Defending From Within
Lessons Learned From The Snowden Affair

Trying To Detect A Malicious Insider, Is More Then Mind Reading

Presented By:
Jim Henderson / CISSP / CCISO
Cyber Security-Insider Threat Training Program Course Instructor
Cyber Threat-Insider Threat Risk Mitigation Specialist
www.insiderthreatdefense.com
www.topsecretprotection.com
Disclaimer

The information / content presented in this document is for informational and educational purposes only.

Any information, content and opinions presented regarding a method or solution to mitigate the Insider Threat, does not imply endorsement by Insider Threat Defense, or any U.S. Government Agency.

Nothing presented in this document, or verbally presented during this presentation should be construed as legal advice or binding.

Please contact a qualified attorney to interpret any federal or state government laws, regulations, or constructs.
The Question Is Are We Learning Anything From Past Insider Threat Incidents?

Let’s First Review The Insider Threat Timeline Of Incidents, Investigations And Reports

Risk Ignorance?
Risk Acceptance?
Risk Transfer?
Risk Mitigation?
What We Know About The Snowden Incident

- Access to large amounts of highly classified information.
- Ability To exfiltrate large amounts of highly classified information without being detected.
- DLP / Insider Threat Auditing And Monitoring Tool Used Not Installed At His Work Location.
- Had Assistance From Co-Worker.
- On June 14, 2013, United States federal prosecutors filed a criminal complaint against Snowden, charging him with theft of government property, and alleging he had violated the U.S.'s 1917 Espionage Act through unauthorized communication of national defense information and "willful communication of classified communications intelligence information to an unauthorized person."
- In March 2014, Snowden stated that he had reported policy or legal issues related to spying programs to more than 10 officials, but as a contractor had no legal avenue to pursue further whistleblowing.
What We Know About The WikiLeaks / PVT Bradley Manning Incident

Potential Espionage Indicator

- While in Army Intelligence School PVT Manning was reprimanded for posting messages to friends on YouTube that apparently revealed sensitive information.

- PVT Manning displayed anti-social behavior. At Fort Drum Manning had trouble with his roommates, screamed at superior officer and was referred to an Army mental health counselor.

Contributing To The WikiLeaks Incident

- Access to large amounts of highly classified information.
- Ability To exfiltrate large amounts of highly classified information without being detected.
Manning discussed how common and easy it was for soldiers to bring removable media into their work environment, making it easy for him, or anyone else, to siphon data from classified networks without raising suspicion.

(01:52:30 PM) Manning: funny thing is... we transferred so much data on unmarked CDs...
(01:52:42 PM) Manning: everyone did... videos... movies... music
(01:53:05 PM) Manning: all out in the open
(01:53:53 PM) Manning: bringing CDs too and from the networks was/is a common phenomenon
(01:54:14 PM) Lamo: is that how you got the cables out?
(01:54:28 PM) Manning: perhaps
(01:54:42 PM) Manning: i would come in with music on a CD-RW
(01:55:21 PM) Manning: labelled with something like “Lady Gaga”... erase the music... then write a compressed split file
(01:55:46 PM) Manning: no-one suspected a thing
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 Are The Organizations Weakest Points?

How May An Insider First Try To Remove Or Disclose Protected Information From Your Organization?

- Government agencies and defense contractors (DoD, IC, DIB) spend millions of dollars on Certification and Accreditation to lock down information systems.
  - Yet access to the information is not always limited to individuals with a need to know (Open Network Shares, Databases, Etc.)
- By Use Of USB Storage Devices (Portable Hard Drives, Thumb Drives, MP3 Players, Etc.)
- By Use Of Smartphones (Verbally, Pictures, Recording)
- By Using A Smartphone’s Hot Spot Capability To Connect A Classified Standalone Computer System To The Internet, Then Upload The Classified Information To Webmail Or Any Other Source.
- By Use Of Removable, Writeable Media (Floppy Disk, DVD-CD)
- By Use Of Fax Machines, Multi-Function Devices Connected to Internet (Without Authentication)
- By Using Computer Webcams, By Using Cloud Storage.
- By Using Stenography Software Application (Not Preventing Software Installs)
• By Using Screen Sharing Software (No Installation Required) On Un-Classified Systems That Contain Sensitive Information.
• By Using A Computer's Microphone To Dictate Classified Information To A Sound File, Then E-Mailing The Sound File To The Insider's Personal E-Mail Account.
• By Scanning Sensitive Or Classified Documents To An Unattended Internet Connected Scanner With E-Mail Capabilities, And E-Mailing To The Individual's Personal E-Mail Account.
• By Downloading All The Information From A Network Share, To A Local Hard Drive (1st). Then Disconnecting The Computer From The Network. Install 2nd Hard Drive. Boot From CD And Clone to 1st Hard Drive. Walk Out Door With HD.
• By Using A Portable Hand Held Document Scanner.
• By Using E-Mail Or Web Based Personal E-Mail, Or Using Other FREE Internet Based Large File Transfer Services.
• By Posting Information Not For Public Disclosure On Social Networking Websites, Resumes
• By Having Discussions In Public Areas, About Information That Is Sensitive And Not For Public Release
• By Walking Out The Front Door (No Security Guard Inspections)

Data Exfiltration Enablers - From Simple To Advanced
Malicious Insider Tactics And Behaviors

What are some of the tactics and behaviors of past malicious Insiders?

The CERT Insider Threat Center conducted an analysis of 120 espionage cases in 2010. They mapped the espionage cases to the DoDI 5240.06 Counterintelligence Awareness And Reporting.

Espionage Cases Analyzed

<table>
<thead>
<tr>
<th>Abugida</th>
<th>Haseen</th>
<th>Navy - United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Al Halabi</td>
<td>Ahmad</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Allen</td>
<td>Michael</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Ames</td>
<td>Aldrich</td>
<td>Central Intelligence Agency (CIA)</td>
</tr>
<tr>
<td>Anderson</td>
<td>Ryan</td>
<td>Army - National Guard</td>
</tr>
<tr>
<td>Anzalone</td>
<td>Charles</td>
<td>Marine Corps</td>
</tr>
<tr>
<td>Alainoni</td>
<td>Leandro</td>
<td>Federal Bureau of Investigation (FBI)</td>
</tr>
<tr>
<td>Baba</td>
<td>Stephen</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Bell</td>
<td>William</td>
<td>Hughes Aircraft</td>
</tr>
<tr>
<td>Bergersen</td>
<td>Oreaq</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>Betts</td>
<td>Greer</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Brackenbaut</td>
<td>Herbert</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Boone</td>
<td>David</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>Bostron</td>
<td>John</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>Carney</td>
<td>Jeffrey</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Casolino</td>
<td>Giuseppe</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Charlton</td>
<td>John</td>
<td>Lockheed Martin Corporation</td>
</tr>
<tr>
<td>Chin</td>
<td>Larry</td>
<td>Central Intelligence Agency (CIA)</td>
</tr>
<tr>
<td>Chung</td>
<td>Donfan</td>
<td>Boeing Company</td>
</tr>
<tr>
<td>Clark</td>
<td>James</td>
<td>Department of State</td>
</tr>
<tr>
<td>Country</td>
<td>Alan</td>
<td>Marine Corps</td>
</tr>
<tr>
<td>Coleman</td>
<td>William</td>
<td>Naval Reserve - United States</td>
</tr>
<tr>
<td>Conrad</td>
<td>Clyde</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Cooke</td>
<td>Christopher</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Corley</td>
<td>Robert</td>
<td>Marine Corps</td>
</tr>
<tr>
<td>Davies</td>
<td>Allen</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Davenport</td>
<td>Rahag</td>
<td>Johns Hopkins Applied Physics Laboratory</td>
</tr>
<tr>
<td>Diaz</td>
<td>Matthew</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Dolese</td>
<td>Thomas</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Drummond</td>
<td>Nelson</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Ellis</td>
<td>Robert</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Farnsworth</td>
<td>John</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Fundt</td>
<td>James</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>Ford</td>
<td>Kenneth</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>Franklin</td>
<td>Lawrence</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>French</td>
<td>George</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Gessner</td>
<td>George</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Gowada</td>
<td>Nashr</td>
<td>Northrop Corporation</td>
</tr>
<tr>
<td>Graf</td>
<td>Ronald</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Greenlief</td>
<td>David</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Greiner</td>
<td>Douglas</td>
<td>Central Intelligence Agency (CIA)</td>
</tr>
<tr>
<td>Grunden</td>
<td>Oliver</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Hagwood</td>
<td>Robert</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Hall</td>
<td>James</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Hamilton</td>
<td>Frederick</td>
<td>Defense Intelligence Agency</td>
</tr>
<tr>
<td>Hansen</td>
<td>Robert</td>
<td>Federal Bureau of Investigation (FBI)</td>
</tr>
<tr>
<td>Harris</td>
<td>Ulysses</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Hellenbeck</td>
<td>Joseph</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Horton</td>
<td>Brian</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Name</td>
<td>Occupation</td>
<td>Agency/Department</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Howard</td>
<td>Edward</td>
<td>Central Intelligence Agency</td>
</tr>
<tr>
<td>Jenett</td>
<td>Eric</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Kadieh</td>
<td>Ben-Ami</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Kean</td>
<td>Bruce</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Keyser</td>
<td>Donald</td>
<td>Department of State</td>
</tr>
<tr>
<td>Kim</td>
<td>Robert</td>
<td>Office of Naval Intelligence</td>
</tr>
<tr>
<td>King</td>
<td>Donald</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Kunkle</td>
<td>Craig</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Lallas</td>
<td>Stephen</td>
<td>Department of State</td>
</tr>
<tr>
<td>Ledbetter</td>
<td>Gary</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Lee</td>
<td>Peter</td>
<td>Los Alamos National Laboratory</td>
</tr>
<tr>
<td>Lee</td>
<td>Wen</td>
<td>Los Alamos National Laboratory</td>
</tr>
<tr>
<td>Lessenhien</td>
<td>Kurt</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Leung</td>
<td>Katrina</td>
<td>Federal Bureau of Investigation (FBI)</td>
</tr>
<tr>
<td>Linka</td>
<td>Robert</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>Longdon</td>
<td>Clayton</td>
<td>Marine Corps</td>
</tr>
<tr>
<td>Madsen</td>
<td>Lee</td>
<td>Defense Intelligence Agency</td>
</tr>
<tr>
<td>Mak</td>
<td>Chi</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Mekhalba</td>
<td>Ahmed</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>Meng</td>
<td>Xiaodong</td>
<td>Quantum3D, Inc.</td>
</tr>
<tr>
<td>Mintkenbaugh</td>
<td>James</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Mira</td>
<td>Francisco</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Mohammed</td>
<td>Ali</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Montanaro</td>
<td>Ronald</td>
<td>Defense Intelligence Agency</td>
</tr>
<tr>
<td>Montes</td>
<td>Ana</td>
<td>Defense Intelligence Agency</td>
</tr>
<tr>
<td>Moore II</td>
<td>Edwin</td>
<td>Central Intelligence Agency</td>
</tr>
<tr>
<td>Morison</td>
<td>Samuel</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Mueller</td>
<td>Gustav</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Nestadt</td>
<td>Frank</td>
<td>Los Alamos National Laboratory</td>
</tr>
<tr>
<td>Nicholson</td>
<td>Harold</td>
<td>Central Intelligence Agency</td>
</tr>
<tr>
<td>Ott</td>
<td>Bruce</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Patton</td>
<td>Ronald</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>Peri</td>
<td>Michael</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Perkins</td>
<td>Walter</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Pickering</td>
<td>Jeffrey</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Pitts</td>
<td>Earl</td>
<td>Federal Bureau of Investigation (FBI)</td>
</tr>
<tr>
<td>Pollard</td>
<td>Jonathan</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Ramsay</td>
<td>Roderick</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Regan</td>
<td>Brian</td>
<td>National Reconnaissance Office (NRO)</td>
</tr>
<tr>
<td>Rhodes</td>
<td>Roy</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Richardson</td>
<td>Daniel</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Rondeau</td>
<td>Jeffrey</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Rosenberg</td>
<td>Julius</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Schoon</td>
<td>Charles</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Schwartz</td>
<td>Michael</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Sellon</td>
<td>Philip</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Smith</td>
<td>Richard</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Smith</td>
<td>Timothy</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Snell</td>
<td>Morton</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>Sommersay</td>
<td>Albert</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Spade</td>
<td>Henry</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Squillace</td>
<td>Theresa</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>Stabo</td>
<td>Zoltan</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Thompson</td>
<td>Harry</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Tobias</td>
<td>Michael</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Trottmann</td>
<td>George</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Varker</td>
<td>Otto</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Walker</td>
<td>Arthur</td>
<td>VSE Corporation</td>
</tr>
<tr>
<td>Walker</td>
<td>John</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Walker</td>
<td>Michael</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Warren</td>
<td>Kelly</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Weinmann</td>
<td>Ariel</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Whalen</td>
<td>William</td>
<td>Army - United States</td>
</tr>
<tr>
<td>Whitworth</td>
<td>Jerry</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Wittman</td>
<td>James</td>
<td>Navy - United States</td>
</tr>
<tr>
<td>Woznieski</td>
<td>Jean-Philippe</td>
<td>Australian Defense Intelligence Organization</td>
</tr>
<tr>
<td>Wolf</td>
<td>Ronald</td>
<td>Air Force - United States</td>
</tr>
<tr>
<td>Wood</td>
<td>James</td>
<td>Air Force - United States</td>
</tr>
</tbody>
</table>
Personal Predispositions / Contributing Factors

Organizational Contributors and Mitigators

Non-Organizational Contributors and Mitigators

Crime Script

Concerning Behaviors

Personal Stressors

Professional Stressors

Personal Predispositions

Incident
# Personal Predispositions / Contributing Factors

<table>
<thead>
<tr>
<th>Personal Predispositions</th>
<th>Stressors</th>
<th>Concerning Behavior</th>
<th>Crime Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mental Health Issues</td>
<td>Financial Stressors</td>
<td>Deception: Non-Technical</td>
<td>Information Transfer</td>
</tr>
<tr>
<td>Social Skills and Decision Making Deficits</td>
<td>Personal Stressors</td>
<td>Financial Issues</td>
<td>Deception: Technical</td>
</tr>
<tr>
<td></td>
<td>Professional Stressors</td>
<td>Social Networks</td>
<td>Unauthorized Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suspicious Travel</td>
<td>Unauthorized Modifications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communication: Non-Technical</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communication: Technical</td>
<td></td>
</tr>
</tbody>
</table>
Insider Actions Mapped To DoDI 5240.06

- E3.1.1 – Unauthorized contact 107/120
- E3.1.4 - Attempts to Obtain Classified Materials 28/120
- E3.1.8 – Keeping Classified Material 50/120
- E3.1.9 – Access without Authorization 10/120
- E3.1.10 – Transmitting Classified Material 20/120
- E3.1.12 – Removing Classified Material 71/120
- E3.1.14 – Discussing Classified Material 45/120
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 organization’s 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. Threat.
- An Insider Threat Program (ITP) is designed to help address these challenges listed above and more, with an enterprise Insider Threat Risk Management approach.
National Insider Threat Program Policy

- Designate an Insider Threat Senior Official
- Promulgate overarching Insider Threat Policy and Implementation Plan (Examples: DOE, DSS)
- **Implement An Insider Threat Program:**
  - User Activity Monitoring Of Classified Networks
  - Evaluation Of Personnel Security Information
  - Employee Awareness Training
  - Training Specific To Insider Threat Program Personnel
  - Analysis, Reporting, And Response
  - Protection Of Civil Liberties
- Perform Self-Assessments
- Produce Annual Report On Insider Threat Program Status
- Enable Independent Assessments By The NITTF
Insider Threat Program - Risk Mitigation Framework

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 Insider Threat Program (ITP) that is comprised of individuals from various departments, business units and supporting functions. Because each organization is unique, the structure of the ITP may be different.

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 Insider.

ITP Core Goals

The core goals of an ITP are to integrate and utilize the various security disciplines, business units and functions in an organization to support the ITP. Existing security disciplines and business units must work together in concert and concentrate their efforts on protecting the organizations critical assets.

The ITP will:

1) Develop a mutually supportive Enterprise Insider Threat Risk Management Framework.
2) Develop and implement sharing policies and procedures so the organization’s ITP can access, share, and integrate information and data derived from various security disciplines and departments from across the organization, including CI, Security, Information Assurance, Human Resources, Personnel Security offices, etc.
3) Provide much greater attention to ensure that basic and simple security countermeasures (Policies, Procedures, Awareness Training, Physical, Operational and Technical Security Controls) are in place, functioning and operating as intended.
4) Identify and assess existing threats, vulnerabilities and weaknesses that could enable Insider Threats, and develop additional risk mitigation strategies as need to protect the organizations data, information systems and networks.
5) Investigate and respond to threats against an organization assets by Insiders.
Insider Threat Program Team

ITP Team Members
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. Names may vary depending on the organization.

- Insider Threat Program Manager, Insider Threat Program Personnel
- Human Resources / Personnel Security
- Physical Security / Facility Security
- Counterintelligence Investigators
- C-Suite Management (CEO) / Senior Directors
- Mid Level Management / Business Unit Managers
- Chief Risk Officer / Risk Management
- Chief Privacy Officer
- Chief Information Officer (CIO) / Information Technology (IT) Department
- Chief Information Security Officer (CISO)
- Cyber Security Program Manager
- Information Systems Security Manager / Officer
- Information Assurance Manager / Officer
- Network Security / IT Security / Database Administrators
- Security, Education Training And Awareness
- Computer Security Incident Response Team
- Records / Information Management
- Legal / General Counsel
ITP Concept Of Operations (CONOP)

- A CONOP should be developed for ITP. The CONOP provides for a plan of actions and expectations. It should be reviewed at all organizational levels, to include the organizations legal department.
- The CONOP formalizes the roles, expectations and contributions of each security discipline and supporting elements. It also identifies limitations and restrictions to ensure each security discipline and supporting elements conduct activities within their authorities. It also lays out the plan for collection, handling, and analysis of data.
- It outlines the notification procedures and the referral process for findings reported by the Suspicious Activity Reporting Program and other sources. It should also identify and reference any Memo of Understanding (MOU) / Memo Of Agreement (MOA) between business units or other business partners connected to the organizations network.

Insider Threat Defense Program Information

- All ITP Personnel who manage or support the ITP must protect the information, documents, files and material they handle in connection with their ITP duties in accordance with the sensitivity or classification of the information, and in accordance with current and applicable Federal laws, rules, regulations, and policy.
- All ITP personnel managing and supporting the ITP at any level will complete a nondisclosure agreement.
- The organizations security classification guide or data management plan must provide guidance on how ITP information is marked and protected.
Insider Threat Risk Management

Organizations need to conduct an Insider Threat Risk Assessment to assess their vulnerability to the Insider Threat.

This Risk Assessment Will:

1) Identify all the weaknesses, threats and vulnerabilities within the organization that could enable an Insider Threat.
2) Provide visibility into the areas that the organization can take (Implement, Enhance) to detect, deter, mitigate or prevent an Insider Threat incident.

Examples Of Problems That An Insider Threat Risk Assessment Might Provide:

- Inadequate security policies and procedures
- Inadequate Insider Threat Awareness Training
- Inadequate Management, Operational and Technical Control for Information Systems Security
- Risks posed by 3\textsuperscript{rd} Party Insiders: Vendors, Contractors, Subcontractors, Maintenance Personnel
- Inadequate Insider Threat Program Personnel (More People Needed, Specialized Training Needed)

Insider Threat Risk Mitigation

- A Plan Of Action & Milestones POA&M’S process can provide a roadmap of an organization security weaknesses and Insider Threat Program weaknesses.
- The POA&M will help to identify mitigation strategies needed, funding required and prioritize, monitor and report on the progress of corrective actions needed to the security posture of an organization.
HOW BAD IS THE INSIDER THREAT PROBLEM?

**Investigator Discusses Navy Yard Findings, Insider Threat**
3 weeks ago
www.defense.gov

**97% of U.S. Enterprises Fear Insider Security Threats**
Dan Kobialka, Vormetric, an enterprise data security solutions provider, last week released its latest Insider Threat report of big data, cloud and IT security threats.
2 weeks ago
mspmentor.net

**Biggest source of DOD's cyber threats: inept co-workers**
2 weeks ago
defensesystems.com

**INSA Publishes White Paper on Insider Threat Programs in the US**
The Cyber Council Insider Threat Task Force of the Intelligence and National Security Alliance (INSA) has published a white paper called "A Prel......
3 months ago
news.softpedia.com

**Unintentional Insider Threats: A Foundational Study**
Software Engineering Institute, Carnegie Mellon University,
3 months ago
resources.sei.cmu.edu

**Half of IT Decision-Makers Admit They're Vulnerable to Insider Threats**
3 months ago
www.esecurityplanet.com

**The Enemy Within: an emerging threat...**
true...
2 months ago
www.clearswift.com
US Navy Bribery Scandal: The Fourth Officer’s ‘Bucket List’ in Exchange for Classified
5 minutes ago
www.ntd.tv

Ex-Microsoft Employee Charged With Trade Secret Theft
1 month ago
www.bloomberg.com

How Microsoft tracked down a spy who leaked its secrets
4 weeks ago
www.zdnet.com

Edward Snowden: the whistleblower behind the NSA surveillance revelations
2 months ago
www.theguardian.com

NSA employee implicated in Snowden probe resigned, memo says
2 months ago
www.washingtonpost.com

Rules that keep feds from trolling Facebook, Twitter could have led to Snowden, Alexis
1 month ago
p.washingtontimes.com

Report: Secret budget cited 4,000 NSA leaks
2 months ago
www.cbsnews.com

Ex-State Department advisor Stephen J. Kim sentenced in leak case
A former State Department arms expert who leaked classified information to a Fox News reporter was sentenced Wednesday to 13 months in prison after a pointed court-
Hundreds of Classified Leaks Under Review by IC Inspector General

Hundreds of cases of unauthorized disclosures of classified information were under review by the Office of the Inspector General of the U.S. Intelligence Community

2 months ago
blogs.fas.org

APNewsBreak: Defense contractor to plead guilty

1 month ago
www.federalnewsradio.com

Engineer accused of trying to smuggle military jet engine documents, blueprints to Iran

3 months ago
www.foxnews.com

Army Officer Freaks Out Thousands Of Government Employees With Cybersecurity

1 month ago
www.businessinsider.com

Stolen F-35 secrets now showing up in China’s stealth fighter

1 month ago
www.foxnews.com

Hawaii soldier accused of spying convicted

2 months ago
www.hawaiinewsnow.com

Navy Suspends Admirals’ Access to Classified Information

The U.S. Navy suspended access to classified information for two of its top admirals handling intelligence matters after putting them on leave this week pending a review of

3 months ago
www.bloomberg.com

Naval Espionage: Stopping a Dangerous Insider Threat

1 month ago
www.fbi.gov
Former defense contractor pleads guilty to sharing classified documents
Federal prosecutors say 50-year-old Bruce Schliemann, a former defense contractor and retired Navy SEAL, faces up to one year in prison and/or a fine of up to $100,000 when

WASHINGTON: ‘Zero Dark Thirty’ leak investigators now target of leak probe | Insider

IRS Financial Systems Vulnerable to Insider Threats

Congress Presses TSA To Crack Down On “Insider Threats” From It’s Own Employees

LewisGale Regional Health System Suffers Insider Breach

Arcadia Home Care Acknowledges Insider Breach

Leader of ID Theft Ring Targeting Government Employees Sentenced to 12
IRS Employee Takes Home Thumb Drive With Data on 20,000 Colleagues

1 month ago
www.nextgov.com

Fort Benning Employee Charged with $2.2 Million Identity Theft Scheme Targeting
Tracy Mitchell allegedly used service members' stolen identities to file more than 1,000 fraudulent tax returns....

2 months ago
www.esecurityplanet.com

Miami Police Officer Gets 12 Years in Prison for Identity Theft
Malinsky Bazile used Florida's driver's license database to steal the identities of 700 middle-aged women....

2 months ago
www.esecurityplanet.com

Two Men Jailed for Identity Theft at Medical Lab
Angelo Ponds and Sean Guillaume were sentenced to 48 months and 94 months in prison, respectively....

2 months ago
www.esecurityplanet.com

Insider threat
Whether malicious or unintentional, the risk from employees - on premise or contracted - continues.

Home Depot Employees Arrested for Insider Breach

2 months ago
www.esecurityplanet.com

Former Mount Sinai Medical Center Employee Jailed for Identity Theft
Oliver Gayle was sentenced to 51 months in prison....

2 months ago
www.esecurityplanet.com

Former TD Bank Employee Admits Identity Theft

1 month ago
www.esecurityplanet.com
North Country Hospital Acknowledges Another Data Breach
2 months ago
www.esecurityplanet.com

Two Sentenced for Identity Theft Scheme Targeting U.S. Government Employees
3 months ago
www.esecurityplanet.com

Log audit reveals developer outsourced his job to China
3 months ago
www.net-security.org

Feds: Ex-Lilly employees sold secrets
3 months ago
www.theindychannel.com

Veterans’ Hospital Volunteer Charged with Theft of Patients’ Identities
Ricardo Jacinto Rodriguez is accused of stealing 106 patients’ names and Social Security numbers, which were then used to file fraudulent tax returns....
3 months ago
www.esecurityplanet.com

Prison Medical Records Clerk Indicted for Identity Theft
3 months ago
www.esecurityplanet.com

State Farm Admits Insider Data Breach
A call center employee misused at least 11 customers’ credit card numbers.....
3 months ago
www.esecurityplanet.com

Holy Cross Hospital Acknowledges Insider Breach
Patients’ names, birth dates, addresses and Social Security numbers were accessed by a former employee....
3 months ago
www.esecurityplanet.com
California’s Northern Inyo Hospital Suffers Insider Data Breach
'A hospital can only do so much in the case of a rogue employee,' hospital administrator John Halfen said....

3 months ago
www.esecurityplanet.com

Bed Bath and Beyond Acknowledges Insider Breach
A cashier stole an undisclosed number of customers' credit card information....

3 months ago
www.esecurityplanet.com

HSBC Acknowledges Insider Breach

3 months ago
www.esecurityplanet.com

UConn Health Center Admits Second Insider Breach This Year

3 months ago
www.esecurityplanet.com

W.J. Bradley Mortgage Capital Admits Insider Breach

3 months ago
www.esecurityplanet.com

Providing peace of mind is how we’re engineering a better world. • Intel® Core™ i5 vPro™ processor

Learn More

Washington Court Clerk Fired for Insider Breach

3 months ago
www.esecurityplanet.com

Riverside Health System Acknowledges Four-Year Insider Breach

3 months ago
www.esecurityplanet.com

Systems Administrator Admits Sabotaging Ex-Employer's Server

3 months ago
www.esecurityplanet.com
PAST MISTAKES
NOT BEING PROACTIVE
+ NO COMMITMENT TO ADDRESS MOST BASIC RISKS
  + VULNERABILITIES / WEAKNESSES
+ NO INSIDER THREAT RISK MITIGATION PROGRAM
  + RISK AVOIDANCE, +RISK TRANSFER,
  +RISK ACCEPTANCE
+ NO DETERNANTS TO INSIDERS
= INSIDER THREAT
LESSONS TO BE LEARNED

- The Insider Threat problem is real and here to stay unless we learn from our past mistakes and failures.

- This is a National Security problem, not just for the U.S. Government, but for DoD, IC and DIB contractors and private sector organizations.

- DIB contractors should not wait for a revision to the NISPOM to take action. Steps can be taken now to develop and implement an Insider Threat Program, using the National Insider Threat Policy as a reference and basic framework until formal policy and guidance is released. Build something and start mitigating Insider Threat risks now, before your company makes the headlines.

- Insider Threat auditing and monitoring tools support the Insider Threat Program, but are only 1 of many countermeasures that can be implemented to detect, deter and mitigate the Insider Threat.

- Going forward U.S. Government agencies and DoD, IC and DIB contractors and business must be proactive, think outside the box and expanded their vision of the many vulnerabilities that exist in their organizations.

- To combat malicious Insiders will require a serious commitment from EVERYONE. Senior DoD, IC, Government Officials, Senior Management for DoD, IC, DIB Contractors, Supervisors, Managers and the workforce.

- Without a commitment from the top on down, we will continue to see more Insiders go bad. A point to make here is; “Your Only As Strong As Your Weakest Link”. This is a TEAM EFFORT, not just a security problem.

- A breakdown from the top on down in funding, policies, support, communication, information sharing, common sense, etc. is a vulnerability waiting to be exploited by the “Malicious Insider”.

Organization must change their current Insider Threat Risk Avoidance Strategy from; “Hoping It Won’t Happen” or the “Just Accept The Risk Mentality”. These Insider Threat Risk Mitigation Strategies have not been successful and are no longer acceptable when protecting an organization’s critical assets.
QUESTIONS?

Are You Ready To Build Your Insider Threat Program?
CONTACT INFORMATION

Jim Henderson, CISSP, CCISO
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 / E-Mail Addresses:
www.insiderthreatdefense.com
jimhenderson@insiderthreatdefense.com
www.nationalinsiderthreats sig.org
jimhenderson@nationalinsiderthreats sig.org