INSIDER RISK MANAGEMENT SECURITY PARTNERSHIPS SUMMIT 2024

Summary of Insights

Canadian Insider Risk Management Centre of Excellence (CInRM CoE)

Toronto, Ontario

CanadianInsiderRiskManagementCOE@carleton.ca

FIRPA
FVEY Insider Risk Practitioner Alliance

CANADIAN INSIDER RISK MANAGEMENT CENTRE OF EXCELLENCE

Sponsored by DTEX accenture EVERFOX Control Risks Deloitte.

Five Eyes Insider Risk Practitioner Alliance (FIRPA)

Vision

To grow, support, and prepare a global community of skilled insider risk practitioners under a trusted unified alliance.

Call to Action

Foster growth in Centre of Excellence (COE) insider risk hubs to link a network of practitioners to exchange best practices and information, collaborate in training, workshop, and conference venues.

Canadian Insider Risk Management Centre of Excellence (CInRM CoE)

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 non-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, 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.

BACKGROUND – Insider Risk Management Security Partnerships Summit 2024

FIRPA held its fourth event, organized and led by the CInRM CoE in Toronto, Ontario on September 19, as part of Canadian Insider Threat Awareness Month (CITAM).

The Summit consisted of a day-long agenda covering various topics across 14 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 153 participants, representing 80 organizations, including representatives from the private sector, federal, provincial, and municipal levels of government, and academia from Canada, Australia, 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.

KEY TAKEAWAYS – Executive Summary

- The need for collaboration across industries and organizations - **building security allies** - to manage insider risks effectively is of vital importance.
- International cooperation, particularly within the Five Eyes (FVEY) community is vital as insider risks extend beyond national borders, necessitating collaboration on shared risk indicators and solutions.
- There is a **delicate balance** between employee monitoring and privacy.
    - Leverage tools that allow real-time monitoring of employee activities without creating an overly intrusive work environment. Behavioural analytics, particularly identifying anomalies, are key tools; however, when implementing, caution is urged to avoid creating a "Big Brother" atmosphere in places of employment.
    - Organizations need to consider the implementation of continuous personal vetting throughout employees' term of employment. Initial background checks are no longer sufficient, and regular updates and monitoring should be a part of any InRM strategy.
    - Transparency and ensuring broad employee engagement within security policy development are identified as critical strategies to mitigate working tension when enhancing InRM program capabilities.
- Organizations should build a culture of collaboration and education where employees feel trusted, yet accountable. To foster this environment employers are suggested to develop open communication channels and regular check-ins between managers and their staff.
- While technology, such as artificial intelligence (AI) and machine learning, have a role in threat detection, human oversight remains indispensable.
    - Technology is a tool, but strategic decisions require human input, particularly in aligning security and operational efficiency.
    - AI has significant potential in future insider threat detection, specifically in analyzing behavioural patterns over time. However, there are concerns regarding the ethical and privacy implications of such technologies.
- The importance of addressing employee grievances proactively. Many instances of insider threat were linked to employees being "burned out" and feeling marginalized within the organization, leading them to act out or leak information. Regular, anonymous surveys, "pulse checks", and introducing ombudspersons were recommended as tools to foster a culture of transparency and trust.

- Organizations are encouraged to prioritize mental health programs to maintain a healthy and secure work environment.

Insights – Present-Day Insider Risk Management

- **Collaboration**
  - Collaboration is key – ensure continuous engagement with leading experts to exchange ideas and knowledge, fostering an environment of learning and continuous improvement. Sharing best practices across organizations is essential for growth and adaptation in a rapidly evolving threat landscape.
  - Open, transparent communication within and between organizations ensures that all voices are heard, and new perspectives are considered.
  - **Breaking Silos -** organizations often focus inward, but true progress requires collaboration for the greater good. Breaking down barriers between departments and entities can lead to more effective solutions.
  - **Summits are Essential but Not Sufficient** - while events like the Canadian national summit are crucial for bringing together experts and sharing knowledge, they must be part of a broader, sustained effort to drive real change.
  - **FVEY Insider Risk Practitioner Alliance (FIRPA)** as a conduit for collaboration
    - FIRPA working groups have collaboratively addressed specific insider risk issues and are working to build community frameworks that not only help organizations to benchmark their programs, but also establish industry standards.
    - Continuous learning is the foundation of progress. Master classes have been created to educate practitioners, sharing knowledge and best practices to strengthen the insider risk management community.
    - Sharing opportunities, such as FIRPA-led initiatives, create spaces for dialogue and cooperation. Whether through working groups or building frameworks, these collaborations enable the industry-at-large a clearer path forward,

establishing baselines and best practices guided by experienced practitioners.
        - The development of standardized playbooks has proven instrumental in managing insider risks. These resources offer actionable strategies and guidelines that organizations can implement to improve their security posture.
    - Centres of Excellence, within FIRPA, are **independent not-for-profit** organizations that offer three main solutions:
        - Events
            - Bringing people together;
        - Research and Development
            - What is currently happening in the space that people need to be aware of; and
        - Education
            - How to build a IRM practice
    - Operational Information Exchange (OIE) offered by the C-InRM CoE are opportunity for:
        - Efficiency
            - By sharing research and resources, organizations can streamline efforts, ensuring that valuable time is spent on action rather than duplicating work. This enables teams to focus on implementation rather than exhaustive data gathering.
        - Research
            - With time constraints often leaving little room for research, the ability to share findings across organizations helps the wider community gain a more complete understanding of the issues at hand, leading to more informed decision-making.
        - Reducing redundancy
            - Avoiding the duplication of research and risk management efforts is a key benefit of collaboration. When teams share their findings, everyone benefits without repeating the same work, allowing for rapid adopiton and more efficient progress.
        - Informal Benchmarking

- Through shared insights and informal discussions, organizations can benchmark their efforts against one another. This includes obtaining ideas from others' successful examples or realizing they may be pioneering on their own, this shared knowledge provides valuable context for progress and innovation.

➢ **Complexity**
  - Balance
    - Managing insider risk requires navigating organizational complexities that span employee morale, workforce health, operational efficiency, and intersections with national security.
    - Striking the right balance between surveillance and privacy is key to comprehensive insider risk monitoring. Employees who feel constantly watched may suffer from a sense of mistrust, leading to disengagement, which can negatively impact morale and productivity.
    - While security measures are essential, they can also slow down workflows and create friction within operations. It is important to balance security protocols with operational efficiency to avoid stagnation and maintain a productive workforce.
  - Foreign Interference (FI)
    - Having a dedicated team focused on FI allows organizations to spot trends more easily. Consistent monitoring by a specialized team enhances the ability to detect anomalies and risks before they escalate.
    - Individuals don't typically join organizations as spies, but they may "flip" at some point. Common triggers include personal grievances, lack of promotion, mental health struggles, family pressure from abroad, or a desire to influence overseas conflicts. Understanding these nuanced motivations is key.
    - Watching for changes in employee behaviour, such as decreased performance, increased requests for access to specific subsets of information, or noticeable emotional shifts are important indicators of potential insider threat activity.

These could be signs that something has changed in personal situations or that individuals may be under pressure.
        - Supervisors and colleagues play a crucial role in recognizing shifts in employee behaviour. Reporting unusual actions or behavioural patterns can help prevent risks before they materialize.
        - Certain roles, especially those involved in sensitive areas like AI or quantum research, are at greater risk of foreign interference. Countries like the People's Republic of China are often open about their interests in these fields. It's important for organizations to treat security as an investment rather than just a line-item cost.
        - In some cases, FI threat actors are detected not because of changes in behaviour but due to strong security measures, such as being detected in areas they weren't authorized to access (physical and logical).
        - FVEY partners are leveraging AI and advanced analytics to combat FI. However, it's critical to verify the accuracy and reliability of these tools to ensure they are effective and tailored to the organization's needs. The best approach is to use the highest quality technology that the organization can afford.
- **Modernization**
    - Urgency
        - Organizations must make modernization happen—there is no room for excuses. Establishing a dedicated program and developing a clear strategy are critical first steps in staying ahead of evolving risks.
    - Marketing and Transparency
        - A transparent approach, combined with effective marketing of an insider risk management program, are essential to build trust and ensure that stakeholders understand the value and importance of modernization efforts.
    - Enhance the Entire Organization
        - Modernization should improve all verticals within an organization. This includes planning for success by

implementing effective access controls and developing a robust Incident Response Plan in collaboration and routine engagement with all corporate administrative areas and core business.

- Modelling
  - Developing a governance model to validate initially detected suspicious behaviours can help to clarify doubts, using as a tool to identify potential insider threat activities and ensure that risks are addressed systematically.
- Technology
  - Leveraging AI and machine learning can streamline threat detection, but it is important to remember that technology is only a tool, not a “silver bullet”. It must be complemented by human oversight and strategic decision-making.
  - Behavioural analytics are powerful for detecting insider threats, but they also raise concerns about privacy ("big brother" perception). Striking a balance between effective monitoring and respecting employee privacy is essential.
  - Proper stewardship of data is crucial, especially when dealing with sensitive employee information. Mishandling or leaking data can bypass even the most advanced technological defenses.
  - Cybersecurity teams often face an overwhelming amount of information. Processing large volumes of data efficiently is a challenge, and evaluating the behaviour of one employee may require the attention of multiple team members, which is not sustainable long-term, without additional investments in technology and outsourcing considerations.

- **Employees**
  - Insider threat is not limited to extreme cases and examples; it applies to all employees, contractors, and military personnel. Human factors represent the biggest opportunity for improving insider threat detection and mitigation, particularly among average, day-to-day employee interactions which may create unintentional risks.

- Employees often weigh the perceived necessity of security policies against the effort required to follow them. They are more influenced by what their peers do and perceive as acceptable, rather than formal workplace policies. This perception shapes the organizational culture and can drive compliance—or non-compliance—with security measures.
- Employees look to their peers to determine what is considered normal behaviour within the organization. If they perceive that others are getting away with rule-breaking or that the organization is not enforcing policies, they are likely to adapt their actions accordingly.
- For employees to contribute effectively, they must feel psychologically safe, included, and able to voice concerns without fear of retribution. This includes fostering an environment where individuals feel comfortable challenging norms and offering new ideas.
- Employee mental health check-ins, both formal and informal, are essential. Continuous monitoring of employee behaviour and mental health, along with regular background checks and personal vetting, should be a standard practice, as individuals' situations change over time.
- Role-based risk approaches should be used to track potential insider threats related as related to specific job positions. This includes monitoring processes, funding, data access, equipment, high-risk work functions, and other critical areas that are susceptible to insider risk based on the nature of the role.
- Organizations must offer trusted channels for employees to express grievances. Perceived unfairness can lead to leaks or insider threats if employees feel they have no other outlet for their frustrations.

- **Organizational culture**
  - The shared perceptions, assumptions, and values within an organization significantly impact insider risk. A positive culture that prioritizes employees' needs, perceptions, and engagement can reduce risks and improve adherence to security policies.

- Collectives within an organization can either amplify or dampen individuals' beliefs, emotions, decision-making accuracy, and cooperation. A strong, positive collective environment fosters better cooperation and security compliance.
- Trust within an organization boosts energy and productivity. In contrast, employees who experience burnout, overwork, chronic stress, or lack of psychological safety are less likely to adhere to security requirements, highlighting the need for a healthy work environment.
- Employees are more engaged when they experience:
    - Personal Meaning
        - Feeling that their work is meaningful.
    - Autonomy
        - Having a sense of agency in their roles.
    - Fair and Ethical Treatment
        - Trusting that the organization is acting in a just manner.
    - Authentic Social Connections
        - Valuing satisfying social bonds at work.
- Many employees feel disconnected from their organization’s values and purpose, which leads to disengagement and increased insider risk. Providing meaningful work can help reconnect employees to the organization's mission.
- Tools for Culture Improvement:
    - A quick security culture assessment method.
    - Tools for supervisors to improve psychological safety.
    - A holistic approach involving HR, CISO, legal, and all organizational departments in insider risk management, even those not traditionally involved.
- Supervisors have a profound impact on organizational culture and insider risk. Front-line managers are critical in engaging employees and maintaining a positive culture, while toxic supervisors are often blamed for organizational issues. Investing in supervisors' people skills and ensuring support from senior leadership is essential.
- Supervisors are pivotal in shaping the mental health and engagement of employees. Organizations should focus on

improving supervisors' skills to foster a healthier and more secure workplace.
    - Commit to customizing science-based tools to meet organizational needs, assess their effectiveness, and seek continuous improvement in organizational culture.
- **Notable Insider Threat Case Study - Cameron Ortis**
    - Ortis sold a trove of sensitive information, not only from the Royal Canadian Mounted Police (RCMP) but also from the Five Eyes (FVEY) Alliance, for a reported $20K. He copied classified documents, removed top-secret markings, and used encrypted methods to transfer the data. He printed 488 classified documents, mainly during holidays and weekends.
    - Recommendations:
        - Strengthen the role of the Chief Security Officer (CSO) and integrate tighter physical security controls.
        - Implement stricter approval processes for access to restricted databases containing sensitive data, such as the Canadian Top-Secret Network (CTSN) in the Ortis case.
        - Enhance the overall security culture within the organization.
        - Address the backlog in personnel security (PERSEC) onboarding processes.
        - Raise standards for information technology asset management.
        - Make security awareness training mandatory for all employees.
        - Reduce the number of high-security zones and printing locations to a strict minimum (this also applies to logical segregation under zero-trust architecture principles).
        - Implement an online platform for the anonymous reporting of security incidents.
        - Develop a dedicated insider threat program to specifically detect and mitigate future risks.
    - Challenges:
        - The implementation of recommendations must be completed swiftly following the incident of a detected insider threat to ensure that any identified control gaps are resolved efficiently.

- Any procedural changes must respect the integrity of ongoing investigations.
- The damage caused by insider threats have a lasting effect on the organization's operations and reputation.
- The pandemic had added another layer of difficulty in addressing ongoing insider risk management challenges.
- It is impossible to eliminate all security risks but mitigating them through these measures is critical.

➢ **What's Coming from the COE**

- Education
  - Development of workplace e-Awareness and training programs, with content drawn from graduate courses and technical certificate offerings, aimed at fostering security awareness across a broader employee organizational base, including those outside traditional security roles.
- Research
  - Insider threat incident sharing under the Canadian Insider Threat Dataset (CITD) concept - A white paper has been produced, and confirmation of an industry sponsor is in progress. The next step includes piloting a proof of concept to validate the parameters of the white paper.
  - CITD Open Source
    - A project to create an open-source dataset of Canadian Insider Threat incidents from 1945 to 2023. The goal is to release version 1.0 of the CITD in 2025.
  - Insider Threat Monitoring Theory
    - In partnership with DTEX, the COE is completing a study under a Carleton University Norman Paterson School of International Affairs (NPSIA) doctoral dissertation process that includes an analysis of 302 insider threat attack incidents across Australia, Canada, and the United States to analyze the monitoring controls that are most associated to low-impact outcomes for organizations.
  - Sector Insider Risk Study – Employee internal reporting of suspicious incidents

        - A collaborative InRM study involving the CInRM CoE, Electricity Canada, and NPSIA. The research will focus on sector-specific risks in a replication study of a previous study using a Canadian finance sector sample.
    - The CInRM CoE is working with Deloitte on a national survey aimed at gaining insights into security risk perceptions within Canadian organizations. This builds on a similar study conducted in Australia, offering an opportunity for industry benchmarking and understanding security controls leveraged by different organizations.
- Ongoing Community Engagements
    - CInRM CoE, in collaboration with MITRE and Accenture, had completed a successful information sharing pilot earlier in 2024 focused, that received positive feedback. The CInRM CoE will continue its collaboration with industry vendors to delivery additional information sharing events over the course of the next year.
    - The CInRM CoE is scheduled to present at a personnel security conference at Defence Research and Development Canada's (DRDC) Ottawa Carling campus in November.