INSIDER RISK MANAGEMENT SECURITY PARTNERSHIPS SUMMIT 2023

Summary of Insights

Canadian Insider Risk Management Centre of Excellence
(C-InRM CoE)

Toronto, Ontario

CanadianInsiderRiskManagementCOE@carleton.ca

FIRPA
FVEY Insider Risk Practitioner Alliance

CANADIAN INSIDER RISK MANAGEMENT CENTRE OF EXCELLENCE

Sponsored by DTEX accenture

Five Eyes Insider Risk Practitioner Alliance (FIRPA)

Vision

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 (C-InRM CoE)

Founded in 2022, the Canadian Insider Risk Management Centre of Excellence (C-InRM CoE) is a not-for-profit entity that fosters academic, private, and public partnerships to generate academic research, provide training and learning opportunities, promote knowledge sharing, and augment resources and capabilities in the professional market to mitigate insider threats to Canadian organizations and critical infrastructure.

The C-InRM 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 sponsorships, federal research grants, academic scholarships, and other contractual arrangements, our products and services include research and analysis, facilitating workshops with subject matter experts, and generating lessons learned, built on a foundation of information sharing among a trusted community of security, intelligence, and defence professionals.

BACKGROUND – Insider Risk Management Security Partnerships Summit 2023

FIRPA held its second event, organized and led by the Canadian Insider Risk Management Centre of Excellence (C-InRM CoE) in Toronto, Ontario on September 28, as part of Canadian Insider Threat Awareness Month (CITAM).

The Summit consisted of a day-long agenda covering various topics across 12 presentations and fireside chats, 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 93 participants, representing 57 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

- While there have been significant compromises in multiple Canadian critical infrastructures over the past decade, **insider risk management is still not a well-defined program area** with dedicated organizational policies and roles. Additional federal legislation and **mandatory insider risk management standards applied to critical infrastructure protection** (e.g., Bill C-26) may assist with overall national resiliency.
  - That said, industry reporting is predicting an **increase in organizations' adoption of formalized insider risk programs** in the near term (i.e., next two years).
- There is **no universal best practice or standard in terms of where an insider risk management program should be centralized within organizations**—it is the area which is most mature in InRM and best able to bring together different corporate administrative functions.
- **Human factors and continuous screening assurance** is critical (i.e., technology alone cannot do it all).
- Insider risk management is not only focused on security mitigation—InRM programs have to **cultivate effective partnerships with HR** to promote healthy organizations that focus on the wellbeing of employees.
- InRM programs should consider **proactive insider threat potential versus the reactive countering of known insider threats**. When potential and actual insider threats are identified, prompt and efficient intervention is necessary—corrective actions should consider solutions that include restricted access and reassignment to different job roles—versus outright job dismissal depending on the severity of the circumstances.
- Words matter—InRM programs must consider the **appropriate organizational contextualized terminology** that will serve to foster broad organizational support for the goals of the InRM program.
- Canadian critical infrastructure requires further **support to mitigate foreign nation-state interference that seeks to leverage insider threats** with privileged access to organizations' assets.
- The value of story-telling—when an insider threat investigation is concluded, **there is an opportunity to share** the indicators of compromise, lessons learned, and follow-on gap remediation, for internal security training and awareness, and external information sharing with partners.

Insights – Present-Day Insider Risk Management

- **International security in the Five Eyes (FVEY)**
  - Human factors are important – technology cannot take precedence over integrative approaches that consider physical and personnel security–i.e., insider threats do not always use technology and technology-only solutions cannot provide organizations with the necessary assurance required for mitigation purposes.
  - Insider threat motivations vary and the surrounding contextual circumstances for compromises may be pre-planned or opportunistic–this means that we can't predict an insider threat attack (but we can take proactive measures in risk management).
  - Senior leadership in organizations need to develop and foster healthy organizations, including measures to reduce workplace burnout and other stressors within the organization that lead employees to not adhere to security and other policy requirements. Front-line managers are a crucial part of the solution.
    - Mental health programs need to be promoted in organizations (i.e., Employee Assistance Programs), and additional campaigns to reduce the stigma of mental health when these mechanisms are used by employees are required. Most individuals that are responsible for deliberate insider threat attacks are not the same as those that require additional EAP support. A partnership with Human Resources is a crucial enabler and is a pattern that works well in effective insider risk management programs. Organizations should seek out a representative case of a recent insider threat compromise as the starting point where an insider risk program may partner with HR to review how proactive and response measures may be enhanced in future cases of suspected threats.
    - Training and awareness must occur across the organization. Insider risk programs must take a "big-picture", enterprise approach and involve cross-departmental collaboration and include additional focused insider risk management training for leadership. Employees in higher-risk functions and groups

should be provided with more tailored training to better protect the organization's assets.
        - Bi-directional loyalty to mitigate insider risk—defined as employees looking out for the well-being of the organization, and leadership looking out for the well-being of employees—is only achieved through continuous engagement with the broader employee base, developing and promoting positive incentives, and rewarding effective supervisors.
    - Employees are the best tool to mitigate insider threats, and this can include approaches such as "see something, say something", but organizational policies and programs must be tailored as it must be considered why these approaches fail in practice:
        - Organizational culture – "don't be a snitch";
        - What are employees' perceptions about what occurs internally after they make a report (i.e., what is the risk to me and what's in it for me);
        - How to cultivate an environment where employees are motivated and want to help the organization; and,
        - Words matter—insider threat mitigation programs should consider labels that are sensitive to the present organizational culture—i.e., insider trust programs, reporting a "concern" versus an "incident".
    - Improvement of comprehensive, fair, and effective continuous screening assurance is a key mitigative measure.
    - A follow-up response control that is effective includes prompt additional inquiries and scrutiny on attempts to access information or facilities that are not clearly within the scope of one's work responsibilities.
- **Canadian national security**
    - Foreign interference is a complex issue that requires continuous information sharing and collaboration between the private and public sectors to protect Canadian national critical infrastructure (CI).
    - No organization is immune from insider threats.
    - At risk CI sectors need further training and awareness on foreign interference threats that leverage insider threats with privileged access.

- Effective insider risk management requires collaboration internally between different areas of corporate administrative management– especially with legal and HR, and increased willingness to work externally with law enforcement and national security agencies.

- **National critical infrastructure protection**
  - There is no universal best practice or standard in terms of where an insider risk management program should be stood up in organizations–it is the area which is most mature and best able to bring together different corporate administrative functions under a centralized program model. Organizations have based their InRM programs within corporate security, cyber security, enterprise risk, ethics and compliance, or legal functions.
  - To ensure communication with different business areas in an organization for a holistic insider risk management program:
    - Implement a federated risk management model for information sharing;
    - Centralize investigations related to suspected insider threats (and ensure that relevant legal and HR data is part of insider threat investigations); and,
    - Establish solid and meaningful partnerships with HR, along the lines of being proactive on insider risk management with a program philosophy being based on providing assistance to enhance employees' well-being rather than only catching and addressing corporate policy violations.
  - Different methods that an insider risk management program may use to combat the negative perception of scope creep (i.e., everything that occurs in an organization counter to organizational policy is by definition insider threat activity) may include:
    - Not being seen as only an enforcement function;
    - Build partnerships across different corporate administrative business areas and engage core business functions;
    - Finding opportunities to have focused discussions on the present threat environment with different stakeholders that are at risk; and,
    - Taking on a philosophy and operational approach of helping rather than dictating through policy

        - Tailoring mitigation approaches to different types of insider threats (i.e., accidental vs. deliberate).
    - There are no single technological solutions for case management and databases—software must be implemented at scale with an organization's available resourcing and aligned to its internal model of information sharing, workflows, and governance.
    - Some common insider risk mitigation practices and ideas to consider as part of programming may include:
        - Identification controls
            - When an insider threat investigation is concluded, consider this as a use case, where indicators of compromise, lessons learned, and follow-up gap remediation, may be re-purposed for internal security training and awareness, and external information sharing with partners—this can occur without compromising individuals' privacy, the integrity of investigations, and/or corporate reputation.
        - Protection controls
            - Architect physical and logical controls with a security-by-design, zero-trust philosophy and approach (i.e., trust but verify) towards creating more friction to employees' and third-party contractors' access to critical business assets, balanced with business requirements in discussion with core business leads.
            - Ensure that third-party contracts have the necessary language to provide assurance that reporting is occurring on potential insider threats in the supply chain linked to critical processes, assets, and information.
        - Detection and Response controls
            - When potential and actual insider threats are identified, prompt and efficient intervention is necessary—individuals should be considered on a continuum and based on the circumstances, their access to critical corporate assets reviewed and adjusted accordingly while an investigation is ongoing (also, consider

solutions that include restricted access and different job roles–versus outright job dismissal).
        - Implement an effective code of conduct reporting program with high integrity towards the protection of employees that report (i.e., whistleblowers).
        - Have a robust logical and physical logging program, and response to detected anomalies, process in place– especially important given the increase in remote work.
        - Ensure that front-line employees are engaged as human sensors–they see the day-to-day operational environment and are well placed to report concerns.
        - Conduct a routine review of the insider risk register– establishing a centralized register is part of the solution, and routine analysis to identify and remediate gaps is another process that should be implemented for a proactive risk management posture.
- Near and long-term challenges and opportunities to insider risk management include:
    - Insider risk management is still not a well-defined program area with supporting organizational roles. Additionally:
        - There is still a gap between cyber and physical security organizational structures and integrated operations;
        - Organizations continue to experience ongoing challenges in the employee vetting process (pre-/during/post-employment);
        - Building awareness with the wider employee base, and business areas that are under increased risk from insider threats, based on the evolving threat environment; and,
        - Additional federal legislation and mandatory standards in InRM applied to the public and private sectors involved in critical infrastructure protection may assist organizations to provide additional focus and resourcing.
    - Increased remote work–how to enhance assurance that insider threat activity is being detected and responded to in a timely manner?

        - This includes increased remote interviewing for employment–how to ensure that the person being interviewed is the same individual who will be arriving to work?
        - Ensuring that logical access to the network and information assets from corporate devices are occurring within countries that are compliant with organizational policies.
    - Ensuring a consistent training and awareness approach, and enforcement standards for employees, as well as third-party contractors.
        - Building meaningful internal awareness programs to cultivate security champions and offer positive incentives to employees to actively onboard policy compliant behaviours.
    - The role of artificial intelligence (AI) to help with the detection of potential insider threats in the future?
        - Advancing from the current model of detection based on data aggregation gathered from past known compromises to the use of algorithms that are created based on models of actual human behaviour under different circumstances of personal and organizational stressors.
- Cyber-security regulation, information sharing, and intelligence gathering
    - Bill C-26, *An Act Respecting Cyber Security* (ARCS) is meant to protect Canadians and bolster cyber security across federally regulated finance, telecommunications, energy and transportation sectors.
        - Part 1 will introduce amendments to the *Telecommunications Act*
        - Part 2 will introduce the *Critical Cyber Systems Protection Act* (CCSPA)
            - The CCSPA will introduce a regulatory regime to protect national security and the safety of Canadians, and is meant to increase cyber threat information sharing.

        - The obligatory reporting of cyber security incidents will include any incident (act, omission, or circumstance) that interferes, or has the potential to interfere with, the confidentiality, integrity, or availability of critical cyber systems—including compromises caused by insider threats.
    - There are continued attempts originating on the dark web to recruit via underground job boards, employees with privileged access to organizations' critical systems and information.
    - Small and medium business are as vulnerable as larger enterprises and critical infrastructure, to insider threats.
        - In-house cyber-intelligence expertise to detect insider threats may not be sustainable for smaller organizations; service offerings from cybersecurity service providers may be able to fill the capabilities gap.
    - There are requirements for additional information sharing between critical infrastructure organizations, as well as determining how to best leverage third-party cyber-security provider services for organizations and within existing information sharing initiatives.