Components and Considerations in Building an Insider Threat Program

Carly Huth
Insider Threat Researcher, CEWM

Carly L. Huth is an insider threat researcher in the Cyber Enterprise and Workforce Management Directorate in the CERT Program at the Software Engineering Institute (SEI). Huth’s current areas of research include the intersections of privacy and technology as well as the effects of the current regulatory environment on insider threat prevention practices.

Robin Ruefle
Technical Staff - CERT

Robin Ruefle is a member of the technical staff of the CERT Program at the Software Engineering Institute (SEI) at Carnegie Mellon University. Ruefle has co-authored: Handbook for CSIRTs 2nd Edition, Organizational Models for CSIRTs Handbook, CSIRT Services List, State of the Practice of CSIRTs, Defining Incident Management Processes for CSIRTs: A Work in Progress, and numerous other articles and guides.
Motivation for a Program

“to ensure the responsible sharing and safeguarding of classified national security information on computer networks.”
Source: Executive Order 13587, quoted in GCN (http://s.tt/1ai6l)

To ensure protection of and appropriate access to intellectual property and other critical assets, systems, and data

To be prepared and ready to handle such events in a consistent, timely, and quality manner including understanding

• who to involve
• who has authority
• who to coordinate with
• who to report to
• what actions to take
• what improvements to make
Goal for a Program

Opportunities for prevention, detection, and response for an insider attack
Component Overview

- Cross-enterprise project planning and implementation group
- Designated staff to manage and operate the Insider Threat Program
- Multi-level training and awareness program
- Infrastructure support
  - Cross-organizational data collection and analysis
  - Incident Response Plan
  - Policies, procedures, and practices created or enhanced to support insider threat program
  - Protection of civil liberties and privacy rights
Insider Threat Program Participants (Notional)

- VP / CIO
  - Assistant Director
- CISO
  - Assistant Director
- VP / CFO
  - Assistant Director
- VP / COO
  - Assistant Director
- VP / Chief Legal Counsel
  - General Counsel
- Director of IT
  - Branch Chief or Unit Supervisor
- Information Assurance
- HR Director
  - Branch Chief or Unit Supervisor
- Physical Security Director
  - Branch Chief or Unit Supervisor
- Legal Counsel

Insider Threat Core Team

- Data Owners
- Legal
- Human Resources
- Information Technology
- SOC/C SIRT
- Software Engineers
- Union Representative
- Physical Security
- Facilities Operations
- Non-management workers
- Internal Audit
- Quality Assurance
- Contracting Group or COTR
- Partners, Suppliers, and Contractors

Note: Text below the separator in each box notes the federal government’s equivalent position.
Multi-level Training and Awareness

General awareness, training, and refreshers for all staff
- Definitions for insider threat
- Types of insider threat crimes and activities and motivations
- How staff can be targeted and social engineered
- When, how, and what to report – regarding suspicious human or computer activity
- Acceptable use policy and repercussions for violation
- Responsibility for protecting IP, data, and systems and for reporting

Role based training for areas of the organization
- HR
- Legal
- IT and Security
- Facilities

Specific training for Insider Threat Program staff
Infrastructure Support

Prevention and Detection

• Data loss prevention
• Monitoring, filtering, blocking

Data Collection and Analysis

• Synthesis and aggregation
• Correlation
• Repository for data analysis
Data Aggregation and Analysis

Determine types of data to be collected
Supporting authority and permission
Methods for obtaining data
Criteria for user monitoring
  • Privileged users
  • Role based
  • Asset based
Criteria for suspicious or potential malicious behavior
Scoring criteria
Alerting mechanisms
Escalation mechanisms
Incident Response Plan

How incidents perpetrated by insiders are:
- Detected
- Reported
- Contained
- Remediated
- Documented
- Prosecuted (if applicable)

How processes change for different types of threats:
- Fraud
- Theft of IP
- Sabotage
- Espionage

How processes change when involvement includes:
- Contracts and SLAs
- Unions
- Privileged users
- Cloud computing servers and data centers
Response Options

Internal

• Retraining
• Personnel actions
• Organizational sanctions
• Legal actions

External

• Referral to internal investigative unit or counter intelligence (if applicable)
• Referral to local or federal law enforcement if applicable

Response Considerations

• Think about response to precursors not just to incidents that have occurred.
• Responses must be documented and practiced consistently
• All response procedures should be coordinated with General Counsel
• Privacy and civil liberties must be consider at all times
Policies, Procedures, and Practices

Examples include but are not limited to:

- Reporting
  - Confidential reporting mechanism
  - Requirement to report
- Information Technology
  - Acceptable use
  - Separation of duties
  - Code reviews
  - Least privilege
  - No shared accounts
  - Change control
  - Configuration management
Criminal Background Screening Best Practices

Practices apply to all employment decisions, including promotions.

Even neutral policies can impact certain groups of candidates more than others; generally, policies shouldn’t automatically exclude all candidates with criminal history.

Be cautious when using arrest records, conviction records provide better evidence.

Train all relevant staff about complying with the equal employment laws and keep all candidate criminal information confidential.
Criminal Background Screening Best Practices

Screenings should be job related and consistent with a business need.

Often, a ‘targeted screening’ is recommended, where the employer considers:

- The nature of the crime
- How long ago the crime took place
- The nature of the job

6 Essential Legal Considerations

Create, maintain and enforce acceptable use and monitoring policies

Obtain employee acknowledgement of policies and communicate any updates

Don’t rely solely on policies; protect proprietary information through technical measures such as access controls
6 Essential Legal Considerations

Consider the need to review logs for evidence when creating your data retention policies

Be cautious of performing your own investigations, make sure to preserve evidence

Be prompt when issuing a legal response

Summary
Implementation Strategy

First 30-90 Days

- Obtain buy-in from top management
- Designate a senior manager to be the Insider Threat Program Manager
- Create a working group to plan the project and implementation (include representative from key areas)
- Collect information on what is already in place and can be leveraged
- Talk to others who have programs, research recommendations
- Identify the organizational structure of an enterprise Insider Threat Program
- Identify roles and responsibilities for the program

Next 90-180 Days

- Develop staffing requirements, competencies, and a workforce management plan
- Develop initial training requirements and materials
- Architect data collection, aggregation, and analysis methodology and tools
The CERT Top 10 List for Winning the Battle Against Insider Threats

10. Learn from past incidents
9. Focus on protecting the "crown jewels"
8. Use your current technologies differently
7. Mitigate threats from trusted business partners
6. Recognize concerning behaviors as a potential indicator
5. Educate employees regarding potential recruitment
4. Play close attention at resignation/termination
3. Address employee privacy issues with General Counsel
2. Work together across the organization
1. Create an Insider threat program NOW!
CERT Resources

Insider Threat Center website
(http://www.cert.org/insider_threat/)

(http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm)

The Insider Threat and Employee Privacy: An Overview of Recent Case Law, Computer Law and Security Review, Volume 29, Issue 4, August 2013 by Carly L. Huth

Insider threat workshops

Insider threat assessments

New controls from CERT Insider Threat Lab

Insider threat exercises

The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) (SEI Series in Software Engineering) by Dawn M. Cappelli, Andrew P. Moore and Randall F. Trzeciak
Points of Contact

Robin M. Ruefle
Technical Team Lead, ETVM
Organizational Solutions
CERT Program, Software Engineering Institute
Phone: +1 412 268-6752
Email: rmr@cert.org

Carly L. Huth
Member of the Technical Staff, ETVM
CERT Program, Software Engineering Institute
Phone: +1 412 268-5760
Email: clhuth@cert.org