DEFENCE AND CRITICAL INFRASTRUCTURE INSIDER RISK WORKSHOPS

Summary of Insights

Australian Insider Risk Centre of Excellence (AIR COE)
Canadian Insider Risk Management Centre of Excellence (CINRM COE)

Washington D.C.

AIRCOE@cybercollaboration.org.au
CanadianInsiderRiskManagementCOE@carleton.ca

FIRPA
FVEY Insider Risk Practitioner Alliance

AUSTRALIAN Cyber Collaboration Centre

AUSTRALIAN INSIDER RISK CENTRE OF EXCELLENCE

CANADIAN INSIDER RISK MANAGEMENT CENTRE OF EXCELLENCE

Sponsored by DTEX

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.

Key Outcomes – Defence and Critical Infrastructure Workshops

- There was universal support from participants to support the centralized COE hub concept, as an intersection of academic, private, and public organizations' mutual interests in insider risk management (InRM)– engagement and development of comparable COEs in New Zealand, the Unted Kingdom, and the United States should be part of the focus of activities over the next year.
    - There was general consensus that funding and in-kind support should be channeled into the COEs to pursue centralized initiatives on behalf of the InRM community of practitioners. This could include standards, best practices, training, workshops, and conferences.
    - The provision of additional support to the COE model to develop national InRM communities of practice and promote an industry view to the national government and regulatory agencies will allow the industry to ensure that their views are proactively represented and incorporated into future national legislation and critical infrastructure protection initiatives. It was underscored that this is even more

important when it is considered that the present 10 per cent of industry with formal InRM programs is expected to increase to a 50 per cent implementation rate by medium to large enterprises by 2025. Finally, it was noted that those U.S. organizations in the workshops likely represented the 10 per cent of present-day industry that was cited in a Gartner 2023 report.

- There is a greater need to share strategic insights across the industry of InRM practitioners, as well as stand-up centralized repositories of information for organizations' tactical and operational purposes as related to enhanced risk modelling and mitigation.
- A Taskforce will be established, led by the Canadian Insider Risk Management Centre of Excellence (CINRM COE), to establish insider risk management guiding principles for program standards and taxonomy for the Five Eyes insider risk practitioner community.
- A second Taskforce will be established, led by the Australian Insider Risk Management Centre of Excellence (AIR COE), that will examine the present state of training, certificates and certification for insider risk management in the Five Eyes and propose a potential centralized training standard that could be undertaken and recognized by the Five Eyes insider risk practitioner community.

BACKGROUND – WORKSHOPS

FIRPA held its first event, led and supported by the Australian Insider Risk Centre of Excellence (AIR COE) and the Canadian Insider Risk Management Centre of Excellence (CINRM COE) in Washington D.C. on September 26.

The two five-hour workshops were divided into defense and critical infrastructure sessions, and included representatives from the national government, private sector, and academia from all Five Eyes (FVEY) nation-states (Australia, Canada, New Zealand, United Kingdom, United States) (See annexes A and B for the workshop agendas).

During facilitated discussions with industry experts, several insights were offered from insider risk practitioners concerning the present-day threat environment and considerations in the short- and long-term.

Defence Workshop – Key Takeaways

The defence workshop included a diverse group of individuals present from a range of agencies including law enforcement, national security and other federal departments in the U.S., Australia, and Canada. The MITRE Corporation provided **research insights into human focused protective security that will be further shared through FIRPA COEs to the broader InRM community of practitioners**.

There are still significant opportunities within government to share more information between agencies. Additionally, it was **noted that there was a clear need to incorporate learnings from the private sector and sharing practices from within the public sector**, in particular the U.S. Department of Defence. Some general comments on the present threat and InRM environment included:

- **Malicious solicitations tactics are evolving**, with traditional phishing email campaign training no longer effective at mitigation accidental insider threats.

- There is a **need for InRM programs to have a greater impact on the climate of an organization** to enable practical risk mitigation activities to evolve and shift complacent organizational cultures.

- There is a **greater need to better understand the reporting behaviours of employees** within the public sector.

The following insights and opportunities were generated from practitioners during the discussion at the workshop:

- **Sharing of cases** across agencies / departments is very poor. Insights are far too siloed which limits progress in insider risk mitigation knowledge.
    - This confirms that there is a need for a codified and tagged centralized repository of insider risk data–similar to threat intelligence feeds.
    - The sharing of data will also assist organizations with the establishment of a lifecycle of insider risk to highlight how and when

to intervene with mitigations that are scaled to specific incident circumstances.

- **Limited clarity** about where the “buck stops” / who is in charge when an insider case occurs. There is often no playbook to follow unless a large-scale breach occurs.

- **Technological interventions** are largely proven but the opportunity for improvement in interpretation techniques on the human side is significant (i.e., screening, analysis, and assessment).

- Insider risk **understanding at the executive level** remains mixed and positioning better within business risk can lead to better outcomes.

- **Deception detection in humans** is very difficult. There is very little understanding of deception as related to individual belief sets with limited data to understand this aspect.

- **Social identity** alignment for employees as linked to the organization they work for remains hard to measure; what is more certain is that dissatisfaction increases insider risk potential.

- **Mental health and well being are not only clinical problems**, but it remains unclear which part of the employee experience is addressing this area within organizations. This impacts to what extent that insider risk management practitioners should play an active role in these functions within an organization.

- The number of organizations with **intentional outreach initiatives** to provide optimized and consistent offboarding is growing and this is very positive. The workshops shared tangible examples of programs engaging up to six months after offboarding having a tangible effect on positive ex-employee sentiment.

Critical Infrastructure Workshop – Key Takeaways

General threat environment. There were several areas of present focus and concern in terms of insider risk management, along with several recommendations:

- **Chinese nation-state talent recruitment program** (as indicated by a U.S. Fortune 500 IT and telecommunications firm).
    - Awareness programs outlining to employees why they may be a target are crucial.

- **Applied research** has become very important to advancing the mission of insider risk management (as indicated by a U.S. Fortune 500 technology firm).
    - Anomaly detection is only one aspect of identification—gathering and applying human behaviour from real case data is more important.

- **Insider threat is a unique issue** that is different, and is not cyber security, physical security or fraud (as indicated by a U.S. defense industrial base research firm).
    - There is a need for more dedicated training.

Practitioners then discussed what seems to be working in terms of risk mitigation, and some lessons learned included:

- **Having executive buy-in for insider risk management** means using the language of enterprise risk (and consider that structuring updates along industry frameworks may result in limited buy-in (i.e., NIST CSF) (as indicated by a U.S. defense industrial base research firm).
    - Insider risk is not a separate enterprise risk—it is part of the narrative on business focused fraud risk, market risk, and other potential instabilities—what does the Board care about?

- **Employees are not good or bad**—and not all policy-violations have to result in job dismissal (as indicated by a U.S. Fortune 500 banking firm).
    - Apply zero trust IT principles and change employees' job roles if required—limit access to critical and sensitive areas; even in highly regulated industries.

- **Western security frameworks will not work** for multi-national organizations operating in countries where the state has absolute authority to coerce and solicit privileged access and sensitive corporate data from employees (as indicated by a U.S. Fortune 500 banking firm).
    - **For countries of concern, add regional teams to foster awareness and training related to suspicious activity reporting.**

- **Why aren't employees reporting?** Research on organizational commitment and loyalty is not clear, and has never been applied in an insider risk context (as indicated by a U.S. defense industrial base research firm).
    - … but it is beginning, CINRM COE has a study that is being peer-reviewed and will be published soon, and touches on the concept of bi-directional loyalty between employers and employees.

- **More collaboration and more and data sharing** on real use cases and standards (as indicated by a U.S. technology firm).
    - FIRPA task force will focus on a common framework approach, guiding program standards approach—industry driven to be proactive in the potential of increased regulations in the near-term / The CINRM COE highlighted that it is in process of launching a centralized insider threat dataset with a taskforce of several Canadian public and private organizations, which led to the a discussion on how can the practitioner community-at-large use the centralized COE conduits more effectively?
    - Having a common InRM taxonomy would help assist the private sector—COEs could be instrumental in promoting centralized standards—**by the InRM community for the InRM community**. National regulators could build evaluation and assurance programs based on these standards.

- How to build or enhance InRM programs in **organizations with explicitly stated high trust cultures** (as indicated by a U.S. Fortune 500 energy and utilities).
    - Need to communicate the program mandate and approach to senior leadership and the executive routinely; a trust but verify approach.

- **More research is required** – Research indicates that individuals' attempts to evade detection controls are based in part, on the perception of distance from a main office (as indicated by a U.S. defense industrial base research firm).
    - Limited study on the variances between insider threat activity in the office, remote work (nationally and internationally), and how the perception of monitoring controls in different contexts affects threat activity.

- **A tool is not a program** – There is a widespread fallacy that still exists that a SIEM or a UEBA tool is the solution to an insider risk program (as indicated by U.S. Fortune 500 technology firm).
    - Organizations need more help setting up governance, policies, data identification, and use case development.
    -
- Artificial Intelligence (AI) **has promising applications** for InRM threat and risk modeling and detection (as indicated by a U.S. Fortune 500 manufacturing firm).
    - More data from real use cases is required to provide greater variation in different scenarios to allow a more accurate AI application.

ANNEX A – INSIDER RISK WORKSHOP FOR DEFENCE

Hosted by the AIR COE and the CINRM COE

Insider Risk Workshop for Defense | September 26, 2023

A collaborative, open-table workshop to uplift Insider Risk programs.

Hosted by Matt Salier, CEO of the Australian Cyber Collaboration Centre, facilitated by:

• Dr. Justin Fidock, *National Security Program Leader,* Australian Defence Science and Technology Group
• Dr. Deanna Caputo, Chief Scientist for Insider Threat Capabilities, and a Senior Principal Behavioral Psychologist, MITRE

WORKSHOP AGENDA:

1000 – Introductions and setting the scene

1030 – Lessons from our Insider Risk programs

1140 – Summarize key insights

1200 – Lunch Break in Le Sel, 1st floor

1300 – Insider Risk programs in 2030

1440 – Summarize possible next steps

1500 – End Workshop

Government Insider Risk Programs – Current & Future Best Practices

Join Dr Justin Fidock from the Australian Department of Defence, Defence Science and Technology Group (DSTG), and Dr Deanna Caputo from The MITRE Corporation, in exploring current best practices for Insider Risk programs, and considering what best practices might look like in 2030. Justin will briefly set the scene by describing a new DSTG research program seeking to enhance protective security resilience. Deanna will describe a collaboration with DSTG that has surfaced a range of Applied Research Capability (ARC) areas of great relevance to improving practices. Participants will then be invited to share what practices and interventions are working, what didn't work, and what others can learn from our efforts.

Our protective security posture and practices necessarily need to evolve in response to threats, risks, opportunities and evidence. With this in mind, part 2 of the workshop will consider what might the insider threat, risk and opportunity landscape look like in 2030? How have we drawn upon scientific evidence to inform how our posture and practices have evolved in response to this landscape? To help focus the exploration, we will first develop a small number of plausible scenarios, such as:

- How might AUKUS nations be exploiting developments in AI and Autonomy in support of enhanced management of insider risk?
- How might our competitors be exploiting developments in AI and Autonomy to increase insider risk?
- With the substantial increase in insider risk management, how are we drawing on technology and scientific evidence to transform how we build and run effective insider risk programs?

Once we have developed a small number of plausible scenarios, we will consider how we could mobilize government, industry, academia and international partners to achieve a transformation in Insider Risk programs. In doing so we will consider such questions as:

- How can collaboration help to drive transformation, and what role could FIRPA play?
- What changes do you believe are needed in practices, culture, training, continuous assessment, policies, and technologies to facilitate transformation?

In the final part of the workshop we will summarize key outcomes to share with the wider FIRPA audience and identify next steps.

ANNEX B – INSIDER RISK WORKSHOP FOR CRITICAL INFRASTRUCTURE

Hosted by the CINRM COE and AIR COE

Insider Risk Workshop for Critical Infrastructure | September 26, 2023

A collaborative, open-table workshop to uplift Insider Risk programs.

Moderated by Mohan Koo, Co-founder and President of DTEX Systems,
Hosted by Victor Munro, Executive Director Canadian Insider Risk Centre of Excellence and Rachael Hamilton, Strategic Lead Australian Insider Risk Centre of Excellence; supported by:

- Dr. Clark Smith, Head of Engineering and Architecture for Cyber, Citi
- Melissa Cardiello, Global Head of Insider Threat and Security Operations, Verizon
- Dr. James Doodson, Insider Threat Group Lead, MITRE Corporation
- Shawn Thompson, Head of Global Insider Risk Services, Mandiant/Google
- Paul Patty, Risk Specialist, BAE Systems Australia

WORKSHOP AGENDA:

Morning Workshop

1000 – Introductions and Setting the Scene
1015 – Lessons from our Insider Risk Programs
1145 – Summarise Key Insights

Lunch Break

1200 – Lunch Commences
1255 – Return to Workshop

Afternoon Workshop

1300 – General Discussion (per notes on page 2)
1415 – Summarise Key Insights
1430 – Formulate Action Plan
1500 – End Workshop

Ideas for Workshop discussion:

- Identifying and addressing the most common gaps and obstacles for insider programs – consider the following categories:
    - Government/industry policy (including executive orders/mandates/regulations)
    - Executive-level sponsorship/governance
    - Issues related to Human Resourcing (including program leadership)
    - Allocation of sufficient program budget
    - Appropriate use of tools and technology (including AI and ML)
    - Enterprise-level measures of security posture
    - Defining and communicating the types of insider risks (risk vs threat) and the need for a universal language/framework?
    - Effective engagement strategies for different stakeholder business units
- What initiatives do you have underway that are showing positive dividends in addressing insider risk?
- How can we drive more 'pro-active' support for these programs vs 're-active' executive support following an insider incident?
- How can we implement a best practice approach for sharing 'early warning behavior indicators' for malicious and non-malicious insider risks/threats within a trusted forum (such as FIRPA)?
- How can better collaboration help to close the gaps – what role could FIRPA play in overcoming program obstacles?
- What initiatives can we adopt for 'breaking down silos' across Defense and industry?
- What are some of the key differences between Defense/Intelligence and Commercial sector Insider programs – how can we benefit by improved sharing via Public-Private partnerships?
- How should Nation State actors and foreign interference be prioritized within both Federal and Critical Infrastructure insider programs?
- Which Critical Infrastructure industries and entities are most at risk today? How can the FIRPA community help to drive maturity for these entities?
- What is lacking from the vendor community today and how can we influence change?
- How can we ensure that FIRPA is truly inclusive in its approach while only permitting 'trusted' entities/individuals to participate?
- How are organizations overcoming employee complacency and strengthening organizational bonds (e.g. NITAM "Bystander Effect")
- How can we collaborate to foster insider risk management training standards across the FVEY community?
- Is the over-simplification of high-profile cases (e.g. unclear distinction between whistle-blower/malicious/unintentional behaviors) leading to confusion for program operations?
- Third Party Insider Risks – how can we get a better handle on contractors and supply chain where risks are prevalent? (This topic needs to be considered with both customers and suppliers in mind)