Insider Threats:

*Actual Attacks by Current and Former Software Engineers*

9 June 2011

Dawn Cappelli
Agenda

Introduction to the CERT Insider Threat Center

CERT’s Insider Threat Crime Profiles

Mitigation Strategies

Discussion
Who is a Malicious Insider?

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.
CERT Insider Threat Center Objective

Opportunities for prevention, detection, and response for an insider attack
CERT’s Unique Approach to the Problem

Database

Research  Lab  Assessments
Workshops
Exercises
CERT’s Insider Threat Case Database

U.S. Crimes by Category

- Sabotage: 123
- Fraud: 196
- Theft of IP: 86
- Misc: 43
IT Sabotage
TRUE STORY:

A company’s mobile devices were suddenly disabled for almost 1000 employees, grinding sales and delivery operations to a halt for several days …

*Logic bomb went off three months to the day after a demoted system architect’s retaliatory resignation.*
MERIT Model of Insider IT Sabotage

- **Actual risk of insider attack**
  - **Technical precursor**
    - **Unknown access paths**
    - **Technical monitoring**
      - **Insider's unmet expectation**
        - **Technical monitoring**
          - **Org's trust of insider**
            - **Precipitating event**
              - **Personal predisposition**
                - **Expectation fulfillment**
                  - **Insider's expectation**
                    - **Insider's unmet expectation**
                      - **Behavioral monitoring**
                        - **Discovery of precursors**
                          - **Sanctions**
                            - **Behavioral precursor**
                              - **Disgruntlement**
Theft of Intellectual Property

WELCOME ABOARD SMITH. I'M SURE THE "KNOWLEDGE AND EXPERIENCE" YOU BRING WITH YOU WILL BE EXTREMELY VALUABLE.
TRUE STORY:

A company sues a former programmer found selling a competing product at a tradeshow….

Investigators found copies of the company’s source code on his home computer that was stolen on his last day of work at the company.
MERIT Model of Insider Theft of IP – Entitled Independent

- Insider contribution
- Insider entitlement
- Insider dissatisfaction
- Insider desire to steal
- Information stolen
- Opportunity to detect theft
- Organization discovery of theft
- Precipitating event (e.g., proposal by competitor)
- Insider planning to go to competitor
- Level of technical and behavioral monitoring
- Insider desire to steal

Denial of insider request

MERIT Model of Insider Theft of IP – Entitled Independent
MERIT Model of Insider Theft of IP – Ambitious Leader

- Insider contribution
- Insider entitlement
- Recruitment of other insiders
- Information stolen
- Increasing access to information
- Insider desire to steal
- Extent of planning to steal
- Opportunity to detect theft
- Org discovery of theft
- Level of technical and behavioral monitoring
- Precipitating event (e.g., proposal by competitor)
- Insider planning to go to competitor
Fraud
TRUE STORY:

A financial organization’s routine audit discovers a $90,000 discrepancy in one of their software engineer’s personal loan accounts…

The employee modified critical source code to siphon off money to cover fraudulent personal loans he had created.
# Summary of Findings - Fraud

<table>
<thead>
<tr>
<th>Current or former employee?</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of position</td>
<td>Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)</td>
</tr>
<tr>
<td>Gender</td>
<td>Fairly equally split between male and female</td>
</tr>
<tr>
<td>Target</td>
<td>PII or Customer Information</td>
</tr>
<tr>
<td>Access used</td>
<td>Authorized</td>
</tr>
<tr>
<td>When</td>
<td>During normal working hours</td>
</tr>
<tr>
<td>Where</td>
<td>At work</td>
</tr>
<tr>
<td>Recruited by outsiders</td>
<td>½ recruited for theft; less than 1/3 recruited for mod</td>
</tr>
</tbody>
</table>
| Collusion                     | Mod: almost ½ colluded with another insider  
|                               | Theft: 2/3 colluded with outsiders |
Common Sense Guide to Prevention and Detection of Insider Threats

## Summary of Best Practices in CSG

<table>
<thead>
<tr>
<th>Consider threats from insiders and business partners in enterprise-wide risk assessments.</th>
<th>Consider insider threats in the software development life cycle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearly document and consistently enforce policies and controls.</td>
<td>Use extra caution with system administrators and technical or privileged users.</td>
</tr>
<tr>
<td>Institute periodic security awareness training for all employees.</td>
<td>Implement system change controls.</td>
</tr>
<tr>
<td>Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.</td>
<td>Log, monitor, and audit employee online actions.</td>
</tr>
<tr>
<td>Anticipate and manage negative workplace issues.</td>
<td>Use layered defense against remote attacks.</td>
</tr>
<tr>
<td>Track and secure the physical environment.</td>
<td>Deactivate computer access following termination.</td>
</tr>
<tr>
<td>Implement strict password and account management policies and practices.</td>
<td>Implement secure backup and recovery processes.</td>
</tr>
<tr>
<td>Enforce separation of duties and least privilege.</td>
<td>Develop an insider incident response plan.</td>
</tr>
</tbody>
</table>
Discussion
Points of Contact

Insider Threat Center
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890

Dawn Cappelli
Technical Manager
+1 412 268-9136
dmc@cert.org

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