National Insider Threat Special Interest Group (NITSIG)

Preventing Insider Threats Starts With The Basics

Insider Threats Made Easy

- Insiders attempting to commit espionage against the government or businesses will in most cases exploit an organizations weakest links that give them the greatest chance of success, without being caught.
- Insiders in most cases know what is checked and not checked and know when they won't be checked or challenged.
- Just trying to use technology to detect and mitigate the Insider Threat problem is not the only answer.

The Most Basic Questions

- What Is The Organizations Weakest Points? (The Insider, Technology)
- How May An Insider First Try To Remove Or Disclose Protected Information From Your Organization?
    - Having Access To The Organizations Data On Network Shares And Databases Without A Valid Need To Know That Is Not Authorized By Management.
    - Use Of USB Storage Devices (Thumb Drives, Smart Phones, MP3 Players, Etc.)
    - Use Of Removable, Writeable Media (Floppy Disk, DVD-CD)
    - By Fax Machines, By Computer Webcams, By Using Cloud Storage, Using Stenography
    - By Using A Computers Microphone To Dictate Protected Information To A Sound File, Then E-Mailing The Sound File To The Insiders Personal E-Mail Account
    - By Scanning Sensitive Or Classified Documents To An Internet Connected Scanner With E-Mail Capabilities, And E-Mailing To The Individuals Personal E-Mail Account
    - By Company E-Mail Or Web Based Personal E-Mail
    - By Posting Information Not For Public Disclosure On Social Networking Websites, Resumes
    - By Disclosing Information Not For Public Disclosure In Public Areas, To The News Media, Other Sources, By Any Means
    - By Work Phone (Verbally Releasing Information To Competitors, Outside Sources, Etc.)
    - By Smartphone (Verbally, Pictures, Recording)
    - By Portable Hand Held Document Scanner
    - By Any Electronic Devices That The Insider Has Brought Into The Organization With Or Without Approval
    - By Walking Out The Front Door (No Security Guard Inspections)
    - By using the company's internal shipping department to ship sensitive information or intellectual property to another source outside the company. Does the company inspect packages before they are sealed and shipped?

Insider Threat Risks Of Concern

The following are some of the concerns an organization should have related to the Insider Threat:

- An Insiders Suitability For Employment, Credibility Assessments
- An Insiders Behavioral Indicators, Suspicious Activities, Signals, Actions
- Existing Threats, Vulnerabilities and Weaknesses That Could Further Enable Insider Threats
- Past Incidents Caused By Insiders
- What Protected Information Does The Organization Have (Digital , Non-Digital Storage Locations)
- An Insiders Access To Information / Need To Know, Unauthorized Access
- An Insiders Awareness To Security Policies, Procedures, Sanctions
- An Insiders Awareness On How To Report Suspicious Or Malicious Activities By Insiders
- More Focused Observation On Employees Activities Regarding Employment Status (Resignation, Termination)

- Privileged Users (Network-IT Security and Database Administrators)
- Release Of Classified, Sensitive or Intellectual Property Information Through Walk-Out, Verbal, Online Social Networking, Blogs, Electronic Devices Or Any Other Means
- Foreign Travel / Contact Reporting
- 3rd Party Insiders: Vendors, Contractors, Subcontractors, Maintenance Personnel

Challenges Detecting Insider Threats
Why Do Insiders Go Undetected?

- It is often difficult to identify Insiders who pose a threat and to detect what they are doing in time to prevent harm to the organization.
- Traditional access controls don't help, because Insiders already have access. Insiders have already obtained a badge to access significant portions of an organization's facilities, and a login and password to access significant amounts of classified information or sensitive information stored on networks.
- Espionage reports and investigations into Insider Threat incidents have shown that Insiders attempting to commit espionage will in most cases exploit an organizations weakest links that give them the greatest chance of success, without being caught.
- Some Insiders may be able to operate in a malicious manner over extended periods of time without detection. This is because employees may not be trained to recognize suspicious behaviors or activities, and may not know how to report this information.
- When employees do recognize suspicious behaviors or activities behaviors, they may be reluctant to report their co-workers. Having an anonymous reporting capability in place may reduce this reluctant to report. It is also important to note that the unwitting Insider Threat can be as much a threat as the malicious Insider Threat.
- Insiders can collect data from multiple information systems and can tamper with security logs and other audit controls. It is sometimes difficult to distinguish malicious actions from legitimate actions.
- The best Intrusion Detection Systems and Firewalls may be useless in protecting an enterprise from the Insider Threat, as they are only part of the Defense-In-Depth security strategies required to mitigate the Insider Threat.

An Insider Threat Program is designed to help address these challenges listed above and more, with an Enterprise Insider Threat Risk Management approach. An Insider Threat Program must be proactive, not reactive.

Contact Information:

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense, TopSecretProtection.Com, Inc.
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 Analyst / Risk Mitigation Specialist
888-363-7241 / 561-809-6800
Connect With Me On LinkedIn:
http://www.linkedin.com/in/isspm
Websites
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org
www.insiderthreatdefense.com
jimhenderson@insiderthreatdefense.com