We Have MET THE ENEMY

Keys to Preventing Insider Misuse In Your Organization

prepared by Al Lewis, CISSP, CISM
PRESENTER: Al Lewis, CISSP, CISM

- 29 years experience in federal information technology (systems integrator, contractor manager, executive)
- Past 15 years spent leading information security teams
  - U.S. Army, FBI, Supreme Court, Department of Energy
  - MITRE – 4 years, information security Policy & Compliance lead
- MS, Information & Telecommunication Systems, Johns Hopkins
It is time for Security Leaders to start looking at the insider threat/misuse problem from the point of view of a non-technologist.

- What are the business costs?
- How do we more effectively manage people?
We have known about the insider threat problem for years now

- CM CERT, SEI
- News headlines
  - Manning, Snowden

- Challenge
  - Involves people, processes, and technology
  - Requires multidisciplinary approach
WHAT IS “INSIDER THREAT”?
FIRST...WHAT IS AN INSIDER?

- Employees
- TRUSTED BUSINESS PARTNERS
  - CONTRACTORS
  - OUTSOURCED COMPANIES

Provided with ACCESS To:
- SYSTEMS
- Data (often sensitive)
INISIDER THREATS CAN BE...

Malicious
• With intent to harm
  • Espionage, fraud, sabotage

Accidental
• Without intent to harm

Q. WHICH IS MORE DESTRUCTIVE?
WHAT DOES A MALICIOUS INSIDER LOOK LIKE?
IT's NOT ME...

NOT ME...

MAYBE ME.
A MALICIOUS INSIDER COULD BE...

Profile

- Anyone
  - Sense of entitlement, or
  - Victim of perceived injustice
- Has access to assets
  - Systems
  - Sensitive data
- Causes harm to organization
  - Denial of service
  - Destruction or alteration of data
UNINTENTTIONAL

NOT

... TO BE...

... IGNORED...
SPECIAL

• Privileges given to:
  • Systems Administrators
  • Executives

Can create a feeling of entitlement where users are no longer willing to abide by rules meant to protect systems and data

Can encourage abuse of policy

“The rules don’t apply to me.”
ASSET LOSS or DESTRUCTION

- Data loss or compromise
- Denial of service

Reputational damage can occur as a result of an executed insider threat
MALICIOUS INSIDER CHARACTERISTICS:

• May take unauthorized material home
• Exceeds scope of work duties
• Remotely accesses systems at odd times
• Demonstrates a pattern of not following rules
• Disgruntled
• Under extreme stress (personal or work-related)
• Unusual behaviors
“But Jim…
…Why are malicious insiders a priority?”

“I have so many other CYBERsecurity Threats To worry about on our network…”
2015 – Cost of cyber crime study
Ponemon Institute © Research Report

- Surveyed 252 organizations in 7 countries
- Companies of 1,000 seats or more

- Malicious Insider –
  - Number one threat in 2 categories
COST & TIME TO RESOLVE
Figure 11. Average annualized cyber crime cost weighted by attack frequency

Consolidated view, n = 252 separate companies

- Malicious insiders: $144,542
- Denial of services: $126,545
- Web-based attacks: $96,424
- Phishing & SE: $85,959
- Malicious code: $81,500
- Stolen devices: $33,565
- Malware: $7,378
- Viruses, worms, trojans: $1,900
- Botnets: $1,075
Figure 13. Some attacks take longer to resolve
Estimated average time is measured for each attack type in days
Consolidated view, n = 252 separate companies

- Malicious insiders: 54.4 days
- Malicious code: 47.5 days
- Web-based attacks: 27.7 days
- Phishing & social engineering: 21.9 days
- Denial of service: 19.3 days
- Stolen devices: 12.3 days
- Malware: 5.8 days
- Viruses, worms, trojans: 2.4 days
- Botnets: 2.2 days
KNOW YOUR ASSETS

• All data and systems
• Data sensitivity categorization completed and applied to all appropriate data
Risk Assessments

IT Enterprise

- Include all parties
  - Business partners
  - Vendors
- Make risk of insider threat assessment part of your standard risk assessment process
- NIST 800-53 Rev. 4
  - 28 controls specific to insider threat
• Anticipate and manage negative issues in the work environment
• Develop a comprehensive employee termination procedure
PEOPLE

- Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior (full employee lifecycle)
- Incorporate insider threat awareness into periodic security training for all employees
TECHNICAL CONTROLS

• Institute stringent access controls and monitoring policies on privileged users.
• Institutionalize system change controls.
• Use a log correlation engine or (SIEM) system to log, monitor, and audit employee actions.
• Monitor and control remote access from all end points, including mobile devices
AGREEMENTS

Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
Establish

• A formal Insider Threat Program (PM-12)
• A baseline of normal network device behavior
• A process whereby the organization clearly documents and consistently enforces policies and controls
RECOVER

• Implement secure backup and recovery processes
Clearly document and consistently enforce policies and controls

Implement strict password and account management policies and practices
Enforce

- Strict password and account management policies and practices
- Separation of duties and least privilege
- Stringent access controls and monitoring policies on privileged users
Resources

Insider Threat

INSIDER THREAT CERTIFICATES AND TRAINING

Our Insider Threat training and certificate programs are available for program managers, vulnerability assessors, and program evaluators. Explore these training opportunities.

Did you know that cyberattacks from employees and other insiders is a common problem that you should be planning for and preventing? Insiders pose a substantial threat to your organization because they have the knowledge and access to proprietary systems that allow them to bypass security measures through legitimate means. The nature of insider threats is different from other cybersecurity challenges; these threats require a different strategy for preventing and addressing them.

At the CERT Insider Threat Center at Carnegie Mellon’s Software Engineering Institute (SEI), we are devoted to combating cybersecurity issues. Our research has uncovered information that can help you identify potential and realized insider threats in your organization, institute ways to prevent them, and establish processes to deal with them if they do happen.

Our Mission: We enable effective insider threat programs by performing research, modeling, analysis, and outreach to define socio-technical best practices so that organizations are better able to deter, detect, and respond to evolving insider threats.
CERT, Software Engineering Institute, Carnegie Mellon University  
Insider Threat Best Practices  
https://www.cert.org/insider-threat/best-practices

CERT Top 10 List for Winning the Battle Against Insider Threats  
Dawn Capelli, CERT Insider Threat Center, RSA 2012  
http://resources.sei.cmu.edu/asset_files/Presentation/2012_017_001_52427.pdf

Federal Bureau of Investigation, The Insider Threat: An introduction to Detecting and Deterring an Insider Spy  
https://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat

The Ponemon Institute, 2015 Cost of Cybercrime Study  