unnecessary silos can prevent relevant information from being connected. International implementation experience presented at the Summit identified formal information-sharing arrangements as a persistent challenge.



Act before certainty.
Waiting for proof of malicious intent can mean waiting until after harm occurs. Organizations need processes to assess ambiguous indicators and intervene proportionately.

04 | MANAGE RISK ACROSS THE WORKFORCE LIFECYCLE

Move from pre-employment screening to continuous workforce assurance.



Screening at the front door provides only a point-in-time assessment.

Organizations generally maintain stronger controls when individuals enter the workforce than they do throughout employment or when individuals change roles or leave.



Risk changes over time.

Financial pressures, workplace grievances, personal circumstances, organizational change and access requirements can change significantly after initial screening.



High-risk roles warrant differentiated assurance.

Organizations should identify positions with access to particularly sensitive information, systems, facilities or decision-making authorities and align controls to the potential consequence of misuse.



Temporary does not mean low-risk.

Contractors, consultants, interns, temporary employees and other third parties may receive significant access without the same organizational history or behavioural baseline as permanent employees.



Departure is a risk event.

Offboarding should address physical and logical access, data movement, intellectual property and unusual activity surrounding departure.

05 | INSIDER RISK IS A SHARED PROBLEM

No organization, industry or country possesses a complete picture of insider risk.

The Summit reinforced the importance of trusted partnerships across the public and private sectors, academia and international practitioner communities.

Emerging technologies, foreign interference, global workforces and interconnected supply chains increasingly create risks that transcend organizational boundaries.

Information sharing enables organizations to learn from incidents they have not personally experienced, identify common indicators and accelerate the development of preventative controls.

The Summit's opening discussions captured this central theme: what affects one organization or sector today may affect another tomorrow, making community and trusted collaboration increasingly important.

06 | UNDERSTAND THE CHANGING RISK ENVIRONMENT

Reassess what constitutes a “crown jewel.”

Organizations should consider not only individually sensitive assets, but how seemingly low-sensitivity information could create significant value when aggregated.



The distinction between “inside” and “outside” threats is becoming increasingly blurred.
The Summit highlighted several developments reshaping how organizations should understand insider risk.



Artificial intelligence changes both risk and defence.
AI is changing how employees create, access, process and share information. Organizations need visibility into how approved and unapproved AI tools interact with sensitive organizational data.



Non-human agents challenge traditional definitions.
As AI agents perform increasingly autonomous functions, insider risk frameworks built around human users will need to evolve.

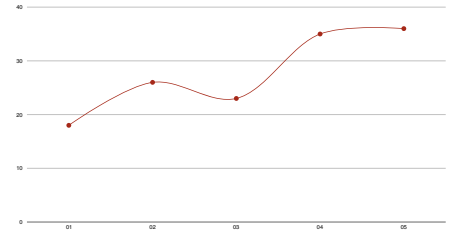


Foreign actors value more than classified information.
Research, intellectual property, infrastructure information, commercial data and other individually unclassified or seemingly low-sensitivity information can become highly valuable when aggregated and analyzed. Summit discussions specifically highlighted the potential value of aggregated information to foreign actors.



Access—not employment status—is increasingly important.
Employees, contractors, partners, suppliers and other trusted parties may all possess legitimate access that can be exploited by external actors.

FIVE QUESTIONS FOR LEADERS



01 WHO OWNS INSIDER RISK?

Is there an accountable executive and empowered cross-functional governance body?

02 WHAT WOULD WE ACTUALLY DETECT TODAY?

Do we have sufficient visibility across people, systems, information and facilities to recognize meaningful deviations?

03 WOULD OUR PEOPLE TELL US?

Do employees trust supervisors, reporting mechanisms and organizational follow-up enough to raise concerns early?

04 WHERE ARE OUR LIFECYCLE BLIND SPOTS?

Does assurance continue through employment, privileged access, role changes, contractors and departure?

05 ARE WE PREPARING FOR TOMORROW'S RISK?

Have AI, non-human agents, foreign interference, third parties and changing workforce models been incorporated into our program?



BUILDING CANADA'S INSIDER RISK MANAGEMENT COMMUNITY

**EFFECTIVE INSIDER RISK MANAGEMENT
DEPENDS ON PEOPLE, PARTNERSHIPS
AND TRUST AS MUCH AS POLICIES AND
TECHNOLOGY.**

As the threat environment continues to evolve, organizations will need to move beyond isolated security controls toward integrated, enterprise-level programs that combine leadership, workforce assurance, behavioural and technical detection, early intervention and trusted information sharing.

The Canadian Insider Risk Management Centre of Excellence will continue to support this development through research, training and learning, practitioner knowledge sharing, information-sharing initiatives and domestic and international partnerships. Those activities align directly with the Centre's stated mandate and current initiatives.

DTEX  **FirstAdvantage**  **Control Risks** **EVERFOX** **Deloitte.**  **EchoMark** **GARDAWORLD**
SECURITY

THANK YOU TO OUR SPONSORS

The 2026 Summit and the broader work of the CInRM CoE would not be possible without the generous support of our industry partners.

We extend our sincere appreciation to our Summit sponsors — DTEX Systems and First Advantage (Platinum), Control Risks and Everfox (Gold), and Deloitte (Silver) — as well as CIBC for hosting us at CIBC Square.

We also thank Deloitte, DTEX Systems, EchoMark and GardaWorld Security for sponsoring the Summit Social, creating an important opportunity for our community to continue building relationships beyond the formal program.

Your support enables us to bring together practitioners from across government, industry, academia and our international partners, while keeping our community initiatives focused on collaboration, knowledge sharing and advancing the practice of insider risk management.

Simply put, these initiatives would not be possible without your partnership. Thank you for investing in this community and in what we are building together.

For inquiries & collaborations:

Canadian Insider Risk Management Centre of Excellence
www.cinrmcoe-cdecgrin.ca
admin@cinrmcoe-cdecgrin.ca

Insider Risk Practitioner Alliance
www.irpa.org





A NOT-FOR-PROFIT ENTITY THAT IS EVOLVING CANADA'S CAPABILITIES IN INSIDER RISK MANAGEMENT BY FOSTERING AN INTERDISCIPLINARY APPROACH AIMED AT ACCELERATING RESEARCH, TRAINING, EDUCATION AND BUILDING SUSTAINED COMMUNITY PARTNERSHIPS.

Founded in 2022, the Canadian Insider Risk Management Centre of Excellence (CInRM CoE) is federally incorporated under the Canada Not-for-Profit Corporations Act, as a public service body, not-for-profit entity and soliciting corporation, based at Carleton University, Norman Paterson School of International Affairs (NPSIA).

The CInRM CoE promotes academic, private, and public partnerships to generate academic research, provides training and learning opportunities, promotes knowledge sharing, and augments resources and capabilities in the professional market to mitigate insider threats to Canadian organizations and critical infrastructure. The scope of its services are offered to all Canadian federal, provincial, territorial (FPT) and indigenous organizations—with a particular focus on fostering critical infrastructure (CI) resiliency—subject to resourcing.

The CInRM CoE fosters an interdisciplinary approach to insider risk management towards the promotion of industry best practices and innovation within an evolving threat environment. Funded by industry contributions and research grants, we offer a national and centralized capability on all matters related to insider risk management. Our products and services include research and analysis, facilitating workshops and knowledge sharing events with subject matter experts, generating lessons learned, providing workplace training, and advocating for new initiatives to enhance Canada's collective resiliency against insider threats. This work is established on a foundation of information sharing among a trusted community of security, intelligence, and defence professionals.