The Insider Threat: Lessons Learned from Actual Insider Attacks

Randall Trzeciak
Insider Threat Center at CERT

Trzeciak is currently a senior member of the technical staff at CERT. He is the technical team lead of the Insider Threat Research team; a team focusing on insider threat research; threat analysis and modeling; assessments; and training. Trzeciak has more than 20 years experience in software engineering; database design, development, and maintenance; project management; and information security.
The Insider Threat: Lessons Learned from Actual Insider Attacks

Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213

Approved for public release; distribution unlimited
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.
## Types of Insider Crimes

<table>
<thead>
<tr>
<th><strong>Insider IT sabotage</strong></th>
<th>An insider’s use of IT to direct specific harm at an organization or an individual.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Insider theft of intellectual property (IP)</strong></td>
<td>An insider’s use of IT to steal intellectual property from the organization. This category includes industrial espionage involving insiders.</td>
</tr>
<tr>
<td><strong>Insider fraud</strong></td>
<td>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 (identity theft, credit card fraud).</td>
</tr>
</tbody>
</table>
CERT’s Insider Threat Case Database

U.S. Crimes by Category

- Sabotage: 134
- Fraud: 248
- Theft of IP: 84
- Misc: 54
- Espionage: 120

CERT’s Insider Threat Case Database
Critical Infrastructure Sectors

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

- IT and Telecomm
- Banking and Finance
- Government
- Public Health
- Commercial Facilities
- Education
- All other sectors

Types of Crime:
- Theft IP
- Sabotage
- Fraud
CERT’s Unique Approach to the Problem

- Research
- Lab
- Assessments Workshops Exercises

- Models
- Database
CERT’s Unique Approach to the Problem

- Research
- Lab
- Assessments
- Workshops
- Exercises
- Models
- Database
CERT Insider Threat Center Objective

**Opportunities for prevention, detection, and response for an insider attack**
Insider Crime Profiles
IT Sabotage
TRUE STORY:

SCADA systems for an oil-exploration company is temporarily disabled...

A contractor, who’s request for permanent employment was rejected, planted malicious code following termination
Insider IT Sabotage

Who did it?
- Former employees
- Male
- Highly technical positions
- Age: 17 – 60

How did they attack?
- No authorized access
- Backdoor accounts, shared accounts, other employees’ accounts, insider’s own account
- Many technically sophisticated
- Remote access outside normal working hours
### Summary of Findings

<table>
<thead>
<tr>
<th></th>
<th>IT Sabotage</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of crimes in case database**</td>
<td>35%</td>
</tr>
<tr>
<td>Current or former employee?</td>
<td>Former</td>
</tr>
<tr>
<td>Type of position</td>
<td>Technical (e.g. sys admins or DBAs)</td>
</tr>
<tr>
<td>Gender</td>
<td>Male</td>
</tr>
</tbody>
</table>

**Does not include national security espionage**
## Summary of Findings

<table>
<thead>
<tr>
<th></th>
<th>IT Sabotage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target</strong></td>
<td>Network, systems, or data</td>
</tr>
<tr>
<td><strong>Access used</strong></td>
<td>Unauthorized</td>
</tr>
<tr>
<td><strong>When</strong></td>
<td>Outside normal working hours</td>
</tr>
<tr>
<td><strong>Where</strong></td>
<td>Remote access</td>
</tr>
<tr>
<td><strong>Recruited by outsiders</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Collusion</strong></td>
<td>None</td>
</tr>
</tbody>
</table>
Fraud
TRUE STORY:

An undercover agent who claims to be on the “No Fly list” buys a fake drivers license from a ring of DMV employees...

The 7 person identity theft ring consisted of 7 employees who sold more than 200 fake licenses for more than $1 Million.
Fraud: Theft or Modification

Who did it?
- Current employees
- “Low level” positions
- Gender: fairly equal split
- Average age: 33

What was stolen/modified?
- Personally Identifiable Information (PII)
- Customer Information (CI)
- Very few cases involved trade secrets

How did they steal/modify it?
- During normal working hours
- Using authorized access
## Summary of Findings

<table>
<thead>
<tr>
<th></th>
<th>IT Sabotage</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>% of crimes in case database</strong></td>
<td>35%</td>
<td>40%</td>
</tr>
<tr>
<td><strong>Current or former employee?</strong></td>
<td>Former</td>
<td>Current</td>
</tr>
<tr>
<td><strong>Type of position</strong></td>
<td>Technical (e.g. sys admins or DBAs)</td>
<td>Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td>Male</td>
<td>Fairly equally split between male and female</td>
</tr>
</tbody>
</table>

**Does not include national security espionage**
## Summary of Findings

<table>
<thead>
<tr>
<th></th>
<th>IT Sabotage</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target</strong></td>
<td>Network, systems, or data</td>
<td>PII or Customer Information</td>
</tr>
<tr>
<td><strong>Access used</strong></td>
<td>Unauthorized</td>
<td>Authorized</td>
</tr>
<tr>
<td><strong>When</strong></td>
<td>Outside 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>
</tr>
<tr>
<td><strong>Recruited by outsiders</strong></td>
<td>None</td>
<td>½ recruited for theft; less than 1/3 recruited for mod</td>
</tr>
<tr>
<td><strong>Collusion</strong></td>
<td>None</td>
<td>Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders</td>
</tr>
</tbody>
</table>
Theft of Intellectual Property

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

Research scientist downloads 38,000 documents containing his company’s trade secrets before going to work for a competitor…

*Information was valued at $400 Million*
Theft of Intellectual Property

Who did it?
- Current employees
- Technical or sales positions
- All male
- Average age: 37

What was stolen?
- Intellectual Property (IP)
- Customer Information (CI)

How did they steal it?
- During normal working hours
- Using authorized access
Dynamics of the Crime

Most were *quick* theft upon resignation

Stole information to
- Take to a new job
- Start a new business
- Give to a foreign company or government organization

Collusion
- Collusion with at least one *insider* in almost 1/2 of cases
- Outsider *recruited* insider in less than 1/4 of cases
- Acted *alone* in 1/2 of cases
## Summary of Findings

<table>
<thead>
<tr>
<th></th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of crimes in case database**</td>
<td>35%</td>
<td>40%</td>
<td>18%</td>
</tr>
<tr>
<td>Current or former employee?</td>
<td>Former</td>
<td>Current</td>
<td>Current</td>
</tr>
<tr>
<td><strong>Type of position</strong></td>
<td>Technical (e.g. sys admins or DBAs)</td>
<td>Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)</td>
<td>Technical (71%) - scientists, programmers, engineers</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td>Male</td>
<td>Fairly equally split between male and female</td>
<td>Male</td>
</tr>
</tbody>
</table>

**Does not include national security espionage**
### Summary of Findings

<table>
<thead>
<tr>
<th>Target</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network, systems, or data</strong></td>
<td>PII or Customer Information</td>
<td>IP (trade secrets) – 71%</td>
<td>Customer Info – 33%</td>
</tr>
<tr>
<td><strong>PII or Customer Information</strong></td>
<td>Authorized</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
<tr>
<td><strong>Unauthorized</strong></td>
<td>Authorized</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
<tr>
<td><strong>Outside normal working hours</strong></td>
<td>Authorized</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
<tr>
<td><strong>Remote access</strong></td>
<td>Authorized</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
<tr>
<td><strong>Remote access</strong></td>
<td>Authorized</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
<tr>
<td><strong>Recruited by outsiders</strong></td>
<td>None</td>
<td>½ recruited for theft; less than 1/3 recruited for mod</td>
<td>Less than 1/4</td>
</tr>
<tr>
<td><strong>Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders</strong></td>
<td>Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders</td>
<td>Almost ½ colluded with at least one insider; ½ acted alone</td>
<td></td>
</tr>
</tbody>
</table>
Mitigation Strategies
Our Suggestion

Continuous Logging

Targeted Monitoring

Real-time Alerting

Insider Threat
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>
Point of Contact

Insider Threat Technical Team Lead
Randall F. Trzeciak
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-7040 – Phone
rft@cert.org – Email

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

© 2011 Carnegie Mellon University

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.
We offer a diverse range of learning products—including classroom training, eLearning, certification, and more—to serve the needs of customers and partners worldwide.