Insider Threat Resource Directory

INSA in partnership with DHS, FBI and ODNI

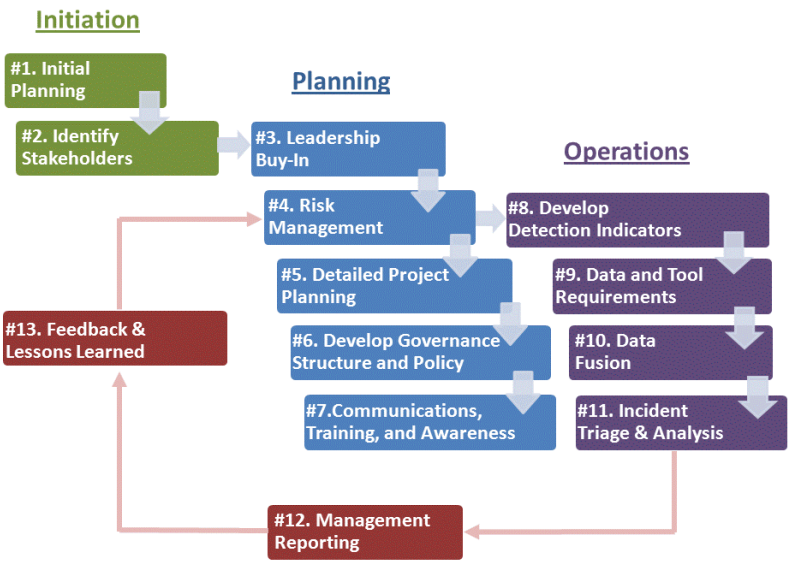
Insider Threat Roadmap | Terms of Reference | Domain Gaps | Insider Threat Resources | Contact Us

Background: The IC Analyst-Private Sector Partnership Program, sponsored by the Department of Homeland Security's Office of Intelligence and Analysis, on behalf of the Director of National Intelligence, facilitates collaborative partnerships between members of the private sector and teams of experienced Intelligence Community (IC) analysts. The areas of focus selected for this year's program, based on intelligence priorities, were: Energy Security, Money Laundering, Identifying and Countering Insider Threats, Air Domain Awareness, Identity Theft and Illicit Activity, Game Changing Biotechnology. Our group, based on individuals experience and expertise, was selected to work on the Insider Threat topic.

Deliverable: Our group set out to develop a resource that provides the essential elements required to initiate an insider threat program. To accomplish this, our group relied on several sources including: personal experience in the public and private sectors, interviews with industry experts, overviews of insider threat programs and countless discussions among team members. The 13 essential elements were developed to follow a timeline from the first step (Initial Planning) to the last (Feedback/ Lessons Learned). In practice the processes required are iterative and will require coordination and communication throughout.

In addition, we reviewed more than 200 insider threat publications, and mapped them to the 13 Essential Elements. The degree of relevance to each element is also indicated in the spreadsheet. We believe that this spreadsheet will serve as a useful resource for any organization that is creating or maturing an insider threat program.

Insider Threat Program Roadmap (Click image for larger version)



1). Initial Planning

Significant theft by trusted insiders or the loss of sensitive data by cyber intrusion were often drivers for establishing a corporate Insider Threat program. It took one company five years and a series of incidents before its senior leadership committed to investing in an Insider Threat program.

Individuals setting up new programs should tap into existing resources as a first step. Some large defense contractors have already implemented some of the functions of a basic Insider Threat program, but most have not formalized the program or integrated it across the organization. A good first step is to determine what resources and programs already exist in security, counterintelligence, information technology (IT), legal, and human resources (HR) before purchasing or building new capabilities. Integrating and building

7). Communication, Training & Awareness

Several companies highlighted the importance of corporate communications. One CSO noted, “An internal corporate communications strategy is absolutely vital.” The CSO stated that you cannot afford an ill thought-out communications plan, as it will destroy employee support for the program just as much as “false positives.”

Several companies expressed the importance of having the CEO conduct or express support the initial rollout messaging. These companies used their corporate communications experts to craft messaging and message delivery strategies. One company even used employee focus groups to test reactions to draft messaging.

upon existing resources saves time and minimizes the costs associated with getting a new program off the ground.

Both pilot and full-scale approaches are viable. One company decided to pilot a program and successfully used suspicious activity they identified during the pilot to justify further investment. A second company went for full program investment and implemented an enterprise-wide deployment upfront. Both approaches worked for their respective corporate cultures and their approaches to managing risk.

2). Identify Stakeholders

While corporate security, CI, or IT security offices tend to lead these efforts, program leaders stressed the importance of getting the right players and functional areas involved with program development, oversight and execution. A team approach is vital.

Examples include: IT, human resources (HR), legal, privacy, ethics, communications, security, CTO, and key business units. One Chief Security Officer (CSO) was adamant about involving the legal department from the earliest stages of program development. This CSO noted that it was helpful to have a single point of contact from the legal department who can work on intellectual property (IP) protection, CI, and insider threat matters.

3). Leadership Buy-in

Senior leadership buy-in must be demonstrated by both initial support for the program and a willingness to make meaningful investments in resources to build essential capabilities. Buy-in requires the decision-making ability to hire the right people, buy or develop technical tools, and create processes for internal stakeholders to implement and oversee the program. It also involves defining measures of success and outcomes. Finally, leadership is directly involved in communicating with the workforce.

One suggestion repeated by several experts for obtaining and sustaining buy-in is to develop a compelling presentation using real insider threat cases from inside the organization itself, or from other organizations in the same sector. Including dollar losses and other business impacts of those cases (reputation loss, stock drops, lost market share, etc.) can help make a business case for insider threat program.

4). Risk Management Process

The risk management process involves identifying and prioritizing critical information and assets, as well as people (employees/vendors/partners) in high-risk groups. In addition, you must identify who has access to the "crown jewels," as well as who should have access. Finally, processes should be implemented for maintaining appropriate access to critical assets over time; employees tend to accumulate an increased level of access over time, and access is not usually taken away when it is no longer needed.

During the risk management stage, one company invested six months to interview over 400 engineers to obtain consensus on protected "classes" of information. This inclusive process played an important role in obtaining buy-in from the workforce when implementing the program. Cross-functional communication and collaboration is essential for establishing an insider threat program.

5). Detailed Project Planning

One CSO felt that hiring experienced CI/law enforcement professionals was the key. One can build a solid program with only a few people if they have the right blend of IT, CI and law enforcement experience. Another company preferred hiring a greater number experienced IT professionals over experienced CI/law enforcement professionals because it was easier to teach IT persons to develop a CI/law enforcement mindset than the other way around. Ultimately, Insider Threat detection and response requires a blended approach.

Most companies emphasized starting with a general safety, security, and IP protection message. Employees need to understand that protecting the company's Intellectual Property, reputation, and financial health directly impacts jobs, stock option prices, etc. One CSO stated, "I'm trying to focus on the 1 percent of bad actors who threaten your lab's reputation and future existence…and I need your (i.e. 99 percent's) help."

8). Develop Detection Indicators

A common theme in company interviews was the need to create a high risk user group based on employee separations, reductions in force, poor performance reviews, and other factors to prioritize threats. One expert mentioned a 30 day rule for increased monitoring prior to a termination or derogatory personnel action. Organizations can also alter or strip such employees of access to sensitive information as a risk mitigation measure.

Several companies noted that it's important to have both technical/IT and reporting program components. One CSO indicated that 80 percent of leads originated from electronic-monitoring & audit programs while the remaining 20 percent originated from employee reporting or other traditional security avenues.

9). Data & Tool Requirements

Several program managers confided obtaining access to relevant underlying data streams was their hardest challenge. Often, the technical aspects are simpler than identifying relevant data streams, obtaining access to those data streams, and getting internal information sharing policies approved. Companies specifically cited challenges with:

- Corporate politics of obtaining the data and information sharing
- Corporate cultural, policy, and legal resistance
- Logistics (where and how is data managed/stored/configured/transferred)
- Understanding the "shape" and format of the data
- Understanding how to get the data on an ongoing basis
- Negotiating with end-users on how they want data to be displayed
- What data will satisfy various program policy requirements?

10). Data Fusion

Four companies in the study invested internal resources to build their own tools. These tools combine technical data with non-technical data, including HR information. One company markets their tool to government agencies and other companies. Two others utilize their tools to enhance and integrate their own Insider Threat capabilities. One company's tool can detect changes in patterns of behavior by performing behavioral analysis and profiling by job function to identify outliers. A few organizations have implemented risk scoring mechanisms in their technologies.

The theme that technology is a tool rather than a complete solution was emphasized during several discussions.

11). Analysis and Incident Management

One CSO noted: "You must have clear authorities and a capability to do something once red flags are identified. This includes some sort of internal capability or process for figuring out if there's actually a problem and (ideally) what type of problem it is. Once you understand what's going on, you have to take some sort of action."

Too much information can lead to false positives which waste investigative resources and deflect attention away from more serious indicators. An Insider Threat program must be designed to minimize false positives, and the process of handling of false positive events should be worked out in advance.

12). Management Reporting

One CSO initiated a quarterly report to show progress and sustain buy-in among stakeholders. It is important to provide metrics to management as an effective way of gaining momentum and support for the program. Another CSO

6). Develop Governance Structure, Policy, and Procedures

Mature insider threat programs in several companies followed a three-tier governance model. The first tier involves engaging corporate leadership, potentially through presenting at an annual meeting and securing an initial commitment to establish an insider threat program. The second tier involves establishing an advisory and review committee, usually composed of vice-president level officials from human resources, privacy, ethics, security, and other relevant departments. Finally, the third tier is a steering committee at the senior manager level responsible for general oversight of the program.

stated that it is not enough to simply identify problems and increase cases. Additional study is needed to illustrate best practice in demonstrating return on investment in insider threat programs.

13). Feedback & Lessons Learned

Multiple experts recommended creation of a mechanism, such as a secure forum, for Insider Threat practitioners to build trust and share lessons learned. Feedback based on case studies ensures that senior leaders and program managers can make appropriate risk management decisions and refine their program. Equally important, case based examples will greatly improve communication, training, and awareness materials and efforts.

Terms of Reference

A Roadmap for Identifying and Countering Insider Threats in the Private Sector

Private industry faces more challenges to safeguarding sensitive, proprietary, and classified information than ever before. The rise of cyber attacks from major state actors has added to, not replaced, traditional insider threats working on behalf of themselves and rival companies. Thus, the private sector must defend itself against the theft of sensitive business information from multiple—and often overlapping—threat vectors. Partnership between the private sector and government in this area should be a national priority.

The Intelligence Community Analyst-Private Sector Partnership Program, sponsored by the Department of Homeland Security on behalf of the Director of National Intelligence, facilitated a six-month partnership between members of the government, private sector, and academia with the directive to conduct research on methodologies for identifying and countering insider threats. The Insider Threat Team scoped this project to focus on identifying best practices for building an insider threat program in the private sector.

The Insider Threat Team studied the challenges of building a corporate insider threat program and the gaps that exist in insider threat defenses from the perspective of six companies representing the critical manufacturing, defense, financial, and telecommunications sectors as well as two trade groups that support small and mid-sized businesses. The team conducted a comprehensive review of insider threat academic literature and applied resources identifying thirteen “essential elements” of an insider threat program. The list of elements, and the relationship between each element, is depicted on a one-page “Insider Threat Program Roadmap.” That blue print, and an Insider Threat program resource guide, are publicly available via the Intelligence and National Security Alliance (INSA) website: www.insaonline.org.

The purpose of this document is to provide a description of the thirteen elements, consolidate information from the literature review and practitioner interviews, summarize how much guidance is available for each of the thirteen components, and identify gaps, research, and practical advice.

Insider Threat News

Google.com
The Moment I Began Selling Secrets To The Russians -- Or So They Thought - Jalopnik
Oct 01, 2015
JalopnikThe Moment I Began Selling Secrets To The Russians -- Or So They ThoughtJalopnikThe binders were inside a large ...
Louis E. Bladel, III Named Special Agent in Charge of Counterintelligence ... - Federal Bureau of Investigation (press release) (blog)
China Cyberspying on U.S.After No-Hacking Deal - Daily Beast
Cyber warriors on the new frontline - The Australian
The Moment I Began Selling Secrets To The Russians -- Or So They Thought - Jalopnik

Gap Identification

Directions for Further Research

Successful insider threat programs must be designed and implemented to fit the unique culture of the company or agency they are designed to protect. Planners must consider organizational culture at each stage or essential element. However, the insider threat team identified several common challenges and deficiencies across most insider threat programs. Based on its literature review and company interviews, the insider threat team identified the following gaps for further research:

Data Fusion: Data normalization and extract, transform, and load (ETL) was by far the weakest category in the literature review, with only 3 citations. Notable gaps exist in private sector insider threat programs’ abilities to integrate, synthesize, and analyze data which resides in various corporate offices. Companies with robust capabilities in this area have dedicated resources for purchasing, customizing, and/or developing technical capabilities to address this challenge.

Management Reporting: Additional study and research is needed to illustrate best practices in demonstrating return on investment in insider threat programs. Development of a management reporting dashboard tool could be useful to convey key information. This tool could be used to generate and visualize metrics so that management understands the value of their insider threat program.

Incident Triage & Analysis: Incident mitigation requires a network of external sources, including information sharing with the US government, to provide timely and relevant threat information. There is minimal literature on what corporate program managers should do after identifying an insider threat, particularly non-cyber courses of action (e.g. HR, legal, law enforcement referrals). Due to the complexity involved with these decisions, this has primarily been the territory of experienced security employees. However, most companies do not keep a dedicated counterintelligence or former federal law enforcement official on staff. Therefore, a quick reference guide identifying a spectrum of possible action options would be useful.

Intelligence and National Security Alliance, 901 North Stuart Street, Suite 205, Arlington, VA 22203 Phone: (703) 224-4672, Fax: (703) 224-4681.