ADVANCED CYBER SECURITY CENTER

Insider Risk Programs: Accelerating Around Human Factors

Cyber Risk Governance Executive Practice Guide

June 2024

TRUSTED NETWORKS.
ADVANCING CYBER STRATEGIES.

Key Themes

Human factors first: Insider risk programs are shifting from an IT focus to organize around human behavior, reflected in cyber and other sensors
While there’s no clear answer on the number of incidents – both malicious and non-malicious – made possible (or more powerful) by insider threats, estimates almost always land above 50%. The persistence of the challenge is made worse by the complexity of the solution. Traditional cyber controls must be combined with distinct strategies and defenses to be effective.

Insider risk programs require specialized approaches and different staff skills, according to MITRE’s Insider Threat Research & Solutions team. SOC analysts struggle to detect insider threats as insiders do not act like APTs. Key findings from MITRE’s research:

- Build a separate and distinct insider risk response teams that include insider threat specialists, IT, HR, legal
- Adopt a human-focused framework, use both cyber and non-cyber data to inform controls, IT data alone is inefficient
- AI-driven analytics may present opportunities to reduce costly false positives, although current data for anomaly detection are limited

Loyalty and culture matter as risk factors and predictors – both staff loyalty to the organization and the organization’s loyalty to its employees. In that context, it’s best to consider alternate names for insider threat and risk programs.

The goal should be deterrence, detection and mitigation, with strong documentation and appropriate exception processes.

MITRE Resources

Contact Us

(617) 485-1112

wguenther@acscenter.org

The Big Picture: Internal Threats Make Everything More Complicated

“Focus on limiting the damage any one person can do”

Avi Gesser, of Debevoise, framed the challenges organizations face in responding to the unique complexities of insider threats with systems and structures built for other tasks. Challenges are particularly significant in the early phases of investigation where it’s not clear yet that an insider is involved.

The priority should always be to limit the damage any single user can cause.

- This can be dialed up or down based on access to sensitive assets or systems
- Controls can start with simple steps: shortening session lengths, alerting on large volumes of data exfiltration, reducing number of session renewals permitted
- Restricting third party access in particular—every partner is a potential threat

Collaboration matters. Build a team of experts including insider threat specialists, IT, HR, legal.

Human-Focused Insider Risk Frameworks:

Effective Detection Combines Psychology and Cybersecurity

Broadcom’s Steve McLennan, an ACSC founder in his prior role as a senior Fidelity IT executive, presented a human-focused insider program framework organized around more traditional security and cybersecurity models as a common structure for HR, IT, cybersecurity collaboration.

Click here for the framework.

Understanding human behavior is the starting point

The framework combines traditional thinking about human motivation and operating environments with a psychology concept called the "dark triad", describing the three negative personality traits of narcissism, Machiavellianism, and psychopathy with common features.

- Humans are an inherent risk, regardless of individual intent
- The same person can experience new motivations or face new triggers
- A change in environment, including changes in access to more valuable resources, may produce changes in behavior

An effective insider risk program will observe behavior that maps to these negative personality factors. For example, a person lacking impulse control might consistently try new things, while a sense of entitlement might drive employees to disregard rules. ***Click here to read more about the triad.***

While using human behavior as a framework for broadscale insider risk analytics, MITRE research shows that applying personality characteristics to individuals isn't actually helpful, putting aside the legality and ethics involved.

With a human-focused framework, technology provides the tools

While human factors can inform predictions of insider risk, technology remains critical to managing an effective program. Available datapoints will expand, adding to the challenge to process all the information.

- Deep link analysis can help make connections across diverse information sources, from Observable Human Indicators (OHI) to traditional cyber and IT inputs
- Surveillance at key points (especially outbound traffic) is critical, although sometimes controversial when focused on individuals

Avoid the problem up front

Invest in intense background checks for sensitive positions.

ADVANCED
CYBER
SECURITY
CENTER

A Technology Firm Perspective: Why We Acted

“[illegible]ement has specific resources – like ransomware keys – they can help.”

> “Adopt Nike’s term: It’s Intelligence Risk – not an Insider Threat program.”

Three unrelated issues highlighted risks both “from” and “to” staff and launched development of the Intelligence Risk program:

- Risky staff at a major client have access to our data
- Privileged accounts were breached in the MGM ransomware attack
- Source code exfiltration was spotlighted at the RSA conference

Early collaboration with peers yielded an interesting lesson: Don’t call it an “Insider Threat” program – Nike’s “Intelligence Risk” program name was adopted to build internal support.

Quickly moving from ideas to action was critical for early success:

- A cross-functional working group brought cybersecurity, IT, HR, legal, and other ‘owners’ together
- A bias for action helped get the program off the ground early
- Prioritization yielded early results: identifying at-risk data sources

> “After one year, the program is very much a work in progress. We’re still looking for the most effective methods of detection and mitigation.”

A survey of participants confirms: Most report their Insider Risk Programs are still in progress, still maturing

Contact Us

(617) 485-1112

wguenther@acscenter.org

ADVANCED
CYBER
SECURITY
CENTER

Discussion Highlights: Use Of Surveillance Tools Differs Widely

> “Decrypting traffic puts a lot of trust on the line”

The underlying issue: How to enable employees to do their best, innovative work while appropriately monitoring systems and behavior:

- Decrypting outbound traffic was either seen as indispensable or off-limits, depending on mission and culture
- Use of CASB platforms such as Zscaler provides the option to select what is/isn’t decrypted for inspection

All tools, behavioral or technical, must be managed carefully and limited or enhanced based on context.

- Large orgs are investing in UEBA (User Entity and Behavior Analytics) to spot patterns and connections that can reveal risk earlier
- Broadscale “organizational” and “cultural” feedback are as important as cyber/IT sensors

The default should always be defensible surveillance that’s carefully focused only on what needs to be watched with robust documentation and appropriate exception processes.

About the ACSC

The Boston-based ACSC advances member cyber defense strategies through regional, national and global practice-sharing networks of industry leaders and provides professional opportunities for rising talent. This Executive Practice Guide reflects key takeaways, with proprietary information redacted, from this NDA-covered session.

Contact Us

(617) 485-1112

wguenther@acscenter.org