CERT

Preventing Insider Sabotage: Lessons Learned From Actual Attacks

Dawn Cappelli

November 14, 2005

© 2005 Carnegie Mellon University
1. REPORT DATE  
14 NOV 2005

2. REPORT TYPE

3. DATES COVERED  
00-00-2005 to 00-00-2005

4. TITLE AND SUBTITLE
Preventing Insider Sabotage: Lessons Learned From Actual Attacks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHOR(S)

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

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

<table>
<thead>
<tr>
<th>a. REPORT</th>
<th>b. ABSTRACT</th>
<th>c. THIS PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

17. LIMITATION OF ABSTRACT
Same as Report (SAR)

18. NUMBER OF PAGES
39

19a. NAME OF RESPONSIBLE PERSON

Standard Form 298 (Rev. 8-98)  
Prepared by ANSI Std Z39-18
Agenda

What is CERT?
Are Insiders a Threat?
CERT/U.S. Secret Service (USSS) Insider Threat Study
Best practices
  • Supporting Findings
  • Case Examples

What’s Next
Questions/Discussion
What is CERT?

Center of Internet security expertise

Established in 1988 by the Department of Defense (DARPA) in 1988 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)
The CERT/CC gains a broad view of Internet security threats with data from many sources. CERT/CC analysts synthesize the data and publish timely, accurate information fast. Researchers develop long-term strategies to improve system security and survivability.
Are Insiders a Threat?
e-Crime Watch

CSO, USSS & CERT/CC

819 respondents

Average number of e-crimes in 2004: 86

35% increase in e–crimes in 2004

68% at least one e-crime or intrusion

39% of the organizations experienced one or more insider attacks or intrusions

20% of all attacks by insiders (versus outsiders)
“We're all too paranoid, no point looking behind your back, we are already here.”

Posted by: Anonymous
“idiocy to say the least
having been a statistic myself
i see that fear and stupidy prevail
nothing is secure
trust no-one
ever”

Posted by: C0rpR4t3_H4C|<
USSS/CERT Insider Threat Study

Definition of insider

Purpose of the study

Study method

Reports
Study Definition of Insider

Current or former employees or contractors who

- intentionally exceeded or misused an authorized level of access to networks, systems or data in a manner that

- targeted a specific individual or affected the security of the organization’s data, systems and/or daily business operations
Study Purpose

Identify information that was known or potentially detectable prior to the incident.

Analyze physical, social and online behaviors of insiders.

Develop information to help private industry, government and law enforcement better understand, detect and prevent harmful insider activity.
Study Method

Incidents perpetrated by insiders in critical infrastructure sectors.

Initial incidents occurred between 1996 and 2002.

Reported publicly or investigated by the Secret Service.

Reviewed primary source material (investigative reports, court documents) and conducted supplemental interviews.
USSS/CERT Insider Threat Study

Definition of insider

Purpose of the study

Study method

Reports

![Bar chart showing cases in Banking & Finance and Cross Sector with categories of Sabotage, Fraud, and Information Theft.]
Insider Sabotage

Who were they?

Why did they do it?

What were the consequences?

Best practices

- Supporting Findings
- Case Examples
Who Were the Insiders?

- Male
- 17-60 years old
- About half married
- Variety of racial & ethnic backgrounds

![Pie chart showing 57% disgruntled and 43% not disgruntled.]
Primary Motive

- Financial: 84%
- Revenge: 92%
- Response to negative event: 92%

Percentage of Sabotage Cases
Consequences to Targeted Organizations

Financial Loss

Harm to Individuals

Experienced financial loss

No financial loss

19%

81%
Consequences to Targeted Organizations

Financial Loss

Harm to Individuals

- 65% No individual harm
- 35% Harmed an individual
Best Practices
Background checks

Conduct background checks & consider results carefully.

- No previous arrest(s): 70%
- Previous arrest(s): 30%
Security Awareness Training

Institute periodic employee security awareness training for all employees.

![Bar chart showing sabotage cases: Planned in advance at 62% and Others knew at 31%.]
Separation of Duties

Enforce separation of duties and least privilege.

![Pie chart showing 29% detected by security staff and 71% detected by non-security personnel.](chart_image)
Password & Account Management

Implement strict password and account management policies and practices.

- Had authorized access: 43%
- Did not have authorized access: 57%
Monitoring

Log, monitor, and audit employee online actions.
System Administrators

Use additional controls for system administrators and privileged users.

- Technical position: 86%
- Non-technical position: 14%
Malicious Code

Actively defend against malicious code.

![Pie chart showing 61% not technically sophisticated and 39% technically sophisticated]
Remote Access

*Use layered defense against remote attacks.*

![Pie chart showing 36% remote access not used and 64% used remote access]
Suspicious Behavior

Monitor and respond to suspicious or disruptive behavior.

No concerning behavior: 20%
Concerning behavior: 80%
Access Following Termination

Deactivate access following termination.

Current employees: 41%
Former employees: 59%
Investigation

Collect and save data for use in investigations.

- System logs not used for investigation: 30%
- System logs used for investigation: 70%
Back Up & Recovery

*Implement secure backup and recovery processes.*

![Pie chart showing 25% no impact on business operations and 75% impacted business operations.](chart.png)
Formal Documentation

Clearly document insider threat controls.

“Most ITs I know, even the entry-level guys, install root kits as a first order of business when they join a company. They do it as a reflex, not because they have malicious intent or plan to hack the company, but to give themselves convenient access so they can work from home or school.”

Posted by: Ben |
## Summary of Best Practices

<table>
<thead>
<tr>
<th>Conduct background checks &amp; consider results carefully.</th>
<th>Actively defend against malicious code.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institute periodic employee security awareness training for all employees.</td>
<td>Use layered defense against remote attacks.</td>
</tr>
<tr>
<td>Enforce separation of duties and least privilege.</td>
<td>Monitor and respond to suspicious or disruptive behavior.</td>
</tr>
<tr>
<td>Implement strict password and account management policies and practices.</td>
<td>Deactivate access following termination.</td>
</tr>
<tr>
<td>Log, monitor, and audit employee online actions.</td>
<td>Collect and save data for use in investigations.</td>
</tr>
<tr>
<td>Use additional controls for system administrators and privileged users.</td>
<td>Implement secure backup and recovery processes.</td>
</tr>
<tr>
<td></td>
<td>Clearly document insider threat controls.</td>
</tr>
</tbody>
</table>
What’s Next

In progress:

- Additional “sector reports”
  - IT sector
  - Government sector
- Training – U.S. Secret Service Electronic Crimes Task Force meetings
- System Dynamics Modeling

Planned:

- Insider Threat Phase 2
System Dynamics Modeling

Model interaction over time between

• organizational culture
• organization’s mission
• policies & procedures
• technology
• behavioral psychology
Management Education on Risk of Insider Threat

Management Simulator for insider threat problem

Decision support system for management

Evaluate relative insider threat risk
Insider Threat Phase 2

Collaborate with government and industry partners

Diagram:

- Insider
- Steal money
- Steal trade secrets
- Sabotage systems
“I worked at a medium-sized software company, and had root access to their main servers. Purely as an intellectual exercise, I thought about how I could most maliciously use that access. This is what I came up with:

Step 1: Hack the backup system: all backups are secretly encrypted as they are made, and decrypted when read back (so that checks of the backups shows nothing.)

Step 2: Wait a year or more.

Step 3: Wipe all the disks on the servers - including the hacked backup encryption/decryption software.

Step 4: Send extortion demand for the encryption key to the backups. Unless they pay, they've lost years of work.

Of course, I didn't actually try it, so I don't know if it would work...”

Posted by: Filias Cupio
Questions/Discussion