INTELLIGENCE INSIGHTS

EXPERT INSIGHTS ON NATIONAL SECURITY DEVELOPMENTS

SEPTEMBER 2022

Background Paper: Insider Threat Program Naming Convention

PRESENTED BY INSA'S INSIDER THREAT SUBCOMMITTEE

INSIDER THREAT SUBCOMMITTEE

EXECUTIVE SUMMARY

Insider Threat practitioners have long debated whether there is, or should be, an official naming convention for Insider Threat Programs,[1] and whether an organization's choice of terminology affects its implementation. How a program is presented may adversely impact organizational culture/climate and influence how personnel view or support the program, which can ultimately determine its effectiveness.[2] Naming conventions or terminology highlighting threats could undermine an organization's goal to provide positive, supportive interventions (as opposed to punitive ones) that mitigate behavioral risks through employee assistance program referrals rather than disciplinary measures.

Program names and descriptions should align with an organization's mission, culture, goals, and objectives. Regardless of naming convention, leaders and/or responsible executives must have a firm philosophy that aligns with the broader strategic vision for the program. Furthermore, overall program characteristics should align with the naming convention; a program should not use "risk management," for example, if it does not integrate risk management principles.

The program structure and where it is house in an organization also affects its execution and way in which the workforce perceives it. In recent guidance for U.S. critical infrastructure organizations, the National Counterintelligence and Security Center (NCSC) wrote, "There is no need to call your program an 'insider threat' program. However, what your program is called and where it is placed can impact both its mission and image. If it is placed under security, it will always be viewed as a security program both by leadership and the workforce."[3]

Some stakeholders argue that these types of programs should use terminology (i.e., insider threat) that is consistent with language used in U.S. legislation, policy, and other government guidance documents. However, no single standard exists. The U.S. government has produced guidelines for federal government organizations and companies doing business with them, but no guidelines or principles exist to govern programs' design and execution in the private sector. More importantly, what governance does exist in the public sector does not explicitly mandate specific terminology. Considering diverging program constructs and a lack of authoritative principles for mitigating risks, a "one size fits all" approach is not likely to work. Rather than providing prescriptive guidance, this white paper seeks to inform the "insider threat" community, managers, leaders, and executives about how various labels might impact their programs' operations.

BACKGROUND

Before discussing terms used by these types of programs to communicate their goals and objectives, it helps to start with a generally accepted definition of "insider" and "insider threat" that applies to both public and private sector organizations.

In Executive Order (E.O.) 13587 of October 2011, President Barack Obama directed federal departments and agencies that work with classified information to establish insider threat programs. The E.O. also established an interagency National Insider Threat Task Force (NITTF) to develop government policy on insider threat deterrence, detection, and mitigation; develop minimum standards; and, assist agencies in implementing insider threat programs.[4] A year later, President Obama issued a memorandum setting National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs,[5] which provides guidance and definitions of terms needed to implement the E.O. With this overarching guidance, most government organizations established insider threat programs initially focused on protecting classified information and information systems that were heavily reliant on technical solutions.

While these documents clarified the focus of insider threat programs intended to protect government classified information, they did not provide broader definitions that could inform private sector entities not working in a classified environment. In 2015, INSA's Insider Threat Subcommittee convened government and industry experts to develop a standard definition of "insider threat" that would consider threats to the government, the national security industrial base, and non-defense-related commercial companies. This INSA Committee agreed upon the following definition of Insider Threat:

> The threat presented by a person who has, or once had, authorized access or knowledge to information, facilities, networks, people, or resources; and who wittingly, or unwittingly, commits acts in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace.[6]

For the purposes of this paper, we will define "insider" in a way that builds on the definition contained in the White House's "National Insider Threat Policy" and broaden it in a way consistent with INSA's 2015 initiative:

> A person who has (or had) authorized access (or knowledge) to any organizational resource to include personnel, facilities, information, equipment, networks, or systems by virtue of employment, detail, assignment, visit, affiliation, collocation, or contractual relationship.

Since these efforts to define and codify programs, best practices have matured and many organizations now focus on holistic prevention and intervention rather than the more traditional, reactive approach responding to events after they occur, or "right of boom." This more modern, "whole person" approach seeks to proactively detect behavioral indicators that have been found to reveal potential concerns before they devolve into incidents or crimes, also known as "left of boom." Some organizations have chosen to dedicate extensive resources to their programs, with investments in the areas of social/behavioral science, threat assessment, workplace violence, risk management, etc. There has also been

some discussion in the "insider threat" community regarding positive attributes/behaviors and how they might play a role in mitigation. This type of thought and scholarship is critical to ensure these programs are fair and balanced, while also considering the complexity of the challenge.

ALTERNATIVE TERMINOLOGY

Depending upon an organization's mission, objectives, and other factors as described below, various terms can be used to label or describe its program. This section examines several real-world use-cases and offers insight into the underlying rationale and perspective behind each naming convention. Illustrative examples of how actual programs demonstrate the notion of "one size fits all" don't apply here; varying missions, organizational culture, and even formal policies or regulations can influence how these programs are applied and how effectively they operate.

INSIDER THREAT/ INSIDER THREAT MANAGEMENT

The term "insider threat" is in wide use and is consistent with policies in place at practically all U.S. government agencies. While this promotes consistency, possible unintended consequences may be that the organization views its workforce as a threat. The term "threat" evokes the idea of malice, and an insider "threat" program may be focusing its attention on the management and mitigation of sinister insider individuals who harm organizations. Instead, the objectives of a program must be broader than just detection and mitigation of "bad actors" within an organization. Non-malicious (unintentional) insiders pose very significant risks through behaviors like careless handling of information and poor cyber hygiene. Moreover, best practices argue that in addition to user activity monitoring, periodic examination of organizational systems, practices, and culture should be performed to identify and correct organizational factors that can lead to an increase in the risks of both malicious and unintentional insider incidents.[7]

CASE 1: USE OF TERM "INSIDER THREAT PROGRAM"

ORGANIZATION TYPE	Domestic federal contractor with over 5,000 FTEs
CONTEXT	The decision to use this terminology was made based on the company's Facility Security Clearance designation. Management decided to align the program and its terminology with the NITTF and its Minimum Standards, EO 13587, and the National Industrial Security Program Operating Manual (NISPOM), among others.
BENEFITS	The program has benefited from using language consistent with the "official" terminology used by the Defense Counterintelligence and Security Agency and the Department of Defense, which oversee the company's compliance with the NISPOM, during audits, inspections, reviews, etc.
CHALLENGES	While the company's mission is security-oriented given its cleared government contracts, the organization did not consider company culture when deciding what to call its Insider Threat Program. As such, program managers frequently explain and defend the rationale behind the terminology when employees question whether the company trusts its workforce.

In this example, there was an obvious benefit in following "official" government terminology since the program's policies and milestones could be more easily defended and assessed to meet government-mandated objectives. However, the organization did not foresee challenges caused by workforce perceptions that insider "threat" program terminology is judgmental, harsh, and in conflict with the ideals of a supportive/trusting organizational culture.

INSIDER RISK MANAGEMENT

While "insider threat" typically connotes a narrower focus on individuals, use of the term "risk" tends to recognize the need for broader, more holistic programs that focus on actions and conditions (including individual behavior and organizational systems) that increase the risk of harm to organizational systems and assets. This use of the term "risk" emphasizes distinctions between (a) the malicious user who steals intellectual property (exemplifying *insider threat*), (b) a negligent user who inadvertently leaks sensitive information (exemplifying *insider risk*), and (c) a toxic organization that creates a work environment and culture that breeds both malicious and unintentional insider threats (exemplifying *organizational risks*).

CASE 2: USE OF TERM "INSIDER RISK MANAGEMENT PROGRAM"

ORGANIZATION TYPE	International company with over 100,000 FTEs in the information technology and management consulting industry.
CONTEXT	In establishing a formal program for the first time, company officials decided to use this terminology based on the firm's adoption of threat management models (e.g., Critical Path Model, Pathway to Violence, etc.); the belief that risk comes in different scales and scopes (risk = threat x vulnerability x consequence); and a decision that the need to pre-empt damaging employee actions – to move "left of boom" – required a broad risk management approach.
BENEFITS	A risk management approach enabled the organization to proactively identify risks instead of reacting to incidents. The program has benefited from being able to recognize potential indicators of insider risk and develop cross-functional responses and mitigation measures.
CHALLENGES	Required buy-in from senior officials throughout the organization that every incident involving an "insider" should be seen as "risk" to the organization. This meant Human Resources, Ethics, and other parts of the organization had to agree upon a clear delineation of roles and responsibilities in furtherance of the broader goal of managing risk. Some awareness and training was required to educate stakeholders on the difference between insider threat and insider risk.

In this example, it appears there was some benefit in using "risk" over "threat" because it allowed for the use of risk management principles and leveraging of common knowledge within industry. Similarly, organizations may face the challenge to align the program within an enterprise risk management office versus a security or legal function.

INSIDER TRUST/TRUSTED WORKFORCE

Like "insider risk," some organizations have chosen to use the broader term "insider trust" to highlight their program's focus on employee actions that increase the risk of harm to organizational systems and assets. For some, insider trust aligns with the popular "Zero Trust" cybersecurity model – which assumes harmful actors have already penetrated your organization – and provides some alignment with functional efforts by cybersecurity teams. Using "trusted workforce," or some adaptation, leverages the broader U.S. government effort to create a continuous vetting of its cleared workforce.

CASE 3: USE OF TERM "INSIDER TRUST/TRUSTED WORKFORCE"

ORGANIZATION TYPE	Financial institution with over 5,000 FTEs
CONTEXT	The consideration to use this terminology was based on Program alignment with the broader "Zero Trust" approach already employed by the Chief Information Officer (CIO).
BENEFITS	The program has benefited from aligning itself with broader defense-related programs; employees understand the "trust but verify" concept.
CHALLENGES	Some employees within the workforce articulated concerns that monitoring employees' trustworthiness suggests the organization "distrusts" employees.

In this example, it appears there were some benefits and challenges in using "trust" over "threat;" however, there is not significant data for a more comprehensive analysis of this approach.

COUNTER-INSIDER THREAT

Counter-insider threat was developed by the Office of the Undersecretary of Defense for Intelligence and Security (OUSDI&S). Like counterterrorism, "counter-insider threat" supports the philosophy that programs need an operational approach in execution and are not simply "policies and governance." Several DoD organizations have adopted this approach; however, no policy exists which dictates naming conventions for Programs.

CASE 4: USE OF TERM "COUNTER-INSIDER THREAT"

ORGANIZATION TYPE	Defense Department organization with over 350,000 FTEs
CONTEXT	The decision was based on the overarching shift within the DoD to change naming conventions from insider threat to counter-insider threa.
BENEFITS	The program has not experienced any benefits from changing its naming convention to align with OUSDI&S.
CHALLENGES	The program has not experienced any additional challenges from changing to align with OUSDI&S.

In this example, there have not been any obvious benefits or challenges in following official government terminology. However, it should be noted that other "counter" programs in government terminology – counterterrorism, counterintelligence, counterproliferation – seek to eliminate threats rather than mitigate them. Defense Department employees could therefore interpret a "counter-insider threat" program as one that seeks to eliminate employees who pose threats by punishing or terminating them rather than one that offers helpful resources – such as employee assistance programs – that mitigate risks through compassionate engagement.

C.A.R.E. PROGRAM

The Collaboration, Assessment, Resolution, and Education (CARE) terminology was recently adopted by a U.S. Government agency. The rebranding resulted from a six-month review by program stakeholders wanting to increase awareness and create an environment that promotes employee assistance before insiders become a threat to the agency.

CASE 5: USE OF TERM "C.A.R.E."

ORGANIZATION TYPE	U.S. Government organization
CONTEXT	The change resulted from a six-month review by program stakeholders wanting to increase awareness and create an environment that promotes assisting employees before they become a threat.
BENEFITS	The C.A.R.E. program aligns with organizational Core Values (Accountability, Integrity, and Reliability) and People Values (Valued, Respected, and Treated Fairly) while staying true to the underlying mission of "insider threat." However, the program has not experienced any benefits from changing the name of their program.
CHALLENGES	The program name does not clearly indicate the program's purpose, which could generate confusion about its role and create unpleasant shocks if employees discover on their own that the organization does, in fact, monitor employees' behavior. However, the program has not experienced any challenges from changing the name of the program.

CONCLUSION

Choice of terminology reflects an organization's culture and its approach to both enterprise risk and employee engagement. Labels that degrade employee trust and engagement can undermine morale, retention, and productivity. Employees are an organization's most valuable asset; they are also its best internal "sensors" to provide early warning of aberrant behavior and risk within the workforce. Consequently, strengthening feelings of mutual regard and responsibility between employees and their organization can mitigate insider problems while simultaneously promoting a cohesive workforce. Therefore, organizations should dedicate considerable effort to ensuring their choice of naming convention aligns with organizational culture, intent, and mission, and contemplate the strategic implications of choosing one name over another.

REFERENCES

[1] To avoid bias toward any one term, "insider threat" programs will be hereinafter referred to as "Programs."

[2] Salvador Ordorica, "How Language and Word Choice Can Affect Your Business," Forbes, September 30, 2021. At https://www.forbes.com/sites/forbesbusinesscouncil/2021/09/30/how-language-and-word-choice-can-affect-your-business/?sh=54d482cc3336

[3] Office of the Director of National Intelligence (2019). The National Counterintelligence and Security Center: Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective. Retrieved from https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf

[4] The White House, Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011. At https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.

[5] See "National Insider Threat Policy," at https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf. For the presidential memo transmitting the policy, see the White House, Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 21, 2012. At https://obamawhitehouse.archives.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand.

[6] Intelligence and National Security Alliance (INSA), Explanation of INSA-Developed Insider Threat Definition, November 2015. At https://www.insaonline.org/wp-content/uploads/2018/10/INSA_InsiderThreat_definition-Flyer.pdf.

[7] Scott Dust, and Elsine Van Os, "Why Hostile Work Climates Provoke Insider Risk," Psychology Today, online post, January 4, 2021. At https://wwwpsychologytodaycom.cdn.ampproject.org/c/s/www.psychologytoday.com/us/blog/what-we-really-want-in-leader/202101/why-hostile-work-climates-provoke-insider-risk?amp. See also Frank L. Greitzer, Jeremy Strozer, Sholom Cohen, John Bergey, Jennifer Cowley, Andrew Moore, and David Mundie. "Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies," 47th Hawaii International Conference on Systems Sciences (HICSS-47), Hawaii, 2014. At https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6758854.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this paper.

INSA MEMBERS

Sue Steinke, Peraton;
Insider Threat Subcommittee Chair

Julie Coonce, Premise;
Insider Threat Subcommittee Vice Chair

James East

Frank L. Greitzer, *PsyberAnalytix*

Kevin Mason, *Ally Financial*

Josh Massey, *MITRE*

J.T. Mendoza

Michael Crouse, *Forcepoint*

Dr. Rajni Goel, *Howard University*

Michael Hudson, *Clearforce*

Dr. Eric Lang

Michael Londregan, *Peraton*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor,
Director of Communications and Policy

Cassie Crotty, *Intern*

Emma McCaleb, *Intern*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S INSIDER THREAT SUBCOMMITTEE

INSA's Insider Threat Subcommittee researches, discusses, analyzes, and assesses counterintelligence and insider threat issues that affect government agencies, cleared contractors, and other public and private sector organizations. The Subcommittee works to enhance the effectiveness, efficiency, and security of government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private and academic sectors