What to Know About Insider Threat and How to Mitigate it

or why…

Hope…is NOT a Strategy!

Michael C. Theis, CISSP, SSA (retired)
Chief Counterintelligence Expert
Technical Lead of Insider Threat Research
and Senior Member of the Technical Staff

CERT Insider Threat Center
Notices

© 2014 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN “AS IS” BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.
What is the CERT Insider Threat Center?

Center of insider threat expertise

Began working in this area in 2001 with the U.S. Secret Service

Our mission: The CERT Insider Threat Center conducts empirical research and analysis to develop & transition socio-technical solutions to combat insider cyber threats.
CERT’s Unique Approach to the Problem

Research Models

Deriving Candidate Controls and Indicators

Our lab transforms that into this...

Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was disabled. *" | eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name "@corp.merit.lab" sender_address | fields - Account_Name] total_bytes > 50000 AND recipient_address!="*corp.merit.lab" startdaysago=30 | fields client_ip, sender_address, recipient_address, message_subject, total_bytes'
Goal for an Insider Threat Program
The Insider Threat

There is not one “type” of insider threat

- Threat is to an organization’s critical assets
  - People
  - Information
  - Technology
  - Facilities
- Based on the motive(s) of the insider
- Impact is to Confidentiality, Availability, Integrity

There is not one solution for addressing the insider threat

- Technology alone may not be the most effective way to prevent and/or detect an incident perpetrated by a trusted insider
What is a Malicious Insider Threat?

Current or former employee, contractor, or other business partner who

- has or had authorized access to an organization’s network, system or data and
- intentionally exceeded or misused that access in a manner that
- negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.
What is an Unintentional Insider Threat?

Current or former employee, contractor, or other business partner who

- who has or had authorized access to an organization’s network, system, or data and who, through
- their action/inaction without malicious intent
- cause harm or substantially increase the probability of future serious harm to the confidentiality, integrity, or availability of the organization’s information or information systems.
Critical Infrastructure Sectors

US Cases by Sectors (Top 6) and Type of Crime

- Theft IP
- Sabotage
- Fraud

- Banking and Finance
- Information Technology
- Government-State/Local
- Commercial Facilities
- Healthcare and Public Health
- Government-Federal
- All other sectors
The Current State of Insider Threats in Organizations
2014 US State of Cybercrime Survey - 1

CSO Magazine, USSS, CERT & PWC

557 respondents

29% of organizations had 500 – 5000 employees

43% of organizations had less than 500 employees

Percentage of Participants Who Experienced an Insider Incident


What percent of the Electronic Crime events are known or suspected to have been caused by:

- **Outsiders**: 37%
- **Insiders**: 32%
- **Unknown**: 31%

2014 US State of Cybercrime Survey -3

*For organizations that could assess the damage from an incident:*

- Insider Incidents were more damaging – 46%
- Outsider incidents were more damaging – 54%

### 2014 US State of Cybercrime Survey -4

<table>
<thead>
<tr>
<th>46% of respondents</th>
<th>Damage caused by insider attacks more damaging than outsider attacks</th>
</tr>
</thead>
</table>

Insiders made up the highest percentage of the following incidents:

<table>
<thead>
<tr>
<th>Incident</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private or sensitive information unintentionally exposed</td>
<td>(82%)</td>
</tr>
<tr>
<td>Confidential records compromised or stolen</td>
<td>(76%)</td>
</tr>
<tr>
<td>Customer records compromised or stolen</td>
<td>(71%)</td>
</tr>
<tr>
<td>Employee records compromised or stolen</td>
<td>(63%)</td>
</tr>
</tbody>
</table>


Insider Threat Activities
Types of Insider Activities -1

Insider IT Sabotage

• An insider’s use of IT to direct specific harm at an organization or an individual
  – Deletion of information
  – Bringing down systems
  – Web site defacement to embarrass organization

Insider Theft of Intellectual Property

• An insider’s use of IT to steal intellectual property from the organization
  – Proprietary engineering designs, scientific formulas, etc.
  – Proprietary source code
  – Confidential customer information
  – Industrial Espionage and Trade Secrets
Types of Insider Activities -2

Insider Fraud

- An insider’s use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud
  - Payroll
  - Reimbursement
  - Unauthorized acquisitions
- Theft and sale of confidential information
  - SSN, PII, etc.
  - Credit card numbers
- Modification of critical data for a fee
  - driver’s license records
  - criminal records
  - qualification for welfare, etc.

Unintentional Insider Threat (UIT)

- An insider whose actions or lack of action without malicious intent causes harm or the possibility of harm
## Types of Insider Activities -3

**UIT - Four Categories:**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| **DISC** | accidental disclosure (e.g., via the internet)  
  sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail |
| **UIT-HACK** | malicious code (UIT-HACKing, malware/spyware)  
  an outsider’s electronic entry acquired through social engineering (e.g., phishing email attack, planted or unauthorized USB drive) and carried out via software, such as malware and spyware |
| **PHYS** | improper/accidental disposal of physical records  
  lost, discarded, or stolen non-electronic records, such as paper documents |
| **PORT** | portable equipment no longer in possession  
  lost, discarded, or stolen data storage device, such as a laptop, PDA, smart phone, portable memory device, CD, hard drive, or data tape |
Types of Insider Activities -4

Insider National Security Espionage

- The act of communicating, delivering or transmitting information pertaining to the national defense of the United States to any foreign government or faction, with intent or reason to believe that is to be used to the injury of the United States or to the advantage of a foreign nation
  - Volunteers
  - Recruited in Place
  - Dispatched

Insider Miscellaneous

- Unauthorized disclosure (information insider believed should be in the public domain)
- Providing address of a person to an acquaintance who physically harmed the individual
- Accessing records of high-profile individuals
## Summary of Insider Threats

<table>
<thead>
<tr>
<th></th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current or former employee?</strong></td>
<td>Former</td>
<td>Current</td>
<td>Current (within 30 days of resignation)</td>
</tr>
<tr>
<td><strong>Type of position</strong></td>
<td>Technical (e.g. sys admins, programmers, or DBAs)</td>
<td>Non-technical (e.g. data entry, customer service) or their managers</td>
<td>Technical (e.g. scientists, programmers, engineers) or sales</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td>Male</td>
<td>Fairly equally split between male and female</td>
<td>Male</td>
</tr>
<tr>
<td><strong>Target</strong></td>
<td>Network, systems, or data</td>
<td>PII or Customer Information</td>
<td>IP (trade secrets) – or customer Info</td>
</tr>
<tr>
<td><strong>Access used</strong></td>
<td>Unauthorized</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
<tr>
<td><strong>When</strong></td>
<td>Outside normal working hours</td>
<td>During normal working hours</td>
<td>During normal working hours</td>
</tr>
<tr>
<td><strong>Where</strong></td>
<td>Remote access</td>
<td>At work</td>
<td>At work</td>
</tr>
</tbody>
</table>
Mitigation Strategies
## Best Practices for Insider Threat Mitigation

<table>
<thead>
<tr>
<th>Consider threats from insiders and business partners in enterprise-wide risk assessments.</th>
<th>Institutionalize system change controls.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearly document and consistently enforce policies and controls.</td>
<td>Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.</td>
</tr>
<tr>
<td>Incorporate insider threat awareness into periodic security training for all employees.</td>
<td>Monitor and control remote access from all endpoints, including mobile devices.</td>
</tr>
<tr>
<td>Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.</td>
<td>Develop a comprehensive employee termination procedure.</td>
</tr>
<tr>
<td>Anticipate and manage negative issues in the work environment.</td>
<td>Implement secure backup and recovery processes.</td>
</tr>
<tr>
<td>Know your assets.</td>
<td>Develop a formalized insider threat program.</td>
</tr>
<tr>
<td>Implement strict password and account management policies and practices.</td>
<td>Establish a baseline of normal network device behavior.</td>
</tr>
<tr>
<td>Enforce separation of duties and least privilege.</td>
<td>Be especially vigilant regarding social media.</td>
</tr>
<tr>
<td>Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.</td>
<td>Close the doors to unauthorized data exfiltration.</td>
</tr>
<tr>
<td>Institute stringent access controls and monitoring policies on privileged users.</td>
<td></td>
</tr>
</tbody>
</table>

Source: Common Sense Guide to Mitigating Insider Threat; http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017
## Mitigation Strategies for Unintentional Insider Threats

<table>
<thead>
<tr>
<th>Threat Vector</th>
<th>UIT-HACK</th>
<th>DISC</th>
<th>PHYS</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training to heighten awareness and reduce human error (BP 3)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Usability of software and tools to reduce human error</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management practices to reduce likelihood of human error (BP 5)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Email safeguards (anti-phishing, anti-malware) (BP 18)</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewalls</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus/anti-malware protection (BP 19)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Data encryption on storage devices (BP 13, 19)</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Password protection on storage devices (BP 7,19)</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Wireless and Bluetooth safeguards (disable, protect) (BP 13)</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Remote memory wipe for lost equipment (BP 13, 19)</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
CERT’s Insider Threat Controls (Public)

- Insider Threat Control: Using Plagiarism Detection Algorithms to Prevent Data Exfiltration in Near Real Time
- Using a SIEM signature to detect potential precursors to IT Sabotage
- Using Centralized Logging to Detect Data Exfiltration Near Insider Termination
- Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources
- Using Universal Serial Bus (USB) Device Auditing to Detect Possible Data Exfiltration by Malicious Insiders
- Detecting and Preventing Data Exfiltration via Encrypted Web Sessions using Traffic Inspection
The Three Pillars of a Robust Strategy

- Accurately Trust
- Right-size Permissions
- Effective Monitoring

No Insider Threat
CERT Insider Threat Center Resources
CERT Insider Threat Resources

Insider Threat Center website (www.cert.org/insider-threat/)

Common Sense Guide to Mitigating Insider Threats, 4th Ed. (www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm)

The Insider Threat and Employee Privacy: An Overview of Recent Case Law, Computer Law and Security Review, Volume 29, Issue 4, August 2013 by Carly L. Huth

New technical controls from CERT Insider Threat Lab

The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) (SEI Series in Software Engineering) by Dawn M. Cappelli, Andrew P. Moore and Randall F. Trzeciak
CERT Insider Threat Catalogue

Content

1. About the Software Engineering Institute
2. About the CERT Insider Threat Center
3. Insider Threat Best Practices
4. Insider Threat Vulnerability Assessment
5. Insider Threat Program Evaluation
6. Insider Threat Program Development Workshop
7. Insider Threat Certificate Programs
8. Insider Threat Program Manager Certificate
9. Insider Threat Vulnerability Assessor Certificate
10. Insider Threat Program Evaluator Certificate
11. Engage with Us
## Insider Threat Assessment Capabilities

<table>
<thead>
<tr>
<th>Information Technology</th>
<th>Software Engineering</th>
<th>Data Owners</th>
<th>Human Resources</th>
<th>Physical Security</th>
<th>Legal / Contracts</th>
<th>Business Partners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Technical Policies and Agreements</td>
<td>Access Control</td>
<td>Recruitment</td>
<td>Facility Security</td>
<td>Agreements to Protect Sensitive Information</td>
<td>Screening / Hiring of Applicants</td>
</tr>
<tr>
<td>Modification of Data or Disruption of Services or Systems</td>
<td>Modification of Data or Systems</td>
<td>Modification of Data, Systems, or Logs</td>
<td>Policies and Practices</td>
<td>Physical Asset Security</td>
<td>Restrictions on Outside Employment</td>
<td>Management of Business Partners</td>
</tr>
<tr>
<td>Unauthorized Access, Download, or Transfer of Assets</td>
<td>Asset Management</td>
<td>Unauthorized Access, Download, or Transfer of Assets</td>
<td>Training and Education, Evaluation</td>
<td></td>
<td>Employee Behaviors in the Workplace</td>
<td>Asset Management</td>
</tr>
<tr>
<td>Detection and Identification</td>
<td></td>
<td>Incident Response</td>
<td>Policy and Practice Monitoring and Enforcement Programs</td>
<td></td>
<td></td>
<td>Incident Response</td>
</tr>
<tr>
<td>Incident Response</td>
<td></td>
<td>Termination</td>
<td>Enforcement and Termination</td>
<td></td>
<td></td>
<td>Contractor / Business Partner Agreements</td>
</tr>
<tr>
<td>Termination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 50 | 5 | 13 | 30 | 7 | 12 | 9 |
Point of Contact

Michael C. Theis
CISSP, Special Agent in Charge (retired)
Technical Lead of Insider Threat Research
and Senior Member of the Technical Staff

CERT Insider Threat Center
Software Engineering Institute (an FFRDC)
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890

+1 703-489-5538 – Phone
mctheis@cert.org – Email

http://www.cert.org/insider_threat/