Article

Critical Considerations When Building an Insider Threat Program

Peter Hadjigeorgiou | Sr. Security Relationship Manager, Code42

Recognizing the growing risk posed by insider threats and committing to build a dedicated insider threat program (ITP) is the beginning of a challenging journey, but one that will ultimately make your company more secure and resilient. When designing and building out a program, the goal is to enable your team to analyze, assess, and act on potential insider threats. The most effective program is the one that can be effectively operationalized and sustained. As you start building or maturing your insider threat program, focus on the unique opportunities and challenges in your organization. There is no one-size-fits-all template for the perfect program. The best program for you will be based on your objectives, security priorities and resources. Here are some key considerations to help you on the journey.

Build you’re A-Team

Successful insider threat programs rely on teamwork across levels and functions. It is important to secure leadership upfront. Appoint an ***executive level leader*** to champion the program, drive priorities, budget, and organizational support. This will help generate support for the program from other functions and help foster collaboration with other stakeholders. For operational management, consider appointing an ***ITP Senior Official***. Prioritize the program by creating a senior level role to lead the strategy and manage the team. Give this individual a seat at the table with peers and the authority to make decisions regarding program objectives, processes, staffing and technology. Last but not least, build a team of subject matter experts with skillsets comprising data protection, endpoint and network security, incident response, forensics, and compliance. Your ***core ITP team*** will be the tactical foundation of your program.

Human Intervention and Response: The difference between traditional IR or SOC response and insider threat

Insider threat manifests itself, and should be handled, differently than other traditional cybersecurity threats. Incident response playbooks, orchestration and automation are all excellent tools to address specific problems. But for insider threat, it’s important to understand how the investigation and remediation workflows will be different than others types of response. Since insider threat is a human problem, perpetrated by one of your own employees, prepare for a human-centric response. Many investigations will involve coordination or meetings with a combination of HR, Legal and others. Eventually someone will have to speak with the employee as well. Who in your organization is prepared to sit across the table from someone who has purposefully tried to steal intellectual property? What are the right questions to ask? What do you do if they lie? Think “training and practice” instead of “automation and orchestration.”

Pick your battles, win over your skeptics and critics

Insider threat covers a wide range of risks. Many resources or guides may have a broader scope or more sophisticated approach than you may need for your organization. Based on your objectives, clearly define a few phases in the maturity or capability of your program. It’s OK to start with the low-hanging fruit or the most basic use cases.

Use the initial phases to test and refine processes. Not everyone will agree on the need for, or scale of, an insider threat program. There will also be varying opinions on the tools, processes, and roles and responsibilities among the stakeholders. Start small, focus on immediate value, demonstrate the quick wins and buy-in will follow. Consider how your program can provide insight, data, and support for the missions and priorities of other areas of the organization (e.g., HR, Legal). By demonstrating the value of an insider threat program to other stakeholders, you can shift the perception of an ITP from common negative stereotypes—expensive, redundant, big brother—to the valuable business and security enabler a good ITP can be.

Clearly define your use cases

Insider threat spans a wide variety of risk vectors. The more you intend to cover, the more complex and costly your program will be. If you have finite resources, a small team, or limited security expertise, consider narrowing the scope of your insider threat use cases. The Intelligence and National Security Alliance (INSA) defines insider threat as:

“The threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who wittingly or unwittingly, commits acts in contravention of law or policy that result in, or might result in, harm through the loss or degradation of government or company information, resources or capabilities; or who commits destructive acts, to include physical harm to others in the workplace.” (Categories of Insider Threats, 2019)

The framers of this definition, composed of public and private sector security experts with decades of experience, have intentionally given us a very broad scope to consider. Think about launching your program in phases, starting with the most pressing use cases (e.g., departing employees, remote workers, high risk employees) and expanding the scope and complexity of those use cases as you mature the processes and capabilities of the team.

One of the most effective ways to design and build an insider threat program is to start with the insider threat risk storylines you are trying to prevent, detect, or respond to and work from there. Think about it as if you were writing the script for an insider threat spy television show. Each episode is your scenario. Who are the characters? Who is the protagonist, what are their motivations, and what actions do they take? Building out these narratives for each risk helps define the policies, processes, and technical tools needed to address them. It also helps avoid scope/scale creep so you can keep your ITP lean, focused, and deliberate.

Pro-tip: Select and deploy the right tools for your mission. Don’t “over-tool” the program. You want your analysts to spend their time investigating, identifying and mitigating risks—not configuring tools, constantly updating rulesets or fixing broken endpoints.

Develop your process, investigation workflows

When you find something (and you will), then what? This part is often overlooked and frequently underestimated. In fact, many ITPs end up stalling because they lack effective processes to manage the number of alerts and investigations being generated. To begin with, ensure you’ve written a comprehensive playbook on how daily operations of your ITP will flow from investigations to escalation and triage to reporting and metrics. How will you manage the volume of investigations and scale the program effectively? Be ready to add capacity for investigations and response. Try to determine your employee turnover, apply generally accepted industry statistics on data exfiltration for departing employees, predict your caseload and stress-test your processes. Conduct live simulations with all the stakeholders involved to see where the gaps or bottlenecks might appear. Encourage participants to raise “what if” questions—even if you can’t anticipate every variable, the more scenarios you test in simulation, the better prepared you will be during real-world investigations.

Dig into the data

Your insider threat program can drive recommendations and change in many areas of the organization. One of the most valuable aspects of an ITP is the visibility it provides: an optimized ITP is the flashlight illuminating the dark corners of your company. In addition to configuring your program to address specific use cases, you can set up your program to assist more generally with visibility and discovery. Where is data going? What cloud applications are employees using? Which parts of the business access or use certain files? As you compile data and metrics, you can compare it with the policies and processes in place to see how effective they are—and if your employees are following the guidelines.

Insider threat programs are uniquely positioned to identify organizational risk in a number of areas:

- Policy and compliance violations: The nature of insider threat cases will reveal which policies aren't being followed. For example, if your company has a policy outlining acceptable backup solutions, but you find a large number of cases where people are using personal cloud storage sites as backup for their work machines, it gives you a starting point to figure out the disconnect between corporate policy and employee actions. Use of unsanctioned applications, including the massive shift we have seen to cloud collaboration tools, often exposes the organization to significant risk. However, it is also frequently an indication that corporate IT systems aren't providing the right tools to enable employees to work as efficiently and productively as possible.
- Security control gaps: In some cases, you may identify behaviors that are risky enough to warrant implementation of additional security measures or controls. For example, developing methods for encrypting and sharing sensitive information with customers or business partners.
- Security training and awareness needs: Analyzing the "demographics" of your cases will help you better understand training and education needs across your organization. For example, if employees in a particular division or business unit continuously violate policy or mishandle data, you can work with HR, business leaders, and others to target additional communications and training to those areas.

Having a clear understanding of how your employees are using (or misusing) data helps drive behavioral and cultural change in your organization. If you have a cloud collaboration policy, but you can demonstrate with data and metrics that a huge percentage of your employees aren't abiding by the policy you can suggest changes to senior leadership (e.g., better training and communication, enforcement of consequences, development of easier and more useful tools or policies). Aside from the discrete use cases around insider threat, your ITP can help identify and quantify organizational risk—and help target areas for improvement.

In closing…

At the end of the day, the best program is the one that works for your organization. Take these recommendations as a set of guidelines and anecdotes based on years of trial and error. You will have your own successes and challenges as you build and mature your ITP but we hope these considerations will accelerate your journey.