Carnegie Mellon
Software Engineering Institute

Insider Threat:
Real Data on a Real Problem

November 9, 2004

Dawn Cappelli
Carnegie Mellon University

Michelle Keeney, J.D., Ph.D.
United States Secret Service

Agenda

- Background – e-Crime Watch survey
- USSS/CERT Insider Threat Study
- Report#1: *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*
  - Sample case studies
  - Findings
- Next steps

Background

- E-Crime Watch – CSO, USSS & CERT/CC
- 500 respondents
- 43% increase in e–crimes in 2003
- 70% at least one e-crime or intrusion
- 29% insiders

USSS/CERT Insider Threat Study

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.

Major Areas of Inquiry

- Incident components
- Incident detection and identification of the insider
- Incident planning and communication
- Nature of harm
- Response of organization and law enforcement
- Insider and organization characteristics
- Insider background and history
- Insider technical expertise and interests

Insider Threat Study:

Illicit Cyber Activity in the Banking and Finance Sector

Banking and Finance Sector

- Analyzed 23 incidents perpetrated by 26 insiders

- Category of major harm to organization:
  - 15 involved the perpetration of fraud
  - 4 involved the theft of intellectual property
  - 4 involved sabotage to the information system/network

Sample Case Studies

Case #1: Investment Banker

- Fraudulent activity for 5 years
- Star producer
- Started losing money – bonuses & job at risk
- Either did not enter losses or entered fake trades
- Lost the bank approximately $691 million

Behavioral Issues

- Circumvented control measures
- Intimidation
- Management awareness/”feel good” culture
- “Suspensions”
- *“It’s only money and it’s not even ours.”*

Technical Issues

- Separation of duties
- *“There are problems when the smart people are smarter than the people auditing them.”*
- Legacy systems/no automated checks
- Easier to commit the fraud from home

The Result

- Approximately $691 million in losses
- 7 ½ years in Federal prison

Case#2: System Administrator

- New college graduate
- Hired as system administrator for credit union
- Fired after approximately two months for non-performance
- After termination, went home and shut down the credit union’s system

Behavioral Issues

- CEO stated he hired insider because he was the only one who came to the interview wearing a tie
- Spent most of his time complaining about the system and recommending that the company change the system, rather than try to learn it and work within the existing system
- Thought everyone else “was dumb” and they did not know what they were doing
- No documentation, no explanation of why terminated
- *“Do you walk up to a car & just try to unlock it? No – that’s disrespectful. Online it feels ok.”*

Technical Issues

- Firewall - remote access
- Personal account disabled but root password not changed
- Shutdown server (recent problems restarting that server)
- Used ISP account to “cover his tracks”
  - Modified IP address history
  - Modified credit union website
  - Removed CEO’s ISP account

The Result

- Credit union shut down for 3 days
- Probation & home confinement for 6 months
- *“You can type my entire name in google & I’m the first [thing] that comes up.”*

Insider Threat Study:

Illicit Cyber Activity in the Banking and Finance Sector

Findings

Major Findings and Implications

1. Most incidents were not technically sophisticated or complex – that is, they typically involved exploitation of non-technical vulnerabilities such as business rules or organization policies (rather than vulnerabilities in an information system or network) by individuals who had little or no technical expertise.

Major Findings and Implications

2. The majority of incidents were thought out and planned in advance. In most cases, others had knowledge of the insider’s intentions, plans and/or activities. Those who knew were often directly involved in the planning or stood to benefit from the activity.

Major Findings and Implications

3. Most insiders were motivated by financial gain, rather than a desire to harm the company or information system.

Major Findings and Implications

4. A wide variety of individuals perpetrated insider incidents in the cases studied. Most of the insiders in the banking and finance sector did not hold a technical position within their organization, did not have a history of engaging in technical attacks or “hacking,” and were not necessarily perceived as problem employees.

Major Findings and Implications

5. Insider incidents were detected by a range of people (both internal to the organization and external), not just by security staff. Both manual and automated procedures played a role in detection.

Major Findings and Implications

6. The impact of nearly all insider incidents in the banking and finance sector was financial loss for the victim organization. Many victim organizations incurred harm to multiple aspects of the organization.

Major Findings and Implications

7. Most of the incidents were executed at the workplace and during normal business hours.

Next Steps

- IT Sector report
- Cross sector report - focus on cases with intent to harm:
  - System
  - Data
  - Organization
  - Individual
- Outreach/training

Contact Information

National Threat Assessment Center
U.S. Secret Service
Email: ntac@secretservice.gov
Website: www.secretservice.gov

CERT® Coordination Center
Carnegie Mellon University
Email: insider-threat-feedback@cert.org
Website: www.cert.org