Preventing Insider Threats Starts with the Basics

Organizations have grappled with how to prevent, detect and respond to insider threats for years, however technology has made it easier and faster for someone—either intentionally or unintentionally—to inflict damage.

The threat from insiders affects industry and government organizations alike, according to speakers at a March 12 Federal Focus event on Insider Threat Detection and Mitigation. A well-thought-out insider threat program that focuses first on the basics, such as training and awareness, and ultimately incorporates sophisticated data analysis tools is the best approach, the speakers said.

Insider threats can be difficult to detect because they are employees and business partners who have legitimate access to systems and information. Sometimes an insider threat is someone such as Edward Snowden who intentionally leaks classified government information, but often it’s an accidental insider who, for instance, unwittingly uploads malware to the network.

Recent statistics show that about 87 percent of organizations had experienced a security breach in the previous 12 months, and more and more data is being improperly accessed and compromised than in the past.

Organizations realize that the threat can come from the inside, not just from bad guys on the outside, said Michael Theis, Chief Counterintelligence Expert and Senior Member, Technical Staff, CERT Insider Threat Center Software Engineering Institute, Carnegie Mellon University. Still, the goal of protecting data is the same, regardless of where the threat originates. “We have added a new dimension to an old program of protecting critical assets,” he said.

Changing behavior
There is no single type of insider threat, nor is there one single program that will work for every organization. However, there is a common approach that speakers recommended: Focus on the people, process and technology, and start with the basics.

“A lot of this activity is simple human behavior, and the behavior and the training is our first best line of defense,” said Paul Christman, Vice President, Dell Software Public Sector. Around 70 percent of IT security breaches can be attributed to human elements, he added.

Agencies should create awareness for their insider threat program, get buy-in for the program from all levels of the organization, and teach employees what they consider appropriate behavior.

Make sure any policy is spelled out in black and white, and is
communicated clearly because change may not always be welcomed, said Joseph Demarest, Assistant Director, Cyber Division, at the FBI. “We find in cyber, involving the workforce in everything we do…that has been helpful,” Demarest said. “But I still think it will represent a change. It has for us.”

Beyond training and awareness, there are other basic activities that agencies can take to help diminish the potential of insider threats, such as knowing what assets need to be protected, maintaining an accurate inventory, segmenting users from the data, authenticating users, having visibility into the network and using encryption.

And never let your guard down. “Trust no one,” said Gustavo Coronel, Security Engineer, Check Point Software Technologies. Assume that everyone who is part of the system could be part of the problem, he said. It’s essential that agencies protect their authentication keys, he added, because “it is the access to everything you have.”

Tailoring a program
It’s challenging for some agencies to develop a single insider threat program that will work organization-wide because “there is not a single risk appetite for the whole department or for the whole government for that matter,” said Mike Maraya, Deputy Chief Information Security Officer, at the Department of Energy (DOE). The solution at the DOE, which is very diverse, Maraya said, was to work off a baseline to develop a customized program for each component based on what they need to protect.

In creating an insider threat program, agencies shouldn’t overlook best practices and models that are already available such as CERT’s guide to mitigating insider threats, and NIST’s cybersecurity framework. Although designed to help agencies identify, protect, detect, respond and recover from cybersecurity risks, NIST’s guide also can be applied to an agency’s insider threat problem, said Brian Peretti, Director, Office of Critical Infrastructure Protection and Compliance, Department of the Treasury.

Beyond sharing best practices, organizations should also share details on threats and system breaches with other organizations, something that has been particularly useful in the financial industry. “We push the information sharing aspect,” Peretti said. “If someone is doing something improper within your organization, how do you let other firms understand that?”

“There are technologies and tools, such as data loss prevention, and security information and event management software, that can help agencies mitigate an insider threat, but ultimately, they will need a more comprehensive analytical approach, said Adam Cohn, Director, Government Affairs and Public Policy, at Splunk. “All data can be potentially security relevant and agencies have access to a lot of data that can be useful if they have the right tools and capabilities,” he said.

Data within an organization is not static—it’s always changing—which makes it hard to manage, said Tom Blauvelt, Continuous Monitoring and Security Solutions Architect, Symantec. As a result, agencies must have “technology and process working hand-in-hand” so that they have the ability to “measure where the information is, along with being able to control” who can perform operations on it.

The goal is to be able to collect and analyze data indicators that, when taken together, may show a pattern that would raise a red flag on a potential insider threat. Advanced analytics would be able to provide agencies with a risk profile of individuals, allowing officials to take action, if necessary. Agencies must first establish a baseline for “normal” employee behavior, so they will be able to identify behavior that is “abnormal” and a potential threat.

Technology has matured enough that security problems can be solved by big data solutions, said Prem Jadhwani, Chief Technology Officer at Government Acquisitions. Combining the right data with the right tools, and knowing what to look for, will help agencies mitigate insider threats. But don’t invest in tools until you address the basics first and have a plan in place. “Always start with the framework,” he said.

The challenging part of any insider threat program is that the goal line is always moving, said Neil Carmichael, Jr. Program Manager, Insider Threat Program, at the National Archives and Records Administration. NARA, which traditionally has stored paper-based classified documents produced by other agencies, now must handle massive amounts of digital files. “Don’t be content with good enough,” he said.

Ultimately, a successful insider threat program will depend on whether an organization makes security part of everything it does, something that is not yet a prevalent practice, said Robert Dix, Vice President, Global Government Affairs and Public Policy, at Juniper Networks. “In the risk environment we live in today, it absolutely demands we have a culture of security,” he said.
**Session Highlights**

Here are some take-aways from the individual sessions

**SESSION 1**

**Detecting and Deterring the Insider Threat**

Speaker
Joseph Demarest, Assistant Director, Cyber Division, FBI

- The FBI helps direct the activities of the National Insider Threat Task Force, which was created after the Wikileaks release of classified documents.
- A good insider threat program needs strong, clear and widely publicized internal policies about what is acceptable behavior and training around them.
- Organizations must know where and what their important assets are and who has access to them.
- There are behavioral indicators that can indicate a potential insider threat such as an employee who takes classified documents home, works odd hours, or has suspicious contact with people outside the organization.

**SESSION 2**

**Enabling Insider Threat Awareness and Response**

Speaker
Paul Christman, Vice President, Dell Software Public Sector

- An organization can never have enough training. Start with the people because that is where all the interaction happens.

**SESSION 3**

**Panel: Managing Risk in the Digitally Connected World—Agency Data Defense Strategies**

Speaker
Tom Blauvelt, Continuous Monitoring and Security Solutions Architect, Symantec

- To help prevent insider exploits, focus on the user and the data.
- Pay attention to the user and make sure they are trusted and managed.
- Technology and process have to work hand in hand so agencies need a strategy that combines the ability to measure where their information is and control who can perform operations on it.

Speaker
Adam Cohn, Director, Government Affairs and Public Policy, Splunk

- Insider threat mitigation requires a multi-faceted approach.
- One critical element of that approach is to establish a central capability to gather and analyze data.
- Ultimately organizations need a more comprehensive analytical approach that lets them correlate, and statistically analyze data.

Speaker
Gustavo Coronel, Security Engineer, Check Point Software Technologies

- Trust no one. Assume that 100% of people who are part of system could be part of the problem.
- To reduce threats: focus on segmentation, authentication, visibility and encryption.
- The management network should be the very first thing an agency segments internally.

“**Know your assets... Then once you know what you’ve got, put a value to it. Know your risk appetite and risk tolerance. Then you say, tell me what tools are out there to protect my crown jewels.”**

Prem Jadhwani, Chief Technology Officer, Government Acquisitions
Session Highlights
Here are some take-aways from the individual sessions

**Speaker**
Robert Dix, Vice President, Global Government Affairs and Public Policy, Juniper Networks

- In certain levels of an organization the focus is on performance and functionality and keeping the shop running. The culture of security isn’t pervasive.
- Moving to a robust enterprise risk management program and implementing basic cyber hygiene across the environment will deal with a lot of insider threat issues.

“A lot of this activity is simple human behavior, and the behavior and the training is our first best line of defense.”
Paul Christman, Vice President, Dell Software Public Sector

**Speaker**
Prem Jadhwani, Chief Technology Officer, Government Acquisitions

- One problem with insider threat is a lot of people don’t know they have been victims of threat until well after the fact.
- Insider threat must focus on the people, process, and technology issues.

**SESSION 4**

**Understanding Insider Behavior and Detection in Your Environment—Create a Security Awareness Culture**

**Speaker**
Neil Carmichael, Jr. Program Manager, Insider Threat Program, National Archives and Records Administration

- NARA’s scope has changed and its electronic footprint is growing. It has agency partners who make permanent records, and historic, and classified documents, more of which are digital.
- Communication about an insider threat program is key because buy-in is essential.
- The goal line is always moving. Don’t be content with good enough.

**Speaker**
Mike Maraya, Deputy Chief Information Security Officer, Department of Energy

- Energy’s approach to insider threats has been to work closely with the office of intelligence and counterintelligence.
- Energy has a diverse mission set, so instead of developing one single insider threat baseline or multiple baselines, it customized programs for different offices.
- Insider threat is not a technology problem, and technology alone is not going to solve it.

**Speaker**
Brian Peretti, Director, Office of Critical Infrastructure Protection and Compliance, Department of the Treasury

- Financial institutions maintain that the insider threat is not a larger threat than any other threat, it’s just different.
- NIST cyber security framework, which is based on the five pillars of identify, protect, detect, respond and recover, can be applied to the insider threat problem.
- Information sharing on incidents is key to addressing insider threats.

**Speaker**
Michael Theis, Chief Counterintelligence Expert and Senior Member, Technical Staff, CERT Insider Threat Center Software Engineering Institute, Carnegie Mellon University

- The insider threat isn’t new; organizations are trying to protect critical assets, as they have always done.
- There is no one type of insider threat. Each organization has to have its own model, based on what they are most concerned about, for instance a bank would be concerned with fraud.
- CERT soon will publish a document that addresses the perception problem as it relates to insider threat program and its potential misuse.