Although insider threats are relatively rare, the impact they can have on an organization can be catastrophic because of the level of trust and access a rogue employee has to sensitive systems and data.

The case of Edward Snowden, charged with leaking classified information from the National Security Agency, is one recent example.

It can be difficult for agencies to prevent against insider threats because an insider is someone who is authorized to be on an organization’s system, usually takes action during normal business hours, and can be motivated by different factors including fraud, theft of intellectual property, and sabotage.

By taking the right multi-faceted approach, however, agencies can put together a program that allows them to detect, protect and respond to insider threats, according to speakers at an Oct. 22 “Insider Threat Mitigation Strategies” event.

There is no “silver bullet” when it comes to guarding against insider threats—no single tool or approach will solve the problem. “It’s more of a silver buckshot,” said James Trainor, Deputy Assistant Director, Cyber Division at the FBI, speaking at the event.

This “buckshot approach” involves training people to recognize clues and potential security threats, ensuring the entire organization is involved and sharing data that may identify a potential insider threat, and using the right technology and tools to help detect anomalies.

This comprehensive approach depends on the people, process, and technology working in concert against insider threats, said Dan Waddell, Director of Government Affairs, (ISC)². “Even if you have a really good tool... you have to make sure you have the people and processes in place,” he said.
When agencies draft their insider threat strategy, they should start small, according to speakers at the event. Insider threat programs are designed to protect the critical assets of the organization so agencies should prioritize not just the data, but also the employees that can do the most significant damage.

Agencies should define what “normal” is for them, which makes it easier to recognize something suspicious happening on a network. Then they should define what constitutes an insider threat to the organization; for example, does it include subcontractors or the supply chain, as well as disgruntled employees?

It’s important that agencies establish a risk profile for the information they are trying to protect, and not try to do too much too soon. Focus initially on a high-risk group of people, high-risk data or a high-risk application rather than jumping to more nuanced psycho/social indicators, which can be difficult to measure.

Taking preemptive approaches to security, such as creating documents that are encrypted from the start, and supporting cloud environments that are FedRamp approved, can boost insider threat programs. So can using available resources such as research from CERT, based at Carnegie Mellon University.

Building public/private partnerships to collect and share insider threat data would go a long way to helping agencies, however there isn’t a model yet on how to do that securely.

“I think we will be cooking with gas when you see industry sharing insider threat indicators the way they are with advanced persistent threat indicators,” said Patrick Reidy, Director of Global IT Security/Chief Information Security Officer, CSC.

Sometimes reducing the risk can be a relatively simple tactic. Whittling down the number of users who have administrative access on a network, or establishing an anonymous tip line both help reduce insider threats.

Much of detecting insider threats, said Eric Chiu, Founder and President, HyTrust, depends on enforcing the right policies, and having the right level of monitoring and data security to ensure the environment is safe. Ultimately, though, agencies have to change the way they think about security, he said. Agencies should focus less on keeping the bad guy out and simply “assume the bad guy is already on their network.”

For more information on events go to: www.1105publicsector.com/events

### Session Highlights

**Taking Steps to Detect and Deter the Insider Threat: An Executive Overview**

**Speaker**

James Trainor, Deputy Assistant Director, Cyber Division at FBI

- Reducing insider threat is about risk management and what actions are taken on the front end (who is allowed into the organization), back end (what actions are taken before a person leaves the organization) and in between (what is the culture, policies and procedures of the organization).
- Insider threats fall into one of four groups: trained spy, the sloppy employee, the saboteur and the leaker.
- The FBI’s insider threat program determines who are the high-risk employees, what is the most sensitive information that needs protection, and who has access to it.
- Set a baseline for “normal” behavior, provide training, follow your intuition if something doesn’t seem right, and don’t establish an organization based on fear.

**Enhancing Internal Security with Improved Situational Awareness**

**Speaker**

Eric Chiu, Founder and President, HyTrust

- A virtualized environment increases the chances for catastrophic failure, so make sure there is a mitigation plan in place in case of a disaster.
- Every organization should assume the bad guy is already on their network. This will fundamentally change how to protect critical systems and data.
- Ensure federated systems—or shared environments among different parties—are secure by enforcing access control over employees and outside vendors.
- Training, two factor encryption, proper authorization and enforcing policy-based controls are all part of mitigating threats.

**Speaker**

Wesley Ellis, Consulting Manager, Professional Services, Guidance Software

- When it comes to cloud computing, know who has access to those end points, what resides on those end points and which servers are hosting that data.
- Agencies should know what their “business normal” is; then it’s easier to detect anomalies when they occur.
- Organizations need to have the right prevention, detection and response procedures in place to protect against threats.
- Find the right balance between implementing security policies without interfering with business functions.

**Speaker**

Kenneth Johnson, Senior Architect, Advanced Programs, Adobe

- The heart and soul of digital rights management is digitally encrypting documents and allowing only a specific audience access to them.
SESSION HIGHLIGHTS

• When mitigating risk against insider threats: create a policy that is associated with the risk profile for the information of your organization; create documents at a level where encryption is baked in; aim your infrastructure at cloud environments that are FedRamp approved.
• Federation of services shouldn’t mean co-location of data. Build in mitigation of risk at the document level, data level or service level.
• To reduce insider threat, agencies should immediately audit any user level, root access level, event.

INSIDER THREAT MITIGATION-ONE PERSON CAN MAKE A DIFFERENCE

SPEAKER
Patrick Reidy, Director of Global IT Security/Chief Information Security Officer, CSC

• When creating an insider threat program start with a simple hypothesis and focus on either a potential high-risk group of people, a single high-risk application, or a single piece of high-risk data.
• A good threat indicator needs to be observable to a system, and have to be differentiated, meaning it always detects the bad guy and never the good guy.
• Human decision making in the analytic chain should always be part of an insider threat program.
• Focus attention on the person who has motivation to do damage, consider establishing an anonymous tip line, and institute training.

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

• An insider threat program should work organization-wide, or it won’t allow agencies to detect, protect or respond to insider threats.
• Tools are limited in their ability to detect malicious users because insiders are people authorized to use your systems.
• The harm caused by unintentional insider threat is the same caused by intentional insider threat — having an insider threat program in place could prevent both.
• Insider threat programs are not for monitoring employees they are to protect critical assets of the organization.
• A good component of an insider threat program is training and awareness and reporting suspicious behavior.

SPEAKER
Dan Waddell, Director of Government Affairs, (ISC)²

• First define what insider threat means to your organization—does it include the supply chain, subcontractors — then start defining metrics to help measure that.
• Public/private partnerships to collect and share insider threat data are the way to go, but there isn’t a model yet on how to do that securely.
• There are some good detection and analytics tools available, but without the right people and processes in place, an insider threat program will not succeed.
• A good, interactive, problem solving-based training program, rather than a PowerPoint presentation, is an effective approach to involving users in detecting insider threats.

“...There is a dynamic tension between the search for the insider threat and our ability to federate and encapsulate security in a very content specific way.”
—Kenneth Johnson, Senior Architect, Advanced Programs, Adobe

“...Unlike a lot of other cyber security problems, this is always about human beings and human processes, which you are not always going to be able to get from just analyzing ones and zeros.”
—Michael Theis, Chief Counterintelligence Expert and Senior Member, Technical Staff, CERT Insider Threat Center Software Engineering Institute, Carnegie Mellon University

“...Take a look of separation of duties…[reduce the number] of folks who have administrative rights within your organization. Doing little things to get risk down to a manageable level is a good takeaway.”
—Dan Waddell, Director of Government Affairs, (ISC)²