RSA CONFERENCE 2009

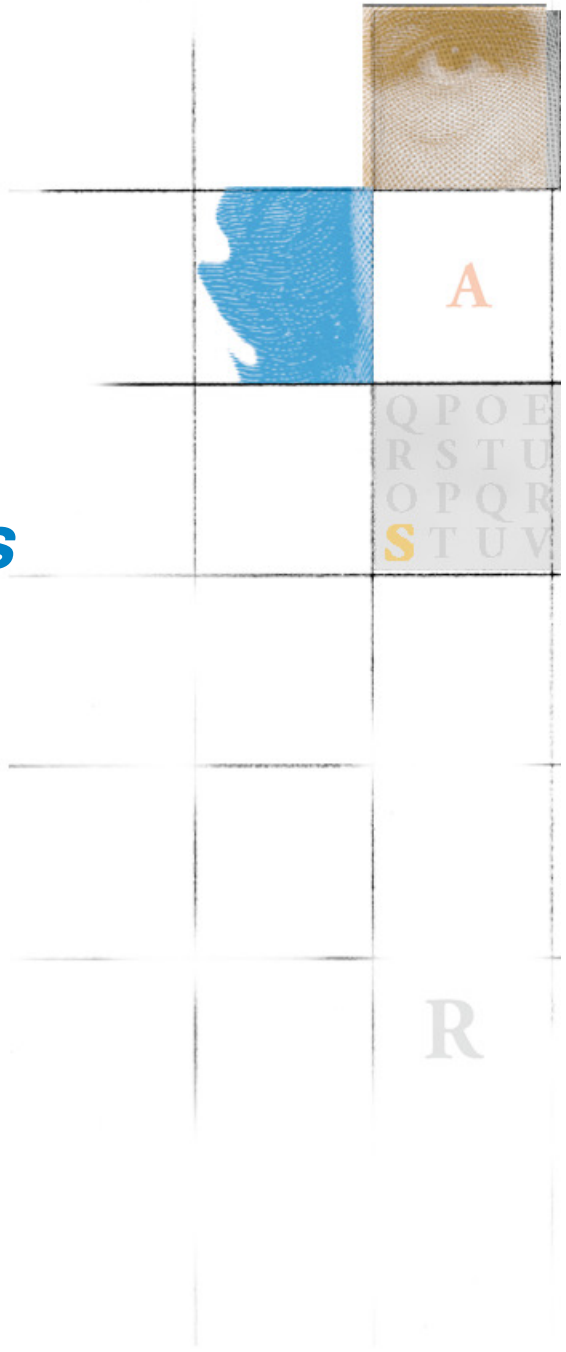
Best Practices For Mitigating Insider Threat:
Lessons Learned From 250 Cases

Dawn M. Cappelli
Randall F. Trzeciak

Carnegie Mellon University Software Engineering Institute CERT Program

04/23/09 | Session ID: RR-302

Session Classification: Advanced



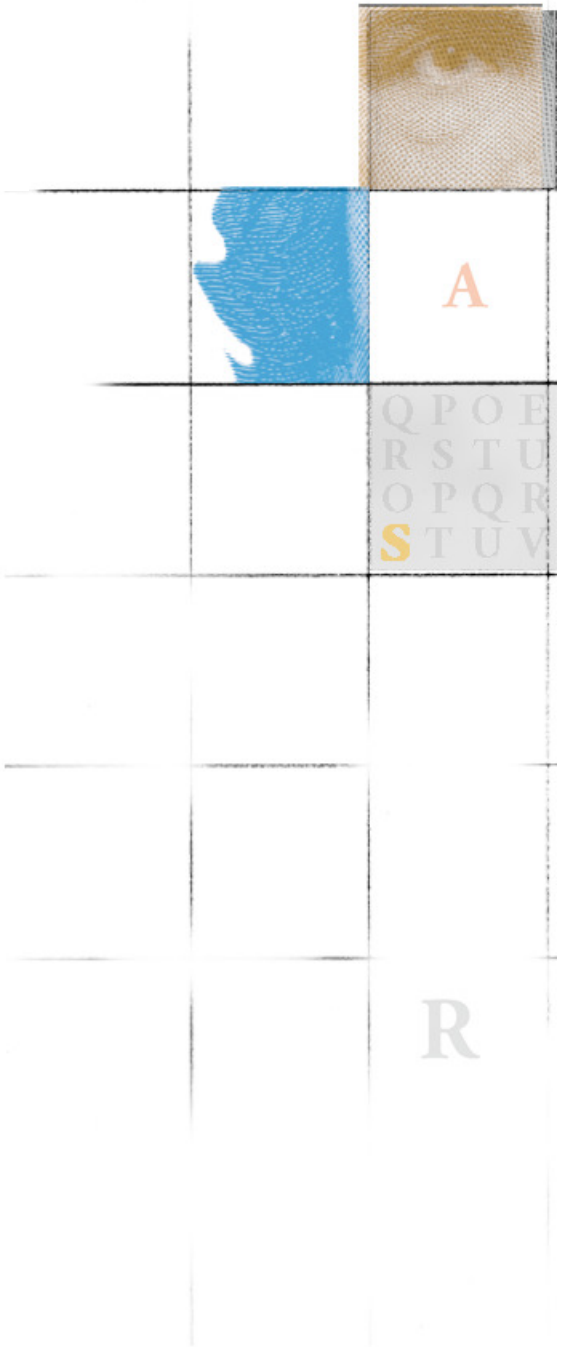
NO WARRANTY

This work 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 Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

Agenda

- Introduction
- Background on CERT's insider threat research
- Best practices for insider threat risk mitigation
- Summary

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)

What to Expect

- Best practices from the CERT *Common Sense Guide to Best Practices for the Prevention and Detection of Insider Threats V3.1*
- Interesting details for actual insider threat cases to reinforce each best practice
- Observations about the current insider threat landscape
- Leave here with justification for implementing these best practices
- It's your enterprise so you need to consider the ramifications of these recommendations

Our Thoughts About Best Practices

Our goal is to use interesting case examples to motivate you to ask yourself

Could something like this happen to me?

The devil is in the details….

CERT's Insider Threat Research

CERT's Definition of Malicious Insider

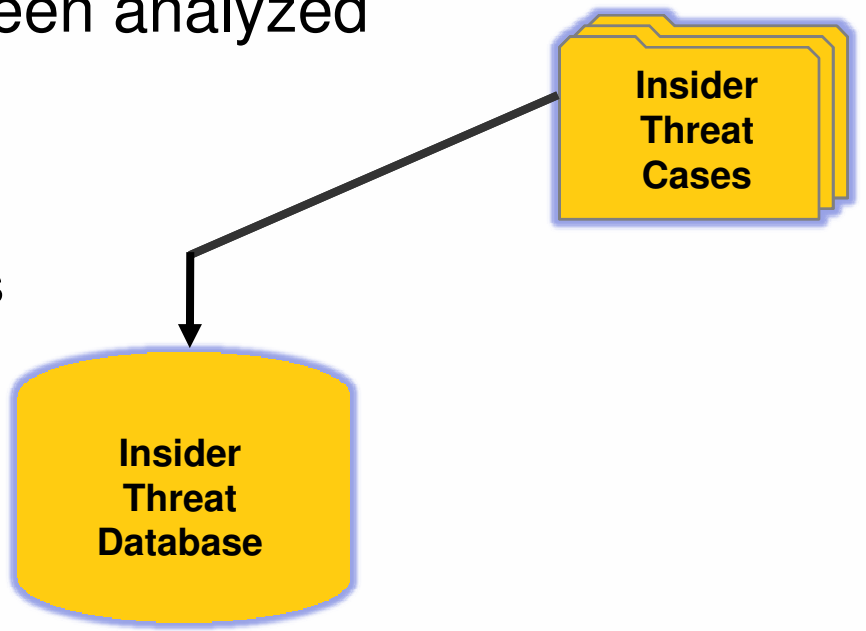
Current or former employee, contractor, or business partner who

- 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.

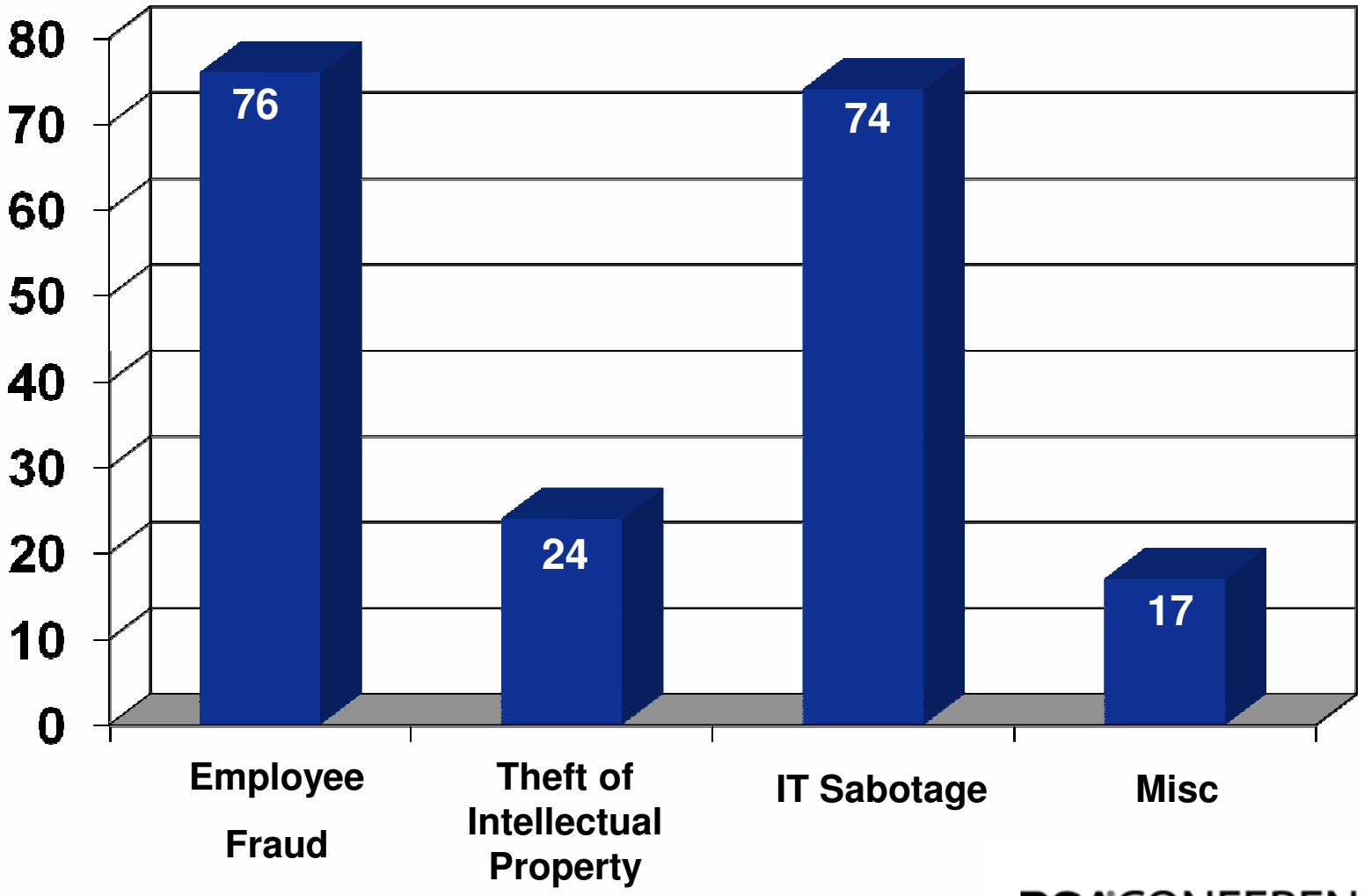
CERT's Insider Threat Research

- Hundreds of cases have been analyzed
  - US cases
  - 1996 to 2009
  - Critical infrastructure sectors
- Funded by:
  - US Secret Service
  - Carnegie Mellon CyLab
  - US Department of Defense
  - Department of Homeland Security
- Data includes both technical & behavioral information

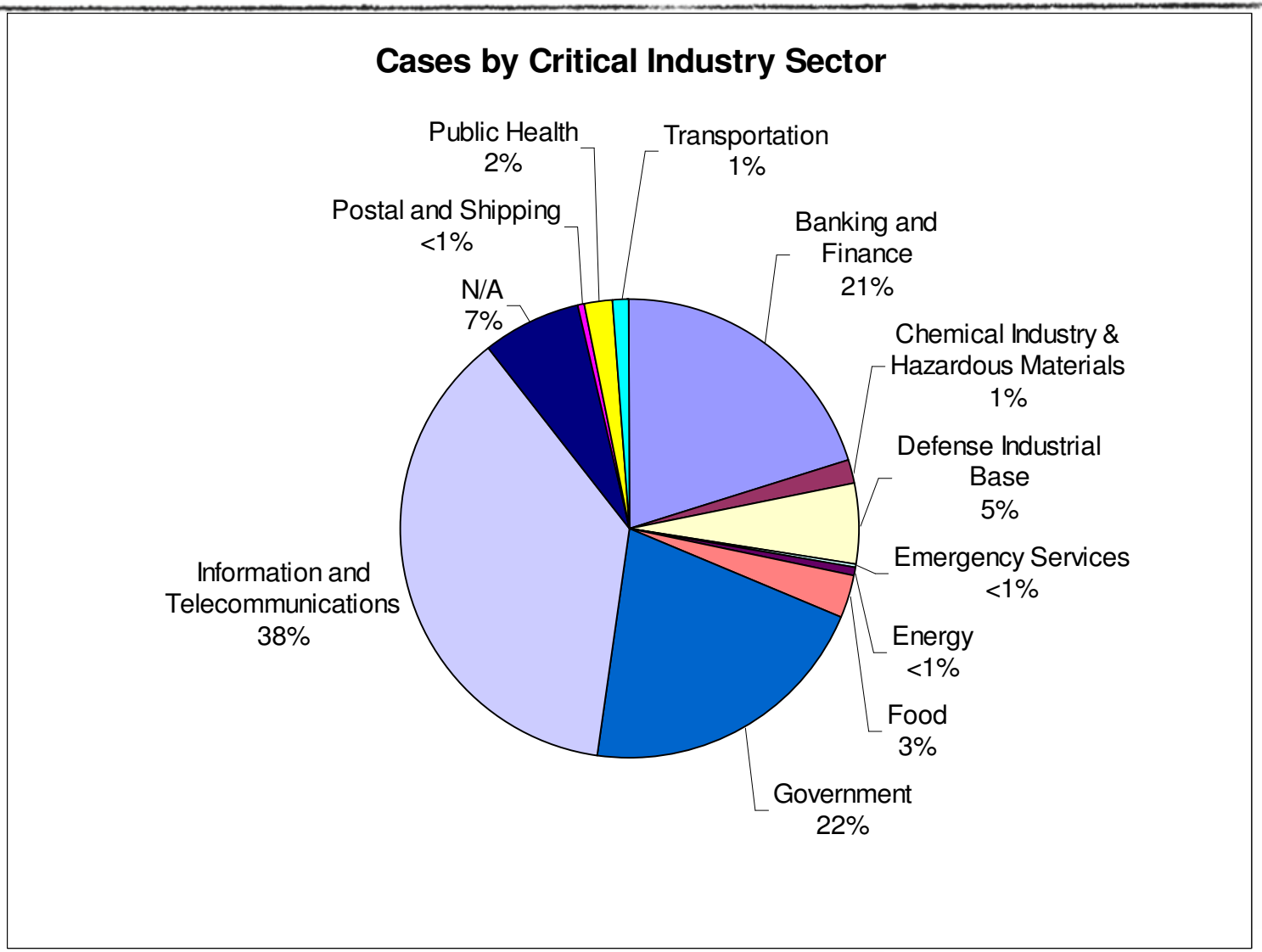


Insider Threat Cases

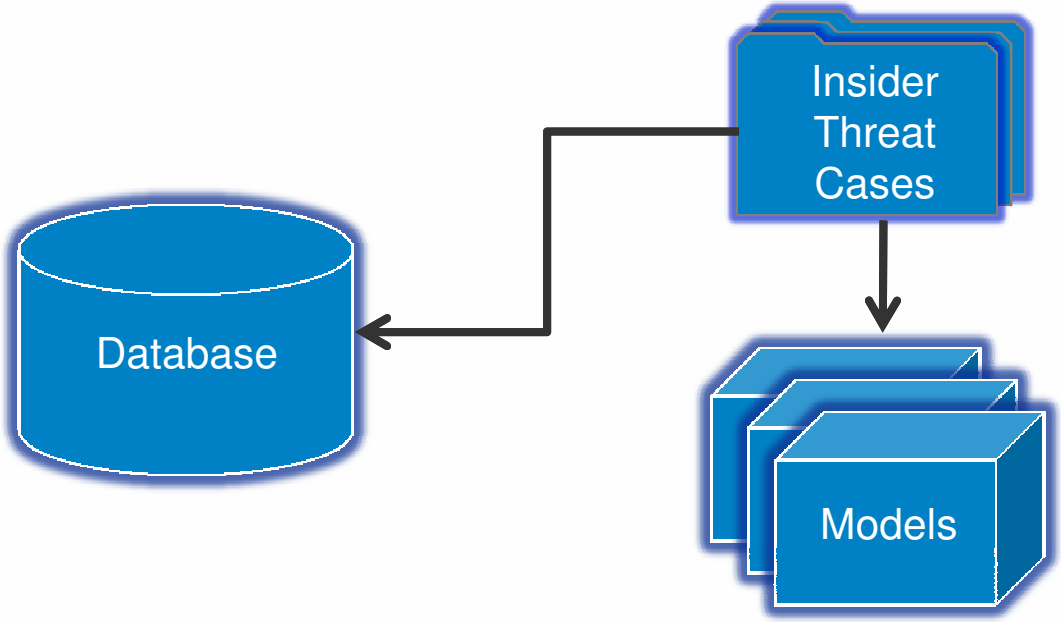
Cases for which CERT has gathered SUFFICIENT information



Critical Infrastructure Sectors



CERT's Insider Threat Research



System dynamics models are built by technical experts & psychologists to analyze & simulate insider threats

- Insider IT sabotage (completed)
- Insider theft of intellectual property (in development)
- Insider fraud

Best practices for insider threat risk mitigation

Best Practice #1

Consider threats from insiders and business partners in enterprise-wide risk assessments.

Phone companies, credit card companies and banks contract with an organization that hires another organization whose system administrator steals personal information for millions of their customers.

Organizations need to develop a risk-based security strategy to protect its critical assets from external threats, insiders, and trusted business partners.

Best Practice #2

Clearly document and consistently enforce policies and controls.

A former contractor remotely connects to the organization's servers, copies business plans and software, then sends email to the organization instructing them to stop using the software because he owns it.

A consistent, clear message on organizational policies and controls will help reduce the chance that employees will inadvertently commit a crime or lash out at the organization for a perceived injustice.

Best Practice #3 :

Institute periodic security awareness training.

A contract programmer enters the organization the night before his last day on the job, enters a co-worker's office, and steals critical source code…to take to his new job with a competitor.

Without broad understanding and buy-in from the organization, technical or managerial controls may be ineffective.

Best Practice #4:

Monitor and respond to suspicious or disruptive behavior.

A disgruntled system administrator amplifies the impact of a logic bomb by centralizing critical programs and intimidating a coworker out of backup tapes.

One method of reducing the threat of malicious insiders is to deal proactively with suspicious or disruptive employees.

Best Practice #5:

Anticipate and manage negative workplace issues.

A database administrator retaliates after a long period of serious conflict with her supervisor and coworkers by wiping out critical data, requiring 115 employees to spend 1800 hours to recover and re-enter the lost data.

Clearly defined and communicated organizational policies for dealing with employee issues will help ensure consistent enforcement and reduce risk when negative workplace issues arise.

Best Practice #6:

Track and secure the physical environment.

A subcontractor at an energy management facility breaks the glass enclosing the emergency power button, then shuts down computers that regulate the exchange of electricity between power grids, even though his own employer had disabled his access to their own facility following a dispute.

Although organizations are becoming more reliant on electronic communication and online transactions to do business, it is still essential that they track and secure the physical environment against internal and external threats.

Best Practice #7:

Implement strict password & account management practices.

A system administrator is terminated for poor job performance, then spends weeks afterward setting up his attack remotely using accounts he created before he left.

If an organization's computer accounts can be compromised, insiders can circumvent manual and automated control mechanisms.

Best Practice #8:

Enforce separation of duties and least privilege.

A disgruntled system administrator is able to deploy a logic bomb and modify the system logs to frame his supervisor even though he had been demoted and his privileges should have been restricted.

Separation of duties and least privilege must be implemented in business processes and for technical modifications to critical systems or information to limit the damage that malicious insiders can inflict.

Best Practice #9:

Consider insider threats in the software development life cycle.

A telecommunications company's services to its customers are suddenly disrupted; the investigation shows that a disgruntled programmer inserted malicious code into their inter-network communication protocol one year earlier, six months before leaving the company to take a new job.

Technical employees have taken advantage of defects introduced in the software development life cycle to deliberately perform malicious technical actions; likewise non-technical employees have recognized vulnerabilities and used them to carry out their fraudulent activities.

Best Practice #10:

Use extra caution with system administrators and technical or privileged users.

An organization refuses to pay a system administrator for his last two days of work when he suddenly quits without advanced notice; he then changes all administrator passwords and demands payment in exchange for the passwords.

System administrators and technical or privileged users have the technical ability, access, and oversight responsibility to commit and conceal malicious activity.

Best Practice #11:

Implement system change controls.

A programmer comments out a single line of code that notifies security whenever a seldom used screen is used to modify critical data, then uses that screen to commit criminal activity without detection for over a year and a half.

Changes to systems and applications must be controlled to prevent insertion of backdoors, keystroke loggers, logic bombs, and other malicious code or programs.

Best Practice #12:

Log, monitor, and audit employee online actions.

A research chemist takes a new job with a competitor but prior to leaving downloads over 38,000 files containing organization trade secrets.

Logging, monitoring, and auditing can lead to early discovery and investigation of suspicious insider actions.

Best Practice #13:

Use layered defense against remote attacks.

After resigning following a salary dispute, a CTO remotely accesses his former employer's systems and re-routes voice mail to a pornographic telephone service, floods email servers with thousands of messages with pornographic images, and sends threatening email to the CEO.

Remote access provides a tempting opportunity for insiders to attack with less risk.

Best Practice #14:

Deactivate computer access following termination.

A system administrator, fired for poor performance, uses a remote connection he had open at the time of termination to shut down and disable the company's manufacturing process on the night of his termination.

It is important that organizations follow rigorous termination procedures that disable all access paths into the organization's networks and systems for terminated employees.

Best Practice #15:

Implement secure backup and recovery processes.

Emergency services are forced to rely on manual address lookups for 911 calls when an insider sabotages the system and steals backup media from an off-site location.

It is important that organizations enhance organizational resiliency by implementing secure backup and recovery processes that are tested periodically, since despite all of the precautions, it is still possible that an insider will successfully attack.

Best Practice #16:

Develop an insider incident response plan.

A manager, suspended because he is suspected of fraudulent activity, uses social engineering to manipulate his employees to unwittingly destroy evidence of his crime.

Procedures for investigating and dealing with malicious insiders present unique challenges; response must be planned, clearly documented, and agreed to by organization managers and attorneys.

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.

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

Immediate Actions You Can Take

- Refer to Common Sense Guide to Prevention and Detection of Insider Threats
  - http://www.cert.org/insider_threat/
  - More details on the best practices
  - Information on different types of insider crimes
  - Mitigation strategies
- Consider the potential impacts of these practices prior to implementing in your organization
- Insider Threat Assessment
- Insider Threat Training / Workshops

Ongoing Research at CERT

- Continue insider threat case collection and analysis
- Transition our research from “The Problem” to “The Solution”
- Identify framework of new and existing controls for prevention and detection of malicious insider activity
  - Develop requirements for tools and best practices
    - Identification and weighting of potential indicators
    - Empirically based on actual cases
  - Collaborate with researchers, developer community, and practitioners
  - Refine based on pilot testing

Points of Contact

Technical Manager, Threat and Incident Management

Dawn M. Cappelli

CERT Program

Software Engineering Institute

Carnegie Mellon University

4500 Fifth Avenue

Pittsburgh, PA 15213-3890

+1 412 268-9136 – Phone

dmc@cert.org – Email

Senior Member of the Technical Staff, Threat and Incident Management

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/