APPLYING INSIDER RISK MITIGATION: CONTEMPORARY ISSUES

Date: July 20, 2023

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On July 20, 2023, Victor Munro, Executive Director of the Insider Risk Management Centre of Excellence, presented on the contemporary issues surrounding the field of insider risk management. The presentation focused on three significant areas: 1) the nexus between whistleblower protections and insider threat management; 2) the balance of mitigating threats without compromising; and 3) the post-COVID impact on threat vectors and role of artificial intelligence in threat mitigation and organizational culture. The presentation was followed by a question-and-answer period with questions from the audience and CASIS Vancouver executives. The key points discussed were technical/behavioral indicators related to at-risk employees and distinction between intentional and unintentional threat behaviors.

NATURE OF DISCUSSION

Mr. Munro's presentation provided an overview of the state of insider risk management in the national security sphere by addressing the current industry challenges related to managing insider threats in medium and large enterprises in Canada. He stressed that a holistic cultural change was necessary to reduce corporate stigma around the issue of insider threats which can regard any form of feedback relating to insider threats as suspicious in nature, increasing distrust amongst employees. Mr. Munro suggested that Canadian-specific industry standards were necessary to gain insight on trends involving insider threats in Canadian organizations. He stated that improving corporate perceptions of insider threat management programs was also a key objective towards enforcing a positive culture towards whistleblowers.

BACKGROUND

Mr. Munro's presentation focused on three key areas linked to mitigating insider threats: the connection between whistleblower safeguards and insider threats; the balance in mitigating threats whilst preserving organizational culture; and the role of artificial intelligence and machine learning in threat mitigation post-COVID.

Mr. Munro stated that it is important for organizations to establish a proper feedback mechanism and understand the distinction between whistleblowers and insider threats so that they don't unjustifiably sanction and conflate those that have noble intentions with those that have malicious intentions. Using the case of Edward Snowden as an example, he queried whether Snowden could be considered either a whistleblower or an insider threat. Although an extreme case, he exemplified the significant events that could arise within organizations when there is not a well-defined and distinct whistleblower system in place. In Canada, the historical issue of whistleblowers raising concerns related to insider/counterintelligence threats has been a rich one. Over the past 15 years, the Canadian insider threat environment has been rife with all different types of insider threats and threat actor motivations. However, the intersection of whistleblowing and insider threats has been particularly significant in the national security sphere where data leaks, both intentional and unintentional, have the capacity to cause great harm on a wider scale. Intentionally malicious leaks, as seen in cases such as the Cameron Ortis affair (of which all details are still to be disclosed) and 2022 Freedom Convoy, can be considerably more transparent than unintentional leaks. However, use cases involving unintentional leakage of information are more significant as they can be used to inform whistleblowing systems, tailoring them in a manner that leads to employees raising their concerns about insider threats appropriately. A calibrated system can alleviate employee concerns of systemic racism and make them less likely to view higher management as obstinate.

Reports, such as those by the intelligence review committee, suggest that there are significant national policy gaps pertaining to whistleblower protections in comparison to the U.S. Surprisingly, despite the fact that Canada has also dealt with data breaches on the level of the Snowden scandal, both the U.S and Canada have taken different measures in risk mitigation. While the U.S government issued a Presidential Executive Order that mandated the creation of insider threat management programs agency-wide, Canada has chosen to implement relatively minor formal federal government policy changes in comparison, opting to initiate best practice guidelines and use gap-assessment tools instead that are outwardly directed towards critical infrastructure protection and industries that are federally regulated. Mr. Munro asserted that greater commitment through a whole-of-government approach towards threat mitigation is necessary by the government, especially when it comes to legislative gaps pertaining to whistleblower policies. When developing a program, a dedicated program, at its base, must define the concepts of insider threats, and their types, as well as insider risks. Policies, programs, and operations to detect, investigate, and respond must ultimately be tailored to these definitions. Following this, the next stage would be to integrate the program with existing policies so that different teams can conduct different functions depending on whether the anomaly has been classified as a whistleblower or insider threat.

The Center of Excellence's research, in conjunction with the Canadian finance sector, found that insider risk management should be thought of as a change management issue, otherwise it can lead to an uncooperative organizational culture that is rooted in suspicion. Dedicated programs must be proactive and transparent, underscoring the need for managers to communicate on the benefits of their program in a clear and concise manner to their employees so that there are no misunderstandings. However, this must be coupled with a positive workplace culture that can incentivize employees to communicate their concerns. Currently the COE's recent research shows that employees are mistrustful of employers and their insider risk programs, a factor that is leading to complacency and a subsequent lack of usage of various internal reporting mechanisms. Thus, this demonstrates the importance of effectively communicating the functions and purpose of an insider risk management program. A program that reinforces positive deterrence and culture, and is holistic in nature, can raise its success rate by maintaining the trust & cooperativeness of the workforce that are subject to it, especially those demographic segments that may be vulnerable to racial profiling. This is in stark contrast to a traditional security program that emphasizes negative deterrence through monitoring, restrictions, and sanctions.

In terms of big data techniques, Mr. Munro stated that the increasing rate of insider threats in organizations could be mitigated through the use of artificial intelligence, namely machine & deep learning techniques that provide enhanced detection and response that go beyond human operator intervention. Through use cases involving insider threats, machine and deep learning systems known as User Entity and Behavioral Analytics systems can quickly find patterns, conduct statistical regression to analyze, indicate probability and identify anomalous behaviors. In addition, transplanting cybersecurity frameworks such as the cyber kill chain, MITRE Enterprise ATT&CK framework can be necessary in threat modeling the Tactics, Techniques, and Procedures (TTPs) of threat actors as it applies to the field of insider risk mitigation. A solid framework can provide justification for investigative actions as well as risk identification. Ultimately, technological tooling and data modeling must take into account various considerations related to data centralization. Level of physical security convergence, baseline behavior, the minimizing of false positives, and contextualizing risk are key factors towards triaging events and establishing investigative priority, while balancing the privacy of the one facing scrutiny.

Finally, Mr. Munro expanded on various gaps related to challenges facing the industry. The first is the lack of communication around insider threats within the organization due to stigma around the issue. De-stigmatizing the issue of insider threat behavior within organizations will make organizations more comfortable towards addressing the issue in a frank manner. In addition, it will also lead to greater access to different types of data that could help remediate the phenomena. In terms of research gaps, anonymous research reports have largely been generalized to the North American context leading to a lack of information around frequency and level of improvement or deterioration. In order to address the aforementioned issues, CoE has dedicated itself to raising awareness on the issue by engaging in research, normalizing discussions of insider risk management, and building a wider public and private community at the same time. Through its increasing social media presence, CoE has also established cross-industry links as well as international ones. For formalized ventures, the CoE is a part of a three-eyes network which leverages public and private connections within the five-eyes to determine information-sharing arrangements, research project initiatives and training opportunities.

Question & Answer

What are the main motivations and TTPs of malicious insiders, and what are ways to differentiate between intentional and accidental insider behavior?

The underlying motivation was the major precursor to differentiating intentional from unintentional behavior. The pathway to harm also determined one actor's TTPs from another. This point in particular is significant because it leads to various UEBA solutions being considered by different organizations. A more varied UEBA system may lead to more opportunities to detect threat behavior; however, more research is needed to conclude this. It should be noted that there is no particular group of TTPs that can fully protect every organization; anomalous events will always challenge pre-established TTPS.

What are some behavioral and technical indicators that can be of assistance?

That managers can act as a line of defense, through frequent engagement and monitoring of activity, in halting a troubled employee's deviation towards threat-like activities. When establishing a baseline of user access, technical indicators can be used to determine a user's baseline of access. On the other hand, behavioral indicators can be more complicated to find, especially if the manager conflates a societal description of normal behavior with the description set out by the organization. In other words, a manager can mark an employee as a potential threat due to odd behavior when there is no reason to do so. Instead of profiling in this manner, managers should engage with their employees that may be under extreme stress, which can lead to their behavior falling outside the norm. Regular engagement and contextualization of indicators can give management a better idea of the state of the employee's mindset and whether further escalation is warranted based on continuing patterns of behavior.

KEY POINTS OF DISCUSSION

- A proper feedback mechanism in conjunction with an organizational culture that is holistic and positive deterrence-based, and in conjunction with a well-thought out change management strategy, can significantly increase the success rate of dedicated insider threat management programs.
- Canadian whistleblowing legislation is woefully inadequate and insider risk management requires a whole-of-government approach, similar to the actions undertaken by the U.S federal government under Obama Executive Order 13587.
- User Entity and Behavioral Analytics systems can quickly find patterns, utilizing statistical regression to analyze, indicate probability and identify anomalous behaviors. Their data can generate use cases of insider threat behaviors.
- Transplanting cybersecurity frameworks such as the cyber kill chain, MITRE framework can be necessary in threat modeling the Tactics, Techniques, and Procedures (TTPs) of threat actors as it applies to the field of insider risk mitigation. A solid framework can provide justification for risk identification, events triage, and further investigative actions.

- De-stigmatizing the issue of insider threat behavior within organizations will make organizations more comfortable towards addressing the issue in a frank manner. In addition, it will also lead to greater access to different types of data that could help remediate the phenomena.

FURTHER READING

CASIS-Vancouver. (2018). Cyber Security in an Information Warfare Age. *Journal of Intelligence, Conflict, and Warfare, 1*(2), 105–112. https://doi.org/10.21810/jicw.v1i2.652

Gratton, P. (2021). Intelligence Challenges of the Data Rich World. *Journal of Intelligence, Conflict, and Warfare, 3*(3), 76–79. https://doi.org/10.21810/jicw.v3i3.2580

Prox, R. (2023). DATA & INFRASTRUCTURE SECURITY: THE RISK OF AI ENABLED CYBER ATTACKS AND QUANTUM HACKING. *Journal of Intelligence, Conflict, and Warfare, 5*(3), 117–121. https://doi.org/10.21810/jicw.v5i3.5179

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University
Available from: https://jicw.org/