Insider Threat Program Training Starts With Security 101

Friday - 8/8/2014, 11:26am ET

Commentary by Jim Henderson
CEO, InsiderThreatDefense.Com
For Federal News Radio

The concept of putting an insider threat program (ITP) in place is to provide greater attention to protecting an organization's assets — personnel, data, information systems and networks — from the malicious insider.

But before an organization decides to put an ITP in place, it should first have its house in order. Just trying to put an ITP in place may provide the organization with a false sense of security.

If you look at the countless surveys, studies and reports that have been written about many government agencies and businesses with regard to cyber threats and insider threats, the foundation of security 101 is not in place. So it is no wonder cyber attacks and insider threat incidents continue to happen.

It's time we get back to the basics. Quite a number of insider threat incidents have happened because basic security 101 and risk management principles were absent, overlooked or ignored. A determined malicious insider will look at all vulnerabilities in an organization and exploit the one with the greatest change of success, and least chance of detection.

The organization should first have a foundation of security in place that starts with:

- □ Governance
- □ Facilities security
- □ Personnel management
- □ Information system security
- □ Baseline security controls
- □ Secure configurations
- □ Information assurance
- □ Inventory of information assets
- □ Data management plan
- □ Data privacy and protection guidance training
- □ Risk management
- □ Communication across the organization's various departments and policies and procedures, etc.

If an organization has its in-house in order, it's off to a much better start to put an ITP in place.
While each organization's ITP could be structured somewhat differently, below is a template for what one could look like:

- **Combating The Insider Threat Problem Using An Enterprise Approach — For an organization to combat the insider threat, it needs to establish a comprehensive and integrated ITP that is comprised of individuals from various departments, business units and supporting functions.** The end result for any ITP is the identification of suspicious or malicious activities and behavioral indicators by the insider, as these are crucial in limiting or neutralizing the potential damage that may be caused by an insider. Communication is critical. Existing security disciplines and business will work together in concert and concentrate their efforts on protecting the organization's critical assets. This approach to risk management will shift from a tactical level, to a strategic level and eliminate communication silos.

- **Insider Threat Program Core Goals — One of the core goals of an ITP is to integrate and utilize the various security disciplines, business units and functions in an organization to support the ITP.** Depending on the business or government organization, the following security disciplines, business units or individuals may be part of developing, implementing, managing or providing support to the ITP.

The individuals that must be part of the ITP include everyone from the ITP manager, ITP analyst(s), to personnel from facilities security, human resources, to counterintelligence investigators, to senior directors, to chief risk officers, to network security administrators, to the legal department, and many others.

The Insider Threat Program Will:

□ Develop a mutually supportive enterprise insider threat risk management framework.
□ Develop and implement sharing policies and procedures so the organization's ITP can gather, access, share, integrate, analyze and respond to information and data derived from various security disciplines and departments from across the organization, including counter intelligence, security, information assurance, human resources, personnel security offices and others that may be indicators of a potential insider threat.
□ Provide much greater attention to ensure that basic and simple security countermeasures, such as policies, procedures, awareness training, physical, operational and technical security controls, are in place, functioning and operating as intended.
□ Identify and assess existing threats, vulnerabilities and weaknesses that could enable insider threats, and develop additional risk mitigation strategies as needed to protect the organization's data, information systems and networks.
□ Investigate and respond to threats against an organization's assets by insiders.

There are certain requirements under the National Insider Threat Policy that agencies need to take into account as they create an ITP.

# 1 - ITP Manager

The ITP Manager plays a vital role in establishing the process of gathering, integrating, analyzing, coordinating and responding to potential insider threat information.

The ITP Manager is responsible for managing and overseeing the ITP and will provide resource and staffing recommendations to the agency director or CEO.

The ITP Manager will draft and submit the ITP concept of operations plan (CONOPS) to the agency director or CEO and provide reports to the agency director or CEO concerning everything from insider threat incidents to status of existing threats to vulnerabilities and weaknesses that could lead to an insider attack to risk mitigation strategies.

# 2 - ITP Personnel

Personnel may be assigned directly to the ITP and **the ITP manager must ensure that they are trained in several different disciplines, including counterintelligence and security fundamentals to include applicable legal issues; procedures for conducting insider threat response action(s) for a potential threat or actual insider threat incident and all applicable laws and regulations regarding the gathering, integration, retention, data classification, safeguarding and use of records and data, including the consequences of misuse of such information.**

# 3 - Information Sharing

A third area under the NITP that organizations must address is enterprise information sharing. In order for the ITP to have any effect against the insider threat, **the ITP manager must direct and coordinate that all relevant organizational components, securely provide the ITP personnel with the information needed to identify, analyze, respond, mitigate or neutralize insider threat matters.**

As a part of information sharing, **the NITP also requires agencies to have an IT auditing and monitoring program.** Various security software tools can be used to audit, monitor or record the activities of insiders using computers, laptops and mobile devices that are connected to an organization's network and the Internet. Insider or user attributable activities to be audited, monitored or recorded may include prohibited activities stated in security policies, anomalous behavior, suspicious activities, unusual actions, unauthorized access to data, exceeding threshold-limits, printing and much more. Another important aspect of this program is the integration and correlation of logs from other sources, facility access logs, phone logs and other communications.

# 4 – Insider Threat Awareness Program

Finally, agencies should establish an insider threat awareness program — yet another NITP requirement. **The program must continuously educate employees on what may be considered suspicious activities, behavioral indicators, signals or indicators of espionage or malicious intent by insiders.** The importance of **detecting problems with an insider, before an incident happens, is crucial to reduce the risk of damage to the organization.** This awareness will create a "See Something-Say Something Culture." **The workforce needs to know what to report, when to report and who to report to.** Good insiders are the eyes and ears of an organization and can be the first line of defense in helping an organization protect itself from malicious insiders.

Aside from the NITP, there are other areas agencies and companies should focus on. One is the personnel security-human resources department (PSHRD). **The PSHRD is a key element supporting the ITP as it will provide services such as hiring, reference checks, law enforcement background checks, polygraphs, security briefings, continuous evaluation of personnel and terminations.**

Another best practice for organizations is to have an employee assistance program. Employees may have personal circumstances that may put the organization at risk. The program can act as a confidential open door to provide an outlet for the insider to turn to for assistance. This is a proactive step to get in front of the insider before an incident occurs.

There are several other important aspects that could proactively address insider threat risks. These could include employee satisfaction surveys, policies coupled with disciplinary actions for non-compliance, and focusing more attention and depth to an organizations vulnerabilities.

An organization must identify and inventory its most important data. Key decision makers or stakeholders must be involved from across the organization to protect the organization's data using an enterprise approach, not a silo-stove pipe approach.

Communication is critical. The workforce must be made aware of the policies and procedures for protecting the data, the sanctions or disciplinary actions for non-compliance, as well as how to report suspicious activities or indicators of a possible insider threat.

The insider threat program sits atop this security foundation as a group that is free from an organization's politics and conflicts of interest. It's number one goal is to protect the organization assets — its people and data.

Commentary Posted On-Line:
http://www.federalnewsradio.com/241/3676312/Insider-threat-training-program-starts-with-Security-101

Jim Henderson, CISSP, CCISO
Founder / Chairman Of The National Insider Threat Special Interest Group
CEO Insider Threat Defense, TopSecretProtection.Com, Inc.
Co-Founder / Chairman Of The National Insider Threat Special Interest Group
Counterespionage-Insider Threat Program Training Course Instructor
Cyber Security-Information System Security Program Management Training Course Instructor
Cyber Threat-Insider Threat Risk Assessment Auditor / Analyst
888-363-7241 / 561-809-6800
Websites
www.insiderthreatdefense.com
jimhenderson@insiderthreatdefense.com
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org