Agenda

Introduction

How bad is the insider threat?

Background on CERT’s insider threat research

Exploration of each type of insider crime:
  • Theft/Modification of information for financial gain
  • Theft of information for business advantage
  • IT sabotage

Best Practice for Prevention and Detection

Discussion
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)

CERT’s Definition of Malicious Insider

Current or former employee, contractor, or 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.

Note: This presentation does not address national security espionage involving classified information.
Types of Insider Crimes

**Insider IT sabotage:** An insider’s use of IT to direct specific harm at an organization or an individual.

**Insider theft of information:** An insider’s use of IT to steal confidential or sensitive information from the organization.

**Insider modification of information:** 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.

Publicly Available Information

**Reports**
- Protecting Against Insider Threat
- Common Sense Guide to Prevention and Detection of Insider Threats, Version 2.1
- Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis

**Podcasts**
- Insider Threat and the Software Development Lifecycle
- Protecting Against Insider Threat
- CERT Execs on the 2006 E-Crime Watch Survey

**Insider Threat Study**
- Insider Threat Study: Blot Cyber Activity in the Information Technology and Telecommunications Sector
- Insider Threat Study: Blot Cyber Activity in the Government Sector
- Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors
- Insider Threat Study: Blot Cyber Activity in the Banking and Finance Sector

**System Dynamics**
- An Experience Using System Dynamics to Facilitate an Insider Threat Workshop

**E-Crime Watch Survey**

Available at: [http://www.cert.org/insider_threat/](http://www.cert.org/insider_threat/)

Two Case Examples
TRUE STORY:
Personal information stolen for millions of customers of phone companies, credit card companies and banks ...

TRUE STORY:
Financial Institution customers lose all access to their money from Friday night through Monday...

Fired system administrator sabotages systems on his way out

The Expanding Complexity of “Insiders”

**Collusion with outsiders**
- Insiders recruited by or working for outsiders, including organized crime and foreign organizations or governments

**Business partners**
- Difficulty in controlling/monitoring access to your information and systems by ‘trusted’ business partners

**Mergers & acquisitions**
- Heightened risk of insider threat in organizations being merged into acquiring organization

**Cultural differences**
- Difficulty in recognizing behavioral indicators exhibited by insiders working for US companies who are not US citizens

**Foreign allegiances**
- US companies operating branches outside the US with the majority of employees who are not US citizens
How bad is the insider threat?

**e-Crime Watch Survey**
CSO Magazine, USSS, Microsoft, & CERT
671 respondents

Percentage of Participants Who Experienced an Insider Incident

<table>
<thead>
<tr>
<th>Year</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>41</td>
<td>39</td>
<td>55</td>
<td>49</td>
</tr>
</tbody>
</table>

**CERT's Insider Threat Research**
CERT’s Insider Threat Research

Insider Threat Cases

Database

Hundreds of cases have been analyzed
- US cases from 1996 to 2007 in critical infrastructure sectors
- US Secret Service
- Carnegie Mellon CyLab
- Department of Defense

Data includes both technical & behavioral information

CERT’s Insider Threat Research

Insider Threat Cases

Models

System dynamics models are built by technical experts & psychologists to analyze & simulate insider threats
- Insider IT sabotage
- Insider theft of confidential information (in development)
- Insider fraud (in development)

Case Breakdown

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft or Modification for Financial Gain</td>
<td>76</td>
</tr>
<tr>
<td>Theft for Business Advantage</td>
<td>74</td>
</tr>
<tr>
<td>IT Sabotage</td>
<td>24</td>
</tr>
<tr>
<td>Misc</td>
<td>17</td>
</tr>
</tbody>
</table>
Brief Overview of Findings From Our Research

Scenario 1:

Theft or Modification of Information for Financial Gain

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
Dynamics of the Crime

Most attacks were long, ongoing schemes

<table>
<thead>
<tr>
<th></th>
<th>At least 1 Insider Colluder</th>
<th>At least 1 Outside Colluder</th>
<th>Outsider Induced</th>
<th>Acted Alone</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Theft</strong></td>
<td>almost 1/3</td>
<td>2/3</td>
<td>1/2</td>
<td>&gt; 1/3</td>
</tr>
</tbody>
</table>

Known Issues

- Family medical problems
- Substance abuse
- Physical threat of outsiders
- Financial difficulties
- Financial compensation issues
- Hostile work environment
- Problems with supervisor
- Layoffs

Technical Aspects - Theft for Financial Gain

Electronically
- Downloaded to home
- Looked up and used immediately
- Copied
- Phone/fax
- Email
- Malicious code

Physically
- Printouts
- Handwritten

Remaining unknown
Scenario 2:

Theft of Information for Business Advantage

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
Known Issues

- Disagreement over ownership of intellectual property
- Financial compensation issues
- Relocation issues
- Hostile work environment
- Mergers & acquisitions
- Company attempting to obtain venture capital
- Problems with supervisor
- Passed over for promotion
- Layoffs

Technical Aspects – Theft for Business Advantage

In order of prevalence:

- Copied/downloaded information
- Emailed information
- Accessed former employer’s system
- Compromised account

Many other methods

Scenario 3:

IT Sabotage with the Intent to Harm Organization or Individual
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 – The Problem

behavioral precursor

disgruntlement

actual risk of insider attack

technical precursor

insider’s unmet expectation

precipitating event

discovery of precursors

behavioral monitoring

perceived risk of insider attack

technical monitoring

org’s trust of insider

insider’s expectation fulfillment

sanctions

ability to conceal activity

unknown access paths

acquiring unknown paths
Scenario 4:

Miscellaneous:

Cases not in the above scenarios

Examples of Miscellaneous Cases
Reading executive emails for entertainment
Providing organizational information to lawyers in lawsuit against organization
 Transmitting organization’s IP to hacker groups
 Unauthorized access to information to locate a person as accessory to murder

Best Practices
Summary of Best Practices

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

CERT Insider Threat Services

- Insider Threat Cases
  - Database
  - Models
  - Reports
  - Presentations
  - Services
  - Training/workshops
  - Customized research
  - Risk management support
  - Controls review
  - Threat analysis/modeling
  - Precautionary planning
  - MERIT Assessment

© 2006 Carnegie Mellon University
Thank you!