FIRPA
FVEY Insider Risk
Practitioner Alliance

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

INSIDER RISK
MANAGEMENT
PARTNERSHIPS
SUMMIT

SUMMARY OF INSIGHTS

2025

SPONSORED BY

DTEX Control Risks EVERFOX Deloitte.

Summary of Insights

INTRODUCTION

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.

The Insider Risk Management Partnerships Summit was organized and led by the CInRM CoE in Toronto, Ontario on September 15-16, as part of Canadian Insider Threat Awareness Month (CITAM).

The Summit consisted of a two day-long agenda covering various topics across 20 presentations and discussion panels focused on present-day insider risk management (InRM) topics of relevance to Canadian private, public, and academic practitioners in the community-at-large. The Summit was a by invitation-only event, attended by 230+ participants, representing over 90 organizations, including representatives from the private sector, federal, provincial, and municipal levels of government, and academia from Canada, Norway, and the United States.

The Summit was held under Chatham House rules. The following summary is a list of key insights that were offered from insider risk practitioners on the present-day threat environment and considerations in InRM for the near- and long-term.

Summary of Insights

Key Takeaways

01. Leadership engagement is critical

Senior executives must be visible, accessible, and actively engaged in building a culture of security awareness. The isolation between C-suite and frontline employees creates vulnerabilities that nation-state actors and malicious insider threats can exploit.

02. Economic pressures are amplifying insider risk

Workforce reductions, budget constraints, and remote work complexities are creating conditions that increase both malicious and unintentional insider threats. Organizations must develop resilience strategies that account for these economic realities.

03. Nation-state infiltration is evolving rapidly

The DPRK IT worker phenomenon represents a new paradigm in insider threats, demonstrating how foreign adversaries are systematically infiltrating organizations through legitimate employment channels.

04. Artificial Intelligence presents dual challenges

While AI offers powerful capabilities for insider threat detection and analysis, it also introduces new vulnerabilities and amplifies existing risks, requiring organizations to balance innovation with security considerations.

Summary of Insights

Key Takeaways

05. Cross-functional collaboration is essential

Successful insider risk management requires breaking down organizational silos and fostering partnerships between security, human resources, legal, privacy, and business operations teams.

06. Cultural transformation alongside technological solutions

While advanced monitoring tools and behavioural analytics are valuable, sustainable insider risk management depends fundamentally on creating organizational cultures built on trust, transparency, and shared responsibility for security.

07. Proactive employee support reduces risk

Organizations that invest in employee mental health, provide clear communication channels for grievances, and offer comprehensive support during transitions (including terminations) have seen lower insider threat incidents.

Summary of Insights

Present-Day Insider Risk Management

Leadership and Organizational Resilience

The relationship between leadership behaviour and insider risk has become increasingly apparent.

Executive visibility and accessibility emerge as critical factors in maintaining organizational security. The growing distance between senior leadership and frontline employees creates information gaps that adversaries can exploit. Regular engagement mechanisms, such as structured listening sessions and accessible communication channels, serve as both early warning systems and preventive measures against insider threats.

Organizations experiencing significant workforce reductions face heightened insider threat activity, particularly when layoffs are conducted without adequate support structures or communication strategies.

Economic pressures are fundamentally reshaping the insider threat landscape. Budget constraints force organizations to make difficult choices between security investments and operational efficiency. However, cutting resources without corresponding adjustments to the overall security posture creates vulnerabilities that sophisticated threat actors actively monitor and exploit.

The transition to remote and hybrid work models continues to complicate traditional insider risk management approaches. Organizations must adapt their monitoring, investigation, and response capabilities to account for distributed workforces while maintaining employee trust, privacy, and productivity.

Summary of Insights

Present-Day Insider Risk Management

Nation-State Insider Threats

The emergence of systematic nation-state infiltration through IT worker placement represents a paradigm shift in insider threat attack methodology. The Democratic People's Republic of Korea (DPRK) has demonstrated the effectiveness of this approach, stealing funds while potentially accessing sensitive information and systems.

Traditional pre-employment screening processes have proved inadequate against sophisticated identity manipulation and document forgery capabilities.

The dual-purpose nature of these infiltrations - generating revenue while conducting espionage - complicates detection efforts. Unlike traditional insider threats driven by personal grievances or ideological motivations, these actors are often competent professionals who maintain low profiles and avoid behaviours that might trigger security alerts.

International cooperation becomes essential when addressing nation-state insider threats, as these operations typically involve complex logistics spanning multiple jurisdictions and exploiting regulatory gaps between countries.

Organizations must enhance their verification procedures, implement multi-layered authentication during hiring processes, and maintain heightened awareness of employment patterns that may indicate coordinated infiltration attempts.

Summary of Insights

Present-Day Insider Risk Management

Artificial Intelligence and Technology Integration

Artificial intelligence represents both an opportunity and a challenge for insider risk management. While AI capabilities enable more sophisticated behavioural analysis and pattern recognition, the technology also introduces new attack vectors and amplifies existing vulnerabilities.

Organizations implementing AI-driven insider threat detection must balance analytical capability with privacy considerations and employee trust. The perception of excessive surveillance can undermine the collaborative culture necessary for effective security awareness and reporting.

The rapid pace of AI development creates challenges for security teams attempting to understand and mitigate emerging risks. Organizations must invest in continuous education and capability development to maintain pace with evolving threats and defensive technologies.

Data quality and governance become increasingly critical as AI systems require comprehensive, accurate datasets to function effectively. Poor data management not only reduces AI system effectiveness but can also introduce biases that compromise security decisions.

Summary of Insights

Present-Day Insider Risk Management

Recognition of foreign interference attempts requires enhanced awareness training that helps employees understand how legitimate professional interactions can be manipulated for intelligence gathering purposes. This includes education about elicitation techniques, cultivation methodologies, and the gradual nature of most coercion attempts.

Foreign Interference and Coercion

Foreign interference activities increasingly target employees through sophisticated social engineering and coercion techniques. These operations often begin with seemingly benign contact through professional networking platforms and gradually escalate to requests for sensitive information or access.

The transnational nature of modern workforces creates additional vulnerabilities, particularly for employees with family connections or financial interests in countries that conduct aggressive intelligence operations. Organizations must develop sensitive approaches to addressing these vulnerabilities without creating discriminatory practices.

Reporting mechanisms must be designed to accommodate the sensitive nature of foreign interference situations, where employees may fear personal or family repercussions from coming forward with concerns.

Summary of Insights

Present-Day Insider Risk Management

Organizational Culture and Employee Engagement

The fundamental role of organizational culture in insider risk management has become increasingly evident. Employees' perceptions of fairness, transparency, and organizational values directly influence their willingness to comply with security policies and report suspicious activities.

Psychological safety emerges as a critical component of effective insider risk management. Employees who fear retribution or judgment are less likely to report concerns or admit mistakes that could have security implications. Creating environments where employees can raise issues without fear requires sustained leadership commitment and cultural transformation.

The relationship between employee engagement and security compliance demonstrates that organizations cannot separate human resources management from security considerations. Disengaged employees pose higher insider risks, while engaged employees serve as additional sensors for detecting anomalous behaviour.

Supervisor training and support represent high-leverage interventions for improving organizational security posture. Front-line managers have the greatest opportunity to observe behavioural changes and maintain relationships that encourage security awareness and reporting.

Summary of Insights

Present-Day Insider Risk Management

Legal and regulatory compliance adds complexity to monitoring decisions, particularly for organizations operating across multiple jurisdictions with different privacy requirements. Security teams must work closely with legal and privacy professionals to ensure monitoring practices meet operational needs while satisfying regulatory obligations.

Privacy and Surveillance Balance

The tension between necessary security monitoring and employee privacy expectations requires careful navigation. Organizations must implement monitoring capabilities that provide security value without creating oppressive work environments that undermine productivity and morale.

Transparency about monitoring practices, when operationally feasible, helps maintain employee trust while enabling necessary security functions. Employees who understand why certain monitoring occurs and how their privacy is protected are more likely to accept and support security measures.

Technology solutions must be selected and configured with privacy considerations integrated from the beginning rather than added as an afterthought. Privacy-by-design approaches help organizations avoid creating systems that generate compliance risks or employee relations problems.

Summary of Insights

Present-Day Insider Risk Management

Research and Data-Driven Approaches

The Canadian insider threat research landscape continues to evolve, with multiple studies demonstrating the value of empirical approaches to understanding and addressing insider risks. Data-driven insights help organizations move beyond anecdotal evidence to develop evidence-based policies and procedures.

Information sharing initiatives, while challenging due to sensitivity concerns, offer significant value for improving collective security awareness and response capabilities. Structured approaches to sharing threat indicators and mitigation strategies benefit the entire community.

Academic partnerships bring analytical rigor and research capabilities that individual organizations struggle to develop independently. These collaborations produce insights that inform both policy development and practical implementation decisions.

Benchmarking studies provide organizations with context for evaluating their security posture relative to industry peers. Understanding how other organizations approach similar challenges helps identify gaps and opportunities for improvement.

Summary of Insights

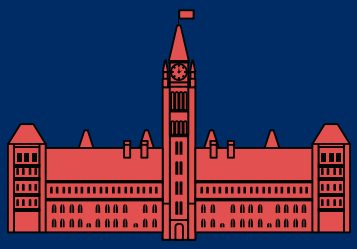
Sector Specific Considerations

Critical Infrastructure Protection

Critical infrastructure sectors face unique insider threat challenges due to the potential for catastrophic consequences from successful attacks. These organizations must maintain higher security standards while operating within resource constraints and regulatory requirements.

The interconnected nature of critical infrastructure systems means that insider threats in one organization can have cascading effects across multiple sectors. This reality requires enhanced information sharing and coordinated response capabilities.

Supply chain vulnerabilities create additional pathways for insider threat actors to access critical systems. Organizations must extend their insider risk management programs to include contractor and vendor personnel who have access to sensitive systems or information.



Government and National Security

Government organizations face persistent targeting from foreign intelligence services seeking to recruit or coerce employees with privileged access. These threats require specialized detection and response capabilities that account for the sophisticated nature of state-sponsored operations.

Security clearance processes, while necessary, create additional complexity for insider risk management. Organizations must balance the need for thorough vetting with operational efficiency and employee privacy considerations.

The classification system creates information silos that can complicate insider threat detection efforts. Organizations must develop approaches that enable appropriate information sharing while maintaining necessary security controls.

Private Sector Adaptation

Private sector organizations may lack the regulatory mandates that can drive insider risk investments, requiring security leaders to build business cases based on risk management and competitive advantage arguments.

Intellectual property protection represents a primary driver for private sector insider risk programs. Organizations must identify and protect their most valuable information assets while enabling necessary business operations.

Customer data protection obligations create additional compliance requirements that influence insider risk management program design and implementation. Organizations must ensure their security measures satisfy both security and privacy regulatory requirements.

Summary of Insights

Emerging Threats and Future Considerations

Artificial Intelligence and Machine Learning Risks

The proliferation of AI technologies creates new categories of insider threats, including the potential for employees to inadvertently or deliberately compromise proprietary algorithms, training data, or model architectures. Organizations must develop specific protections for AI-related intellectual property.

AI systems themselves can become vectors for insider threats when employees with privileged access manipulate training data, alter algorithms, or extract sensitive information learned by AI systems during operation.

The use of AI tools by employees introduces data loss risks when sensitive information is shared with external AI services. Organizations must develop policies and technical controls to prevent unauthorized data sharing while enabling productive use of AI capabilities.

Remote Work and Distributed Operations

The permanent shift toward hybrid and remote work models requires fundamental reconsideration of insider threat detection and response capabilities. Traditional approaches based on physical presence and network perimeter monitoring prove inadequate for distributed workforces.

Home office security presents new challenges, as organizations have limited control over the physical and digital environments where employees handle sensitive information. Education and support become more critical than technical controls in these scenarios.

International remote work arrangements create additional complexity when employees travel or relocate to countries with different legal frameworks or heightened hostile foreign intelligence activities. Organizations must develop flexible policies that account for varying risk levels across different locations.

Summary of Insights

Recommendations for Organizations

Immediate Actions

Organizations should conduct comprehensive assessments of their current insider risk management capabilities, identifying gaps in coverage and opportunities for improvement. This includes evaluating both technical capabilities and organizational processes.

Leadership development programs should incorporate insider risk awareness components, ensuring that leaders at all levels understand their roles in maintaining organizational security and supporting employee well-being.

Employee support systems should be enhanced to provide proactive assistance during periods of personal or professional stress. This includes mental health resources, financial counseling, and career development opportunities.

Medium-Term Development

Cross-functional collaboration structures should be formalized to ensure that insider risk considerations are integrated into all relevant organizational decisions. This includes representation from security, human resources, legal, privacy, and business operations functions.

Technology investments should prioritize solutions that enhance analytical capabilities while maintaining employee privacy and organizational efficiency. Organizations should avoid implementing monitoring systems that create oppressive work environments.

Training and awareness programs should be expanded beyond traditional security topics to include recognition of foreign interference attempts, AI-related risks, and the importance of maintaining organizational culture and values.

Long-Term Strategic Considerations

Organizations should develop strategic partnerships with industry peers, academic institutions, and government agencies to enhance their collective security capabilities and threat awareness.

Research and development investments should focus on innovative approaches to insider risk management that leverage emerging technologies while maintaining human-centered approaches to security.

Organizational culture development should be treated as a long-term investment requiring sustained leadership attention and resource commitment. Culture change initiatives require multiple years to achieve meaningful results.

Conduct a Comprehensive Insider Risk Management Capability Assessment

Cross-functional collaboration structures should be formalized

Organizational culture development should be treated as a long-term investment

Summary of Insights

Conclusion

The insider risk management landscape continues to evolve rapidly, driven by technological advances, geopolitical tensions, and organizational transformations. Success in this environment requires adaptive approaches that balance security effectiveness with operational efficiency and employee well-being.

The insights gathered from this year's Summit emphasize the critical importance of leadership engagement, cross-functional collaboration, and organizational culture in creating effective insider risk management programs. While technology plays an important supporting role, the fundamentally human nature of insider threats means that people-centered approaches remain essential.

Organizations that invest in comprehensive insider risk management programs, maintain strong collaborative relationships within the practitioner community, and adapt continuously to emerging threats will be best positioned to protect their most valuable assets while maintaining productive and engaging work environments.

The Canadian Insider Risk Management Centre of Excellence remains committed to supporting the practitioner community through research, education, and collaboration initiatives. The continued growth and engagement of this community represents Canada's best defense against the evolving insider threat landscape.

Summary of Insights

The Year Ahead: CInRM CoE 2025–26 Initiatives

FIRPA

Five Eyes Insider Risk Practitioner Alliance

The CInRM CoE continues to strengthen international collaboration through FIRPA, with active discussions underway in the United Kingdom for establishing a parallel Centre of Excellence. This expansion will enhance information sharing and joint research capabilities across the Five Eyes community.

IRPA

Insider Risk Practitioner Alliance

Building on successful partnerships with Australia and the United States of America, the CInRM CoE is expanding its cooperation framework to potentially include additional Alliance countries, including Norway and other NATO members, facilitating broader international collaboration on insider threat research and best practices.

Canadian Insider Threat Dataset (CITD) – Phase 2 Implementation

Building on the successful Phase 1 release of the open-source dataset containing 530 Canadian insider threat incidents from 1930 to present, the CInRM CoE is launching Phase 2 with the Canadian Cyber Threat Exchange focused on structured, anonymized data sharing among participating organizations. This initiative will enable real-time threat intelligence sharing while maintaining strict privacy and confidentiality protocols.

Electricity Sector Insider Threat Study – Final Report

In partnership with Electricity Canada, the CInRM CoE will publish the final report of its comprehensive study on insider threat reporting practices within Canada's electricity sector. This follow-up replication study builds on previous research in the financial services sector and provides sector-specific insights for critical infrastructure protection.

Insider Threat Certification and Training Program

The CInRM CoE has its professional certificate program in insider risk management, designed for security practitioners, human resources professionals, and organizational leaders. The program combines academic rigor with practical application, featuring case studies from Canadian organizations and international best practices.

IInsider Risk Management Self-Assessment Tool

Based on industry standards and maturity models, the CInRM CoE will release a comprehensive self-assessment tool over the course of 2026. This resource will enable organizations to evaluate their current InRM capabilities, identify improvement opportunities, and track progress over time.

National Benchmark Study with Deloitte

The CInRM CoE has partnered with Deloitte to conduct a comprehensive national benchmark study on insider risk management practices across Canadian organizations. This research provides the first comprehensive assessment of InRM maturity levels, resource allocation, and effectiveness measures across multiple sectors, enabling organizations to benchmark their programs against national standards.

Summary of Insights

Inquiries And Information About Us

The CInRM CoE operates as a trusted community where participants share resources, collaborate on research, and benefit from collective expertise while maintaining strict confidentiality and professional standards. All activities are conducted with appropriate security protocols and respect for proprietary information.

Organizations interested in participating in CInRM CoE initiatives can learn more about the Centre through its website. Various solutions are available for organizations of all sizes, with specific programs designed to meet the needs of small and medium-sized enterprises, large corporations, government agencies, and academic institutions.

REACH OUT TO US AND ENGAGE WITH THE BROADER COMMUNITY

Website :

www.cinrmcoe-cdecgrin.ca

Email address :

admin@cinrmcoe-cdecgrin.ca