leidos

Eight components to develop a successful insider risk program

EXECUTIVE SUMMARY

While the term “insider threat” has garnered much recognition over the past few years, its applicability to commercial industry has not received the same acceptance as with the government sector. With the commercial industry facing an increasing number of attacks, and employees having greater access to information than ever before, this lack of acceptance can no longer remain the status quo.

When addressing insider challenges, the commercial enterprise should focus on managing the associated risks, taking into account the threats, related vulnerabilities, and affected assets. Further, the singular means of mitigation to address insider threats needs to be expanded to include the comprehensive array of risk treatments.

When implementing an insider risk program, it is necessary to take foundational measures to integrate both technical and non-technical elements for a truly holistic defense. Some steps include constructing proper governance and documentation, defining critical assets vital to business operations, establishing processes for implementation and execution, and ensuring transparent communication with ongoing training for employees.

Insider Risk Management: The Evolution of Insider Threat

In the wake of various high-profile leaks, human-enabled data breaches, and theft of corporate assets over the last several years, the "insider threat" topic has received much attention. The resultant threat-centric focus has not only spawned a thriving industry segment offering technical solutions to what is essentially a human-based phenomenon but also has frequently done so with only perfunctory nods to other fundamental security controls.

This persistent—some say ominous—threat characterization, and its associated rise to prominence through codification in an Executive Order, a Federal task force, and assorted US Government policies, has not often integrated well into existing risk management frameworks practiced within commercial industry.

Doug Thomas, a former counterintelligence advisor to the Director of National Intelligence and the President of the United States, stated, "National security, while funded and executed by the United States Government, is built by industry."[i] Along similar lines, the moniker of insider threat, as fostered by the Federal government, now needs a more relevant characterization for the commercial sector, evolving into more applicable frameworks and practices emphasizing risk management principles.

The Risk Equation

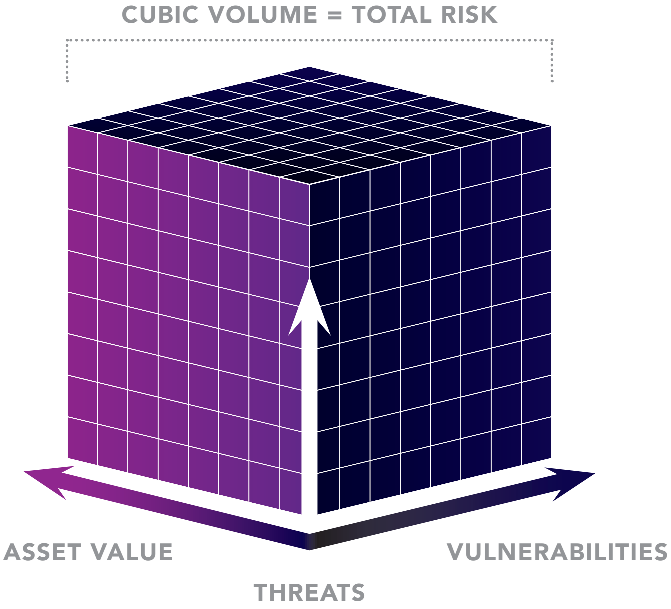
While definitions of risk vary, for this paper—and the sake of simplicity—we refer to the following classic equation: **Total Risk = f (Threat x Vulnerability) Asset Value**

Total risk is a function of the threat / vulnerability paring and asset value. Asset valuation may be expressed either in qualitative (e.g. monetary), quantitative (e.g. relative importance) terms or a hybrid version employing both criteria. This formula also fits well for assessment purposes, as residual risk can be calculated by subtracting the control gap or applied countermeasure efficacy from the calculated total risk.

Figure 1 is a graphical representation of the risk equation, where a respective increase or decrease in any of the variables impacts total risk as reflected by the cube volume change.[ii]

Finally, rather than relying on mitigation as a sole remedy to address every insider risk, the traditional risk treatment options of acceptance, avoidance, and transference need to be added to the insider dialogue.

FIGURE 1



Consider Three Factors of Insider Risk

Today's insider risk programs typically rely solely on mitigation as the remedy to address every insider risk. But this approach leaves out critical measures to address all components of risk.

AN EFFECTIVE, HOLISTIC INSIDER RISK PROGRAM ADDRESSES:

Threats: There are myriad tools on the market for detecting insider threat based on indicators from structured data sources, e.g. databases, logs, and spreadsheets. The difficult part of threat detection is processing the messy, unstructured data sources, such as social media, emails and metadata, the processing of which also necessitates non-technical means and administrative controls.

Vulnerabilities: With a lack of widely adopted standards and few compliance requirements for insider risk programs outside the Federal Industrial Security realm, assessing where an organization's insider vulnerabilities reside can be challenging.

Assets: Identifying what deserves the greatest protection is perhaps the most fundamental, and yet most overlooked aspect of an insider risk program. Tangible and intangible critical assets need to be identified, categorized, labeled and given appropriate physical, logical, and administrative controls.

Accounting for all parts of the risk equation requires collaboration from the entire organizational enterprise to manage their insider challenges properly.

Eight Components to Building a Successful Insider Risk Program

A comprehensive insider risk program requires people, processes, and tools, acting collectively to achieve the greatest benefit and return on investment. There are eight components every organization must consider when building a successful program:

1. Leadership Advocacy

Executive "buy-in" or mere support is not sufficient; a fledgling program needs senior organizational evangelists to succeed. Top-down advocacy is not only critical to launching the program, but it supports program oversight and provides long-term resourcing and sustainment.

It is important that leaders have confidence the insider risk program aligns with the company's corporate culture and values, is legally and ethically sound, and meets all regulatory standards.

2. Governance

In addition to executive leadership advocacy, it is imperative to identify key stakeholders and create a steering committee. The role of the steering committee is to provide strategic guidance in the development and deployment of the program, dispense critical oversight, and communicate with the Board of Directors. Steering Committee membership includes the program's Executive Sponsor, Information Technology, Corporate Security, Human Resources, Legal and Privacy, Ethics and Compliance, Strategy, Finance, Communications, and other key stakeholders from across the organization, as appropriate.

Supporting corporate insider efforts at the operational level are insider risk working groups composed of management-level participants, with core representation similar to the steering committee. The intent of the working groups is to use cross-functional resources to address insider matters and recommend appropriate risk treatments. Working groups may also be empowered to oversee assessments and manage critical corporate assets in conjunction with the respective owners.

3. Documentation

Formal documentation that outlines the charter, roles, authorizations, responsibilities, etc. is imperative for a well-functioning program. One of the first program documents should be a comprehensive Concept of Operations (CONOPs), with associated appendices addressing such items as program staffing, consequence management processes, resources, privacy, and monitoring. The CONOPs should include a mission statement—including an organizational definition of an insider—descriptions of insider risk program initial and full operational capabilities, and be a comprehensive "living document" serving as the insider risk program foundation.

Existing organizational policies should be evaluated for their applicability to the insider risk program. A dedicated organizational policy should be considered to fully articulate the function and authority of the insider risk program.

4. Communication

Before formally launching an insider risk program, Steering Committee representatives and delegates should develop a communications plan that aligns with the organization's mission, vision, and values. Communication themes should include insider risk program transparency, the holistic and preventative nature of the program focusing on employee welfare, and the senior leadership advocacy and support of the program. Messaging should be tailored to all levels of the organization, provide an appropriate understanding of the program, and inform employees of their roles and responsibilities associated with managing insider risk.

Once messaging has been reviewed, finalized, and approved, broadcast the information in as many avenues as possible: webinars, emails, podcasts, posters, and company newsletters. This dissemination plan can also be used for the training and awareness campaign.

A well-rounded communication plan should also account for the means and channels to receive insider information from internal and external sources. Existing reporting mechanisms may suffice, or an organization may wish to stand up other dedicated means, such as the web or a hotline.

5. Critical Assets

Asset value is a key element in the risk equation and organizations should have a good understanding of what they most need to protect. To do so, an organization must have established criteria of what constitutes a critical asset, identify the location and owner of such assets, create and implement a classification schema for all tangible and intangible assets, and have a means to audit who accesses these critical assets.

Critical assets may include physical items and products, data, software, processes, and even individual employees. A data classification schema is imperative to enable technical monitoring capabilities. Proper critical asset management is a key step to provide defensibility in matters of trade secret compromise, particularly if prosecution under various Federal and State statutes may occur.[iii]

6. Technical Tools

While technology plays an important part in the success of a robust insider risk program, the overwhelming amount of information from monitoring tools produces little insight if not partnered with proper analytical capabilities. In addition to network and endpoint monitoring capabilities, insider risk programs should include targeted employee monitoring capabilities, social media surveillance, and robust case management tools.

Given the intrusive nature of some technical tools and the gravity of the results rendered by their employment, it is essential that information collected about individuals is performed in accordance with the organization's privacy requirements, policies, and standards, and with legal counsel approval.

7. Consequence Management

Addressing insider events should be empowered to a response team of individuals with such skill sets as investigations, counterintelligence, and human resources. Validated procedures should govern the opening of inquiries, referral of matters to external agencies for investigation, and near constant interaction with general counsel to ensure privacy and legal concerns are met. As they conduct their activities, the team should frequently consult with the respective risk working group before case escalation.

Consequence management should provide program metrics to help determine the insider risk programs' effectiveness and return on investment. Metrics may include the number of risk alerts generated, the number of inquiries conducted, investigations referred, and the amount of proprietary property recovered. A case management tool will facilitate aggregation of metrics, as well as serve as a central repository for historically documenting individual risk indicators and providing a behavioral baseline of the person throughout their tenure in the organization.

8. Training and Awareness

A well-structured training and awareness program should educate employees about their vulnerability to internal and external threats, provide guidance on protective measures, and reinforce the means to report potential insider concerns.

Awareness should occur at onboarding, and refresher training provided on a recurring basis. The employee should formally acknowledge training and recorded in a manner that makes the records readily available for review.

Execute for Program Success

Addressing insider risk by driving a holistic, proactive, and risk-based approach breeds benefits that include:

- deterring potential insiders
- safeguarding corporate brand and reputation
- protecting intellectual property and informational assets
- improving shareholder and customer confidence

To execute a successful program, the entire organization must be engaged to accurately evaluate key factors that contribute to risk; threats, vulnerabilities, and assets. Next, review the eight components of building a program in the context of people, process, and technology. And finally, partner with qualified and proven practitioners.

ABOUT LEIDOS INSIDER RISK SOLUTIONS

Today's organizations often struggle to manage complex insider risk challenges independently. Although you may be aware threats exist and even understand the detrimental impacts, your organization may lack the internal resources or expertise to recognize vulnerabilities, develop an insider risk management plan, and effectively respond to alleged or suspected insider activity. The Leidos team of insider risk experts bring decades of counterintelligence, investigative, and industry-specific experience to every engagement. Our solutions are designed to assist you through all phases of creating and administering a comprehensive insider risk program.

Partner with Leidos to help safeguard your brand, revenue, resources, and people.

[i] Doug Thomas presentation remarks to the Florida Industrial Security Working Group, Orlando, Florida, May 4, 2016.

[ii] Symantec Corporation,"Assets, Threats and Vulnerabilities: Discovery and Analysis; A comprehensive approach to Enterprise Risk Management." https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/assets-threats-vulnerabilities-01-en.pdf

[iii] 18 U.S. Code, Chapter 90 Protection of Trade Secrets § 1839 (3) (a) states an element of a trade secret is that "the owner thereof has taken reasonable measures to keep such information secret."

ABOUT LEIDOS

Leidos is a global science and technology solutions and services leader working to solve the world's toughest challenges in the defense, intelligence, homeland security, civil, and health markets. The company's 32,000 employees support vital missions for government and commercial customers. Headquartered in Reston, Virginia, Leidos reported annual revenues of approximately $7.04 billion for the fiscal year ended December 30, 2016.

leidos

11955 Freedom Drive
Reston, VA 20190
leidos.com

- **LinkedIn:** Leidos
- **Facebook:** Leidosinc
- **YouTube:** Leidosinc
- **Twitter:** @Leidosinc

FOR MORE INFORMATION

855-56-CYBER / cyber.security@leidos.com / cyber.leidos.com