A ROADMAP FOR

IDENTIFYING AND COUNTERING INSIDER THREATS

IN THE PRIVATE SECTOR

BROUGHT TO YOU BY:

AES CYBERSECURITY
an AES Controls company

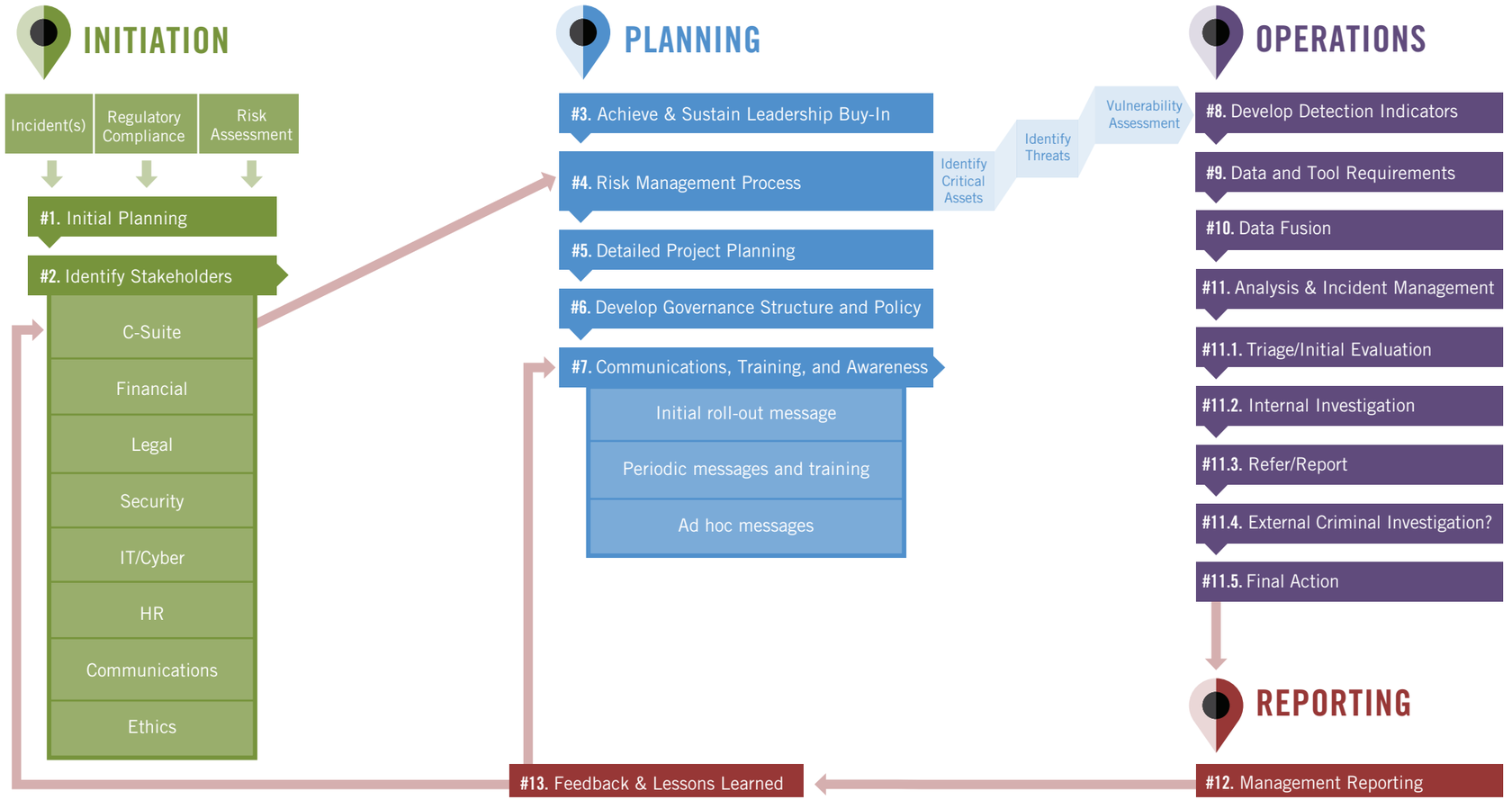
IN COOPERATION WITH:

INFRAGARD
PARTNERSHIP FOR PROTECTION

Private industry faces more challenges to safeguarding sensitive, proprietary, and classified information than ever before. The rise of cyberattacks 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 Private-Public Analyst Exchange Program facilitated a six-month partnership among members of the government, private sector and academia to conduct research on methodologies for identifying and countering insider threats. The team studied the challenges of building a corporate insider threat program and the gaps that exist in insider threat defenses from the perspective of companies representing several major industry sectors as well as trade groups that support small and mid-sized businesses. The effort resulted in this Roadmap and resource guide on best practices for building an insider threat program in the private sector.

INSIDER THREAT PROGRAM ROADMAP



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 before purchasing or building new capabilities. Integrating and building 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, counterintelligence, 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, legal, privacy, ethics, communications, security, Chief Technology Officers and key business units. One company stressed the need to involve the legal department from the earliest stages of program development, noting it was helpful to have a single point of contact from the legal department who can work on intellectual property protection, counterintelligence, 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, companies 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 company felt that hiring experienced counterintelligence/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, counterintelligence and law enforcement experience. Another company preferred hiring a greater number experienced IT professionals over experienced counterintelligence/law enforcement professionals because it was easier to teach IT persons to develop a counterintelligence/law enforcement mindset than the other way around. Ultimately, Insider Threat detection and response requires a blended approach.

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.

7 COMMUNICATION, TRAINING & AWARENESS

Several companies highlighted the importance of corporate communications, noting the internal corporate communications strategy is absolutely vital. It was stated that a company could not afford an ill thought-out communications plan, as it could destroy employee support for the program just as much as "false positives."

Several companies expressed the importance of having the Chief Executive Officer message support for this activity at the initial rollout of the Insider Threat program. 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.

Most companies emphasized starting with a general safety, security, and intellectual property 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 company 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 the study 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 policy 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 company 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
- Knowing what data would satisfy various program policy requirements

10 DATA FUSION

Several companies in the study invested internal resources to build their own tools. These tools combine technical data with non-technical data, including human resources information. Some companies utilize tools to enhance and integrate their own Insider Threat capabilities. Some tools 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.

During the study, there was a prevalent theme that technology is a tool rather than a complete solution.

11 ANALYSIS AND INCIDENT MANAGEMENT

One company 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 company 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. It was stated that it is not enough to simply identify problems and increase cases. Additional study is needed to illustrate best practices 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. Some industry sectors have efforts underway to share this type of information informally with each other.

AES Cybersecurity
an AES Controls company

SALES
Rick Salerno
rsalerno@aescybersecurity.com
513-477-9814

TECHNICAL
Jamie Ahmed
jahmed@aescybersecurity.com
513-377-0035

Chicago Office
801 Lunt Avenue
Schaumburg, IL 60193

Corporate Headquarters
155 Tri-County Parkway
Cincinnati, Ohio 45246

Houston Office
40 FM 1960 W #193
Houston, TX 77090