Network Security, Incident Management, and Insider Threats in the Healthcare Industry

CERT Insider Threat Center

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Randy Trzeciak
May 11, 2011

http://www.cert.org/insider_threat/
Insider Threat Agenda

Introduction

How bad is the insider threat?

Exploration of each type of insider crime:

- IT sabotage
- Theft of Intellectual Property
- Fraud

Mitigation Strategies
Introduction
What is CERT?

Center of Internet security expertise

Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today

Located in the Software Engineering Institute (SEI)

- Federally Funded Research & Development Center (FFRDC)
- Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)
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: 123
- Fraud: 196
- Theft of IP: 86
- Misc: 43
- Espionage: 120
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

Legend:
- Theft IP
- Sabotage
- Fraud
CERT Insider Threat Center Objective

Opportunities for prevention, detection, and response for an insider attack
How bad is the insider threat?
Insider Threat Issue

Insiders pose a substantial threat by virtue of their knowledge of, and access to, their employers’ systems and/or databases.

Insiders can bypass existing physical and electronic security measures through *legitimate* measures.
38% of organizations have more than 5000 employees

37% of organizations have less than 500 employees

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

Most common insider e-crime

<table>
<thead>
<tr>
<th>Crime</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access to / use of corporate information</td>
<td>63%</td>
</tr>
<tr>
<td>Unintentional exposure of private or sensitive data</td>
<td>57%</td>
</tr>
<tr>
<td>Virus, worms, or other malicious code</td>
<td>37%</td>
</tr>
<tr>
<td>Theft of intellectual property</td>
<td>32%</td>
</tr>
</tbody>
</table>

How Insider Intrusions Are Handled

- Internally (without legal action or law enforcement) 76%
- Internally (with legal action) 8%
- Externally (notifying law enforcement) 3%
- Externally (filing a civil action)

Reason(s) CyberCrimes were not referred for legal action

<table>
<thead>
<tr>
<th>Reason</th>
<th>2011</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage level insufficient to warrant prosecution</td>
<td>42%</td>
<td>37%</td>
</tr>
<tr>
<td>Could not identify the individual/individuals responsible for committing the eCrime</td>
<td>40%</td>
<td>29%</td>
</tr>
<tr>
<td>Lack of evidence/not enough information to prosecute</td>
<td>39%</td>
<td>35%</td>
</tr>
<tr>
<td>Concerns about negative publicity</td>
<td>12%</td>
<td>15%</td>
</tr>
<tr>
<td>Concerns about liability</td>
<td>8%</td>
<td>7%</td>
</tr>
<tr>
<td>Concerns that competitors would use incident to their advantage</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>Prior negative response from law enforcement</td>
<td>5%</td>
<td>7%</td>
</tr>
<tr>
<td>Unaware that we could report these crimes</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>Other</td>
<td>11%</td>
<td>5%</td>
</tr>
<tr>
<td>Don't know</td>
<td>20%</td>
<td>14%</td>
</tr>
<tr>
<td>Not applicable</td>
<td>N/A</td>
<td>24%</td>
</tr>
</tbody>
</table>

Insider Crime Profiles
IT Sabotage
**IT Sabotage Incidents**

An IT consultant for a hospital medical supply facility seeks revenge when he loses control of his company

…*System administrator sabotages systems on his way out*

A security guard at a U.S. hospital, after submitting resignation notice, obtained physical access to computer rooms

…*Installed malicious code on hospital computers, accessed patient medical records*
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
MERIT Model of Insider IT Sabotage

- **Actual risk of insider attack**
  - Technical precursor
  - Acquiring unknown paths
  - Org's trust of insider

- **Behavioral precursor**
  - Disgruntlement
  - Insider's unmet expectation
  - Insider's expectation
  - Personal predisposition

- **Technical precursor**
  - Sanctions
  - Expectation fulfillment
  - Precipitating event

- **Actual risk of insider attack**
  - Discovery of precursors
  - Technical monitoring
  - Perceived risk of insider attack
  - Ability to conceal activity
  - Ability to acquire access paths
MERIT Model of Insider IT Sabotage

- **Behavioral Precursor**: disgruntlement
- **Insider's Unmet Expectation**: personal predisposition
- **Sanctions**: expectation fulfillment
- **Discovery of Precursors**: precipitating event
- **Technical Precursor**: ability to conceal activity
- **Perceived Risk of Insider Attack**: org's trust of insider
- **Actual Risk of Insider Attack**: technical monitoring
- **Unknown Access Paths**: acquiring unknown paths

The model illustrates the factors contributing to an insider attack, highlighting behavioral and technical precursors, along with personal predispositions and organizational trust.
## 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>
## 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>
Theft of Intellectual Property

WELCOME ABOARD SMITH. I'M SURE THE "KNOWLEDGE AND EXPERIENCE" YOU BRING WITH YOU WILL BE EXTREMELY VALUABLE.
Theft of Information Incidents

A technical operations associate at a pharmaceutical company downloads 65 GB of information, including 1300 confidential and proprietary documents, intending to start a competing company, in a foreign country...

Organization spent over $500M in development costs
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>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of crimes in case database</td>
<td>35%</td>
<td>18%</td>
</tr>
<tr>
<td>Current or former employee?</td>
<td>Former</td>
<td>Current</td>
</tr>
<tr>
<td>Type of position</td>
<td>Technical (e.g. sys admins or DBAs)</td>
<td>Technical (71%) - scientists, programmers, engineers</td>
</tr>
<tr>
<td>Gender</td>
<td>Male</td>
<td>Male</td>
</tr>
</tbody>
</table>

### Current or former employee?

<table>
<thead>
<tr>
<th></th>
<th>Former</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of crimes in case database</td>
<td>35%</td>
<td>18%</td>
</tr>
<tr>
<td>Current or former employee?</td>
<td>Former</td>
<td>Current</td>
</tr>
<tr>
<td>Type of position</td>
<td>Technical (e.g. sys admins or DBAs)</td>
<td>Technical (71%) - scientists, programmers, engineers</td>
</tr>
<tr>
<td>Gender</td>
<td>Male</td>
<td>Male</td>
</tr>
</tbody>
</table>
## Summary of Findings

<table>
<thead>
<tr>
<th></th>
<th>IT Sabotage</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target</strong></td>
<td>Network, systems, or data</td>
<td>IP (trade secrets) – 71%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Customer Info – 33%</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>Less than 1/4</td>
</tr>
<tr>
<td><strong>Collusion</strong></td>
<td>None</td>
<td>Almost ½ colluded with at least one insider; ½ acted alone</td>
</tr>
</tbody>
</table>
Fraud
**Fraud Incidents**

An accounts payable clerk, over a period of 3 years, issues 127 unauthorized checks to herself and others...

*Checks totaled over $875,000*

A front desk office coordinator stole PII from hospital...

*Over 1100 victims and over $2.8 M in fraudulent claims*
Fraud: Theft or Modification

Most attacks were long, ongoing schemes

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>Theft of Intellectual Property</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of crimes in case database**</td>
<td>35%</td>
<td>18%</td>
<td>40%</td>
</tr>
<tr>
<td>Current or former employee?</td>
<td>Former</td>
<td>Current</td>
<td>Current</td>
</tr>
<tr>
<td>Type of position</td>
<td>Technical (e.g. sys admins or DBAs)</td>
<td>Technical (71%) - scientists, programmers, engineers</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>Male</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>Theft of Intellectual Property</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target</strong></td>
<td>Network, systems, or data</td>
<td>IP (trade secrets) – 71%</td>
<td>PII or Customer Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Customer Info – 33%</td>
<td></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>
<tr>
<td><strong>Recruited by outsiders</strong></td>
<td>None</td>
<td>Less than 1/4</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>Almost ½ colluded with at least one insider; ½ acted alone</td>
<td>Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders</td>
</tr>
</tbody>
</table>
Mitigation Strategies
Our Suggestion

- Continuous Logging
- Targeted Monitoring
- Real-time Alerting

No 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>
Publicly Available Information

Reports

Podcasts

Insider Threat Study

System Dynamics

Cyber Crime Survey

(http://www.cert.org/insider_threat/)
Point of Contact

Insider Threat Center at CERT
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/