Mission First, People Always: Three Ways to Elevate Your Insider Threat Program Using Protective Intelligence

Ryan Matulka

Mission first, people always. This statement, often used in the military, encapsulates the tension between mission accomplishment and its potential human costs. Likewise, reducing insider risk and mitigating threats from organizational insiders can be a daunting task complicated by tradeoffs. Some organizations attempt and struggle to establish effective insider threat programs, challenged to not only obtain the buy-in of their people, but also to achieve a modicum of effectiveness.

There are common reasons these programs may fail to launch or under-deliver: misunderstanding, reactivity, and diffusion of effort. Threat and risk deterrence, detection, and mitigation programs are frequently perceived as adversarial in nature or overly invasive. "Big Brother" is watching me and wants to fire me. This is exacerbated by euphemistic program names which may seed cynicism and erode trust. Often sold as a "proactive" security, an audit of actual insider threat hub practices may reveal an exclusive focus on reactive incident response. We are categorizing what has already happened. When the specialized capabilities of the insider threat team are directed towards more common security matters lacking a clear insider nexus, it will likely reduce effectiveness in their primary domain. Organizations reduce bias in results, tunnel vision, and undesirable outcomes by effectively employing all assets in their intended manner.

> **"Prioritizing one group's interests or discounting another's too heavily is a blueprint for failure. Common ground between internal stakeholders can be achieved by tailoring the insider threat program activities to support the top priorities of the organization.**

RYAN MATULKA

Ryan Matulka is Senior Manager of Cyber Threat Intelligence and Insider Threat at Pacific Gas and Electric Company, one of the largest utility companies in the United States. There he built the company's first insider threat program from scratch. Previously, he served in the U.S. Army as a Special Forces Officer, Unconventional Warfare expert, and master planner responsible for advising and leading foreign and joint military forces. Ryan is a graduate of the United States Military Academy at West Point. He earned an MBA from the UCLA Anderson School of Management and a Graduate Certificate in Cybersecurity Incident Response from the SANS Technology Institute.

Given the human and operational resources at stake, leaders and employees are right to ask tough questions about their insider threat programs.

- **Whose interests does the program serve?** Does it serve investors, customers, employees, or a combination of all of them?
- **What is the goal of the program?** Is the desired outcome to find and mitigate threats, or to keep the company safe and secure? Does the first result in the second?
- **When do we intervene?** Should we intervene in a personal matter if the company has yet to be harmed? What is our duty to act if no policy has been violated yet but there is evidence of risk? Beyond our duty, do we have a responsibility to our people?
- **How do we balance protecting the company with protecting employees?** Is this a zero-sum game between the employer and its employees?
- **Do we trust employees?** Are employees the company's greatest asset or its greatest vulnerability? Or both?

The discussion around these questions is likely to reveal the internal tradeoffs between security, risk, and business objectives inherent to a complex organization. Prioritizing one group's interests or discounting another's too heavily is a blueprint for failure. Common ground between internal stakeholders can be achieved by tailoring the insider threat program activities to support the top priorities of the organization. As such, striking this balance between security and functional business perspectives is paramount for insider threat leadership.

> **Protective intelligence teams do not wait for precipitating events to act. Instead, they take the initiative to analyze past incidents, recognize emerging indicators, reduce vulnerabilities, and improve resilience.**

Despite the abundant programmatic hazards, there are clear models for success, such as a people-centric, protection mindset. According to the Cybersecurity and Infrastructure Security Agency (CISA), the core principles of successful insider threat mitigation programs are "***promoting a protective and supportive culture***," "***safeguarding organizational valuables***," and "***remaining adaptive***." These focal points in CISA's Insider Threat Mitigation Guide foster clear thinking about the most important feature of insider threat programs – the protection of people and organizational interests.

Safety and protection are foundational individual needs and are universally desirable. In the enterprise context, they are essential elements of responsible management. Stated as operating tenets of an insider threat program, these protective principles may be more likely to achieve buy-in than negatively-framed objectives such as "deter threats" or "detect malicious behaviors."

The protective intelligence discipline, like that practiced in the executive protection context, offers a transferrable and repeatable framework to achieve CISA's core principles for successful insider threat programs.

What is Protective Intelligence?

Security practitioners will not find a uniform definition of protective intelligence in professional bodies of knowledge. At a basic level, protective intelligence is simply an investigative and analytical method to proactively identify, assess, and manage threats. There are however several characteristics which set it apart from other security specializations.

The defining attribute of protective intelligence tradecraft is a continuous and ongoing effort to mitigate potential threats well before any adverse effects are realized. Protective intelligence teams do not wait for precipitating events to act. Instead, they take the initiative to analyze past incidents, recognize emerging indicators, reduce vulnerabilities, and improve resilience. Protective intelligence requires a different mindset than some other security disciplines.

Protective intelligence is most frequently applied to protecting high-profile individuals known as "principals," but it need not be limited to this. A compelling question for insider threat professionals is how to expand the beneficiaries from specific individuals to what CISA calls "organizational valuables" – i.e., groups of people, information, intangible assets, physical property, and by extension, the shared interests between groups of stakeholders.

Let's consider how to achieve a protective insider threat culture by examining three key ideas taken from protective intelligence and how they can be applied to insider threat mitigation.

Idea #1: Embrace the Intelligence Cycle

Advances in technology and the behavioral sciences have created a world where insider risk is reasonably foreseeable. Business and security technologies, with identity-based logging, monitoring, and auditing – standard in any modern enterprise – has enhanced the observability of behavioral indicators that would have been undetectable a few decades ago. Furthermore, researchers have developed and tested Structured Professional Judgment (SPJ) instruments which can improve the assessments of security practitioners when applied to individual cases. No one can forecast human behavior, but the use of comprehensive data and tested behavioral models raises the bar for what insider threat programs can achieve. With the substantial insights generated by the marriage of technology and expert human judgement, organizations have a duty of care to proactively manage insider risks.

Protective intelligence, guided by the intelligence cycle, is a way to carry out that duty of care. Intelligence methods are more suited to upfront, proactive work than the traditional "means, motive, and opportunity" investigative

approaches. Protective intelligence is not a substitute for investigations, rather they are complementary.

Protective intelligence starts with an intelligence requirement defined by a decision maker, whereas an investigation is predicated upon an allegation. Protective intelligence produces an assessment that may feed into the investigatory process. A completed investigation produces fact-based findings that can further inform intelligence requirements. Protective intelligence is future-oriented, whereas investigations focus on historical evidence. These subtle, but powerful distinctions put control back into the hands of protective intelligence specialists, allowing them to react less and protect more.

Figure 1. The Intelligence Process

Source: JP 2-0, Joint Intelligence

Idea #2: Elevate Analytical Thinking

The term "false positive," and other binary classifiers, have found their way into the insider threat lexicon, likely through the use of cybersecurity detection tools by insider threat teams. "False positive" means the misclassification of an object by a binary test with only two possible outcomes. Binary tests are appropriate for narrow applications with measurable and distinct criteria. Complex human behavior, on the other hand, should not be reduced to a binary test.

Using binary classifiers to describe human threats is an easy habit to form. Perhaps this is because binary tests can be automated or the terminology may imply precision and certainty. Caution is advised. If simple binary tests are normalized for insider threat practice, it may displace the laborious, but more relevant, expert assessments that require consideration of the totality of the facts. In its worst manifestation, binary thinking can overcome critical thinking. This may reinforce the natural tendency toward bias and cognitive shortcuts and become the acceptable path of least resistance. Lazy thinking is in direct opposition to CISA's first core principle, to build a protective culture. It can cause actual harm.

The management of cognitive bias is built into analytic tradecraft. Protective intelligence-based thinking strives to recognize and alleviate the errors that can creep into any analytical process. Protective intelligence analysts produce threat assessments based on the totality of the observable facts. When categorization of threats is required, it relies on scientifically-developed and tested SPJ instruments. These tools provide a defensible and repeatable way to make sense of large volumes of

evidence and case data. Cultivating a cross-functional team with diverse perspectives and recognizing the limits of one's professional experience and knowledge are two cognitive safeguards integral to Threat Assessment and Management, a key function of protective intelligence teams.

Protective intelligence requires its practitioners to acknowledge and describe uncertainties rather than simplify them through algorithmic and technological paradigms. Used appropriately, technology accelerates visibility and is a necessary part of any modern security posture. The most effective Insider threat leaders balance technological influences with both analytical and procedural approaches—and place human decision makers in the loop. The use of analytic confidence and estimative language to portray the natural ambiguity inherent in human behavior is more defensible than arbitrary and logical classifiers. Models and algorithms do not make decisions about people. People use the wisdom borne of experience and training to make decisions about people.

Idea #3: Reward Protective Outcomes

A protective intelligence approach to managing insider threat programs naturally facilitates a broader range of organizational responses to risk. In the protective intelligence model, success is defined as protecting the "principal" from harm, not

necessarily imposing consequences on a potential threat. Many insider threat hubs measure their success in terms of cases, investigations, and administrative actions. Discipline remains one of many tools available to management. However, if these are the only tools, there will be missed opportunities to create a positive organizational culture resultant from the most successful programs.

Building this flexibility can be accomplished by promoting the supportive side of threat assessment and management. This may include education, awareness, benefits, and services provided to subjects, victims, bystanders, and internal customers. Other noteworthy protective outcomes include remediation of vulnerabilities, creating awareness of threats, driving policy and procedural enhancements, and modifying behaviors through positive reinforcement.

Positive and negative incentives are not mutually exclusive. Both are useful risk mitigation tools and should be preserved as response options. But it is helpful to differentiate the influence of each through the framework of loss aversion. Discipline and adverse actions may be more likely to be perceived negatively by employees and by management. Even if a termination action is necessary and justifiable, should it be viewed as a "success?" It more likely to be viewed as a near-hit, a "cost," or a loss, depending on the circumstances and culture of the organization. On the other hand, outcomes where protecting people, data, and assets was the primary result, may be viewed as "wins" or as demonstration of return on investment (ROI), especially if the insider threat program is focused on the highest organizational priorities. Reframing the success criteria of insider threat programs may require effort to educate stakeholders, but the protective outcomes are more likely to catalyze human-centric stories which can better engage employees and the senior leaders alike.

"Reframing the success criteria of insider threat programs may require effort to educate stakeholders, but the protective outcomes are more likely to catalyze human-centric stories which can better engage employees and the senior leaders alike.

Lastly, thinking more broadly and inclusively about protection will help expand the mindset from threat to be more inclusive of risk. Consider a hypothetical situation where an employee is susceptible to coercion from adversarial foreign interests. The employee has not done anything wrong. There is no evidence of exploitation. They may not even be aware of their vulnerabilities. Security can highlight the potential bad outcomes, management can set expectations, and human resources can provide the necessary resources. This orchestration motivates a level of internal coordination that not likely to result from a narrower focus on malicious behaviors. The natural result of emphasizing protection will allow the company stakeholders to converge around their shared responsibility of protecting common interests.

Conclusion

These three ideas derived from the field of protective intelligence are useful for the insider threat discipline. They have practical and immediate benefits which may enhance performance and drive positive results. But also, they do more to contribute to a culture of support, trust, and safety than the necessary but grim work of finding and neutralizing threats. The modern organization and its insider threat program team have their work cut out for them. The mission is dynamic and complex. When they protect people first, everything else will fall into place.