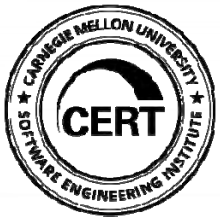


Model-Driven Insider Threat Control Selection and Deployment

Randy Trzeciak

Dan Costa

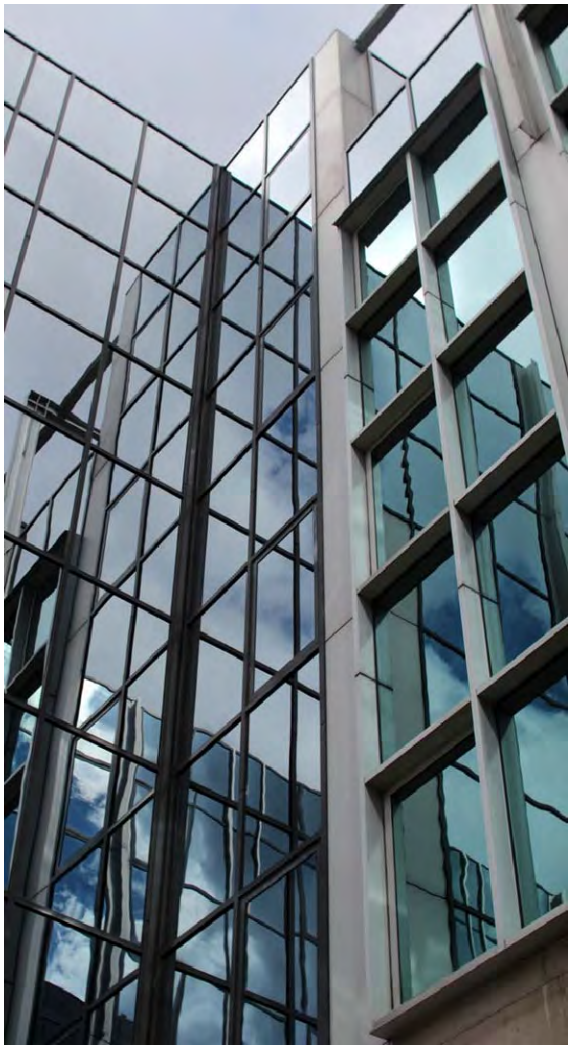
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM17-0967

The CERT Insider Threat Center



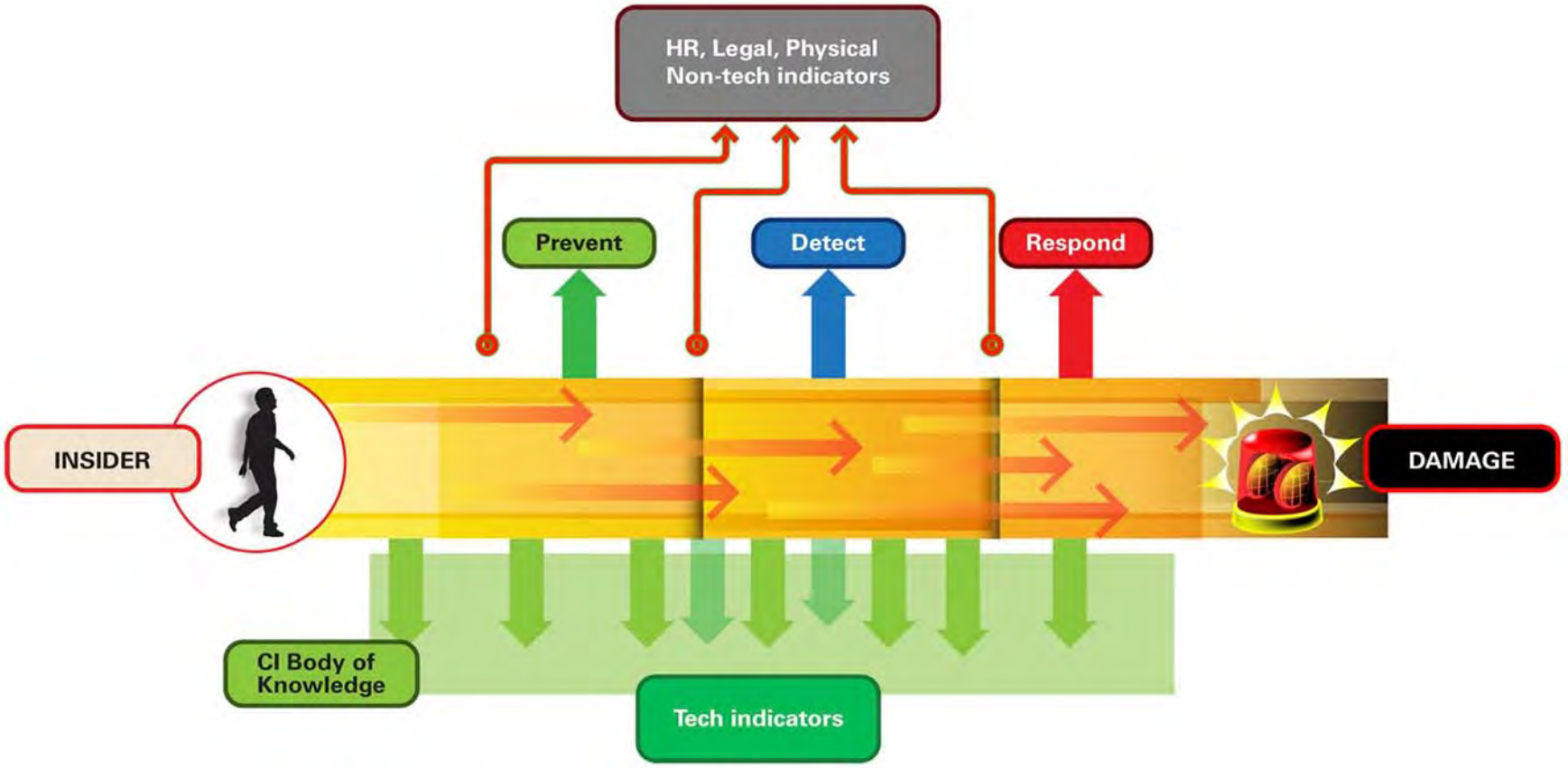
- Center of insider threat expertise
- Began working in this area in 2001 with the U.S. Secret Service
- Mission: enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber and physical threats
- Action and Value: conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats

CERT's Definition of Insider Threat

The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Scope of the Insider Threat

Goal for an Insider Threat Program



Cybersecurity Control Methods

Once risks to the organization have been identified/prioritized, select and implement appropriate security controls.

Technical

- Safeguards incorporated into computer hardware, software, or firmware

Physical

- Cameras
- Alarms

Administrative

- Policies
- Operational procedures

Common Cybersecurity Controls

Technical

- Cryptography
- Virtual Private Networks (VPNs)
- De-Militarized Zone (DMZ)
- Firewalls
- Access Control Lists
- Proxy Servers
- Address Translation
- Intrusion Detection/Prevention Systems
- Honeypots

Physical

- HVAC
- Fire Suppression
- EMI Shielding
- Environmental Monitoring
- Video Monitoring
- Fences, Gates, and Walls
- Lighting
- Access Cards
- Guards
- Locks
- Turnstiles and Mantraps

Administrative

- Policies and Procedures
- Personnel Policies
- Passwords Policies
- Service Level Agreements (SLAs)
- Security Related Awareness and Training
- Change Management
- Configuration Management
- Patch Management
- Archival, Backup, and Recovery Procedures

Classes of Cybersecurity Controls

Class	Family
Management	Certification, Accreditation, and Security Assessments
	Planning
	Risk Assessment
	System and Services Acquisition
Operational	Awareness and Training
	Configuration Management
	Contingency Planning
	Incident Response
	Maintenance
	Media Protection
	Personnel Security
	Physical and Environmental Protection
	System and Information Integrity
Technical	Access Control
	Audit and Accountability
	Identification and Authentication
	System and Communications Protection

Source: NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems"

Control Function Categories

Preventive
- prevent intentional or unintentional harm
- examples: prohibit unauthorized network connections via policy, technical (firewall), and physical (locks) controls

Detective
- identify and report unauthorized or suspicious activity
- examples: log monitoring, system audits, file integrity checkers, motion detection

Corrective
- respond to and fix a security concern, and limit or reduce further damage
- examples: virus removal procedures, updating firewall rules to block attacking IP addresses

Recovery
- restore operations after an incident
- examples: disaster recovery procedures, restoring data from backup after deletion

Deterrent
- discourage security violations
- examples: security cameras, “unauthorized access prohibited” signs, monitoring policies

Compensating
- alternatives to recommended or normal controls that cannot be used
- examples: enhanced monitoring on a server that cannot have antivirus software installed due to interference with a critical application

NIST SP 800-53 Revision 4 Insider Threat Controls

Selecting Security Controls

Consider your possible threat scenarios (fraud, theft of IP, sabotage, etc.)

Decompose the threat scenarios into their component parts

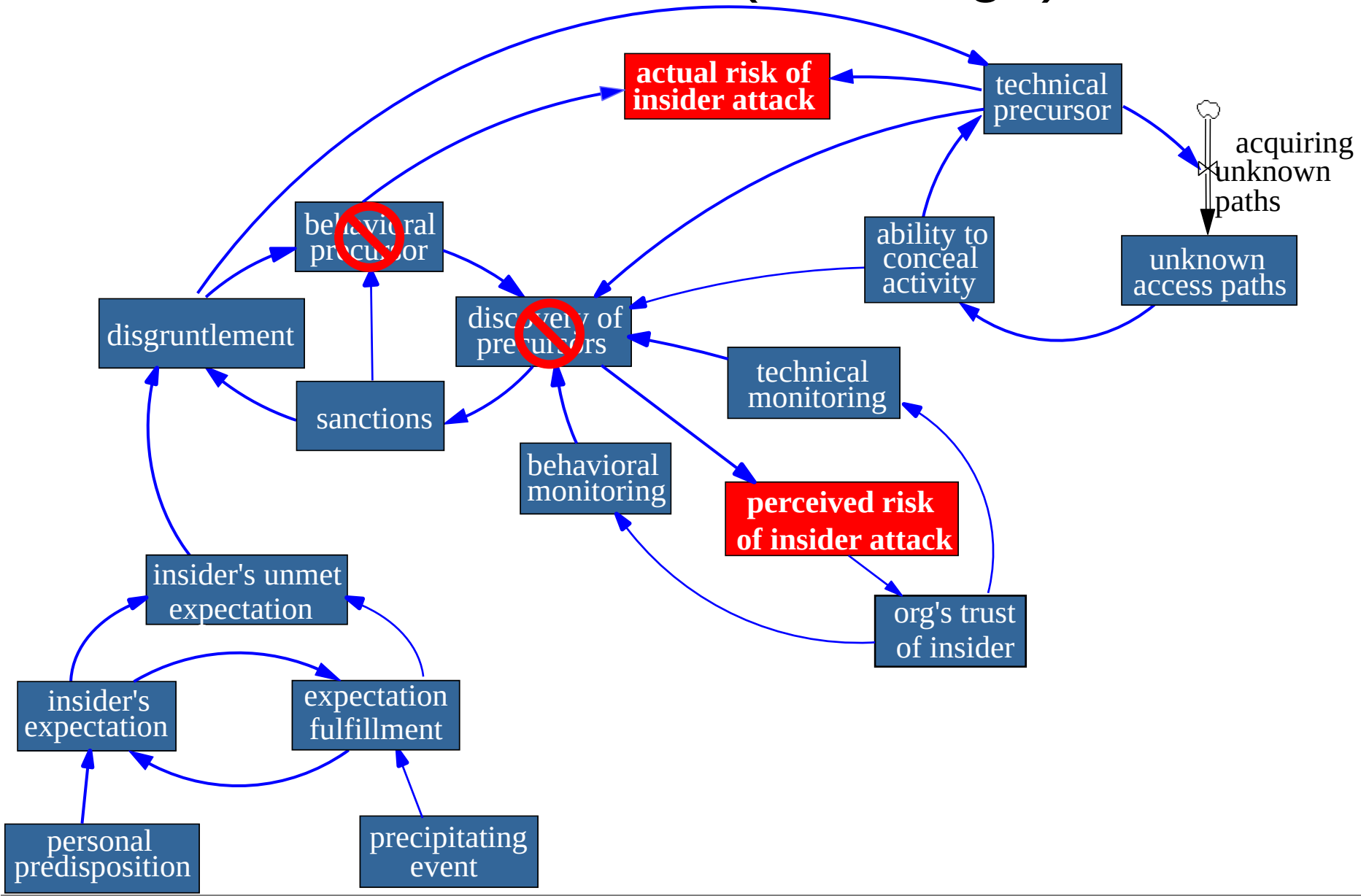
- Models can help here

Map threat scenario (model) components to observables

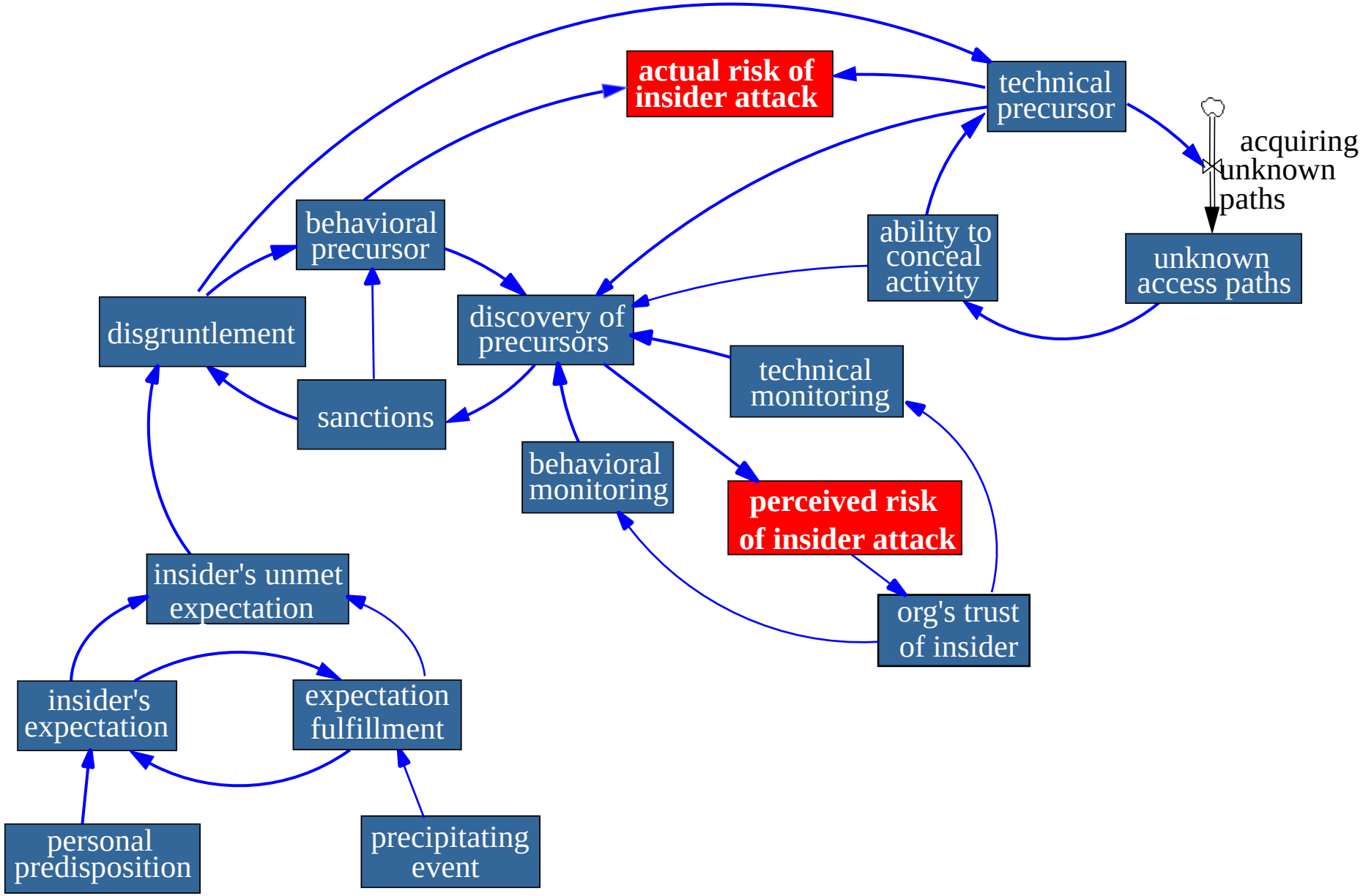
Map observables to controls

- Select controls of varying functions (preventative, detective, corrective, deterrent, etc.) for a defense-in-depth strategy

Insider Incident Model (Sabotage)



Insider Incident Model (Sabotage)



Mapping Model Components to Observables

Model Component	Associated Observables
Personal Predispositions	Co-worker conflicts
	History of policy / rule violations
	Aggressive, angry or violent behavior
Unmet Expectations	Being passed over for a promotion
	Being demoted or transferred
	Issues with supervisor
	Disagreement over salary and compensation
Behavioral Precursors	Co-worker or supervisor conflicts
	Sudden decline in work performance or attendance
	Aggressive, violent, or angry behavior
	Substance abuse
Technical Precursors	Creating backdoor, shared, non-attributable, or unauthorized accounts
	Tampering with, disabling, or attempting to disable security controls
	Downloading and installing malicious code and / or hacking tools
Concealment	Using backdoor, shared, non-attributable, or unauthorized accounts
	Modifying or deleting logs or backups
	Failing to record physical access
Crime Script	Modification / deletion of critical data
	Denial of service attack
	Physical attack to equipment
	Insertion of malicious code into operational system

Mapping Observables to Controls

Observable	Associated Control	Control Type
Co-worker conflicts	Human Resource Management System	Detective
	Anonymous / Confidential Reporting System	Detective
History of policy / rule violations	Human Resource Management System	Detective
	SF-86 Files	Detective
Aggressive, angry or violent behavior	Anonymous / Confidential Reporting System	Detective
Being passed over for a promotion	Human Resource Management System	Detective
Being demoted or transferred	Human Resource Management System	Detective
Issues with supervisor	Human Resource Management System	Detective
Disagreement over salary and compensation	Human Resource Management System	Detective
Co-worker or supervisor conflicts	Human Resource Management System	Detective
	Anonymous / Confidential Reporting System	Detective
Sudden decline in work performance or attendance	Employee Performance Management System	Detective
	Sanctions	Corrective
Aggressive, violent, or angry behavior	Anonymous / Confidential Reporting System	Detective
Substance abuse	Human Resource Management System	Detective
Creating backdoor, shared, non-attributable, or unauthorized accounts	Host-based audit logs	Detective
	Host-based audit logs	Detective
Tampering with, disabling, or attempting to disable security controls	Host-based audit logs	Detective
Downloading and installing malicious code and / or hacking tools	Application blacklisting / whitelisting	Preventative
	Host-based audit logs	Detective
Using backdoor, shared, non-attributable, or unauthorized accounts	Host-based audit logs	Detective
	Authentication server logs	Detective
Modifying or deleting logs or backups	Host-based audit logs	Detective
Failing to record physical access	Badging system logs	Detective
Modification / deletion of critical data	Change and configuration management systems	Detective
	Backup systems	Recovery
Denial of service attack	Server logs	Detective
Physical attack to equipment	Locks	Preventative
	Cameras	Detective
Insertion of malicious code into operational system	Change and configuration management systems	Detective

Security Control Metrics

Coverage

- example: percentage of systems covered by a host-based user activity monitoring system

Latency

- example: average time between malicious activity and discovery by insider threat team

Compliance

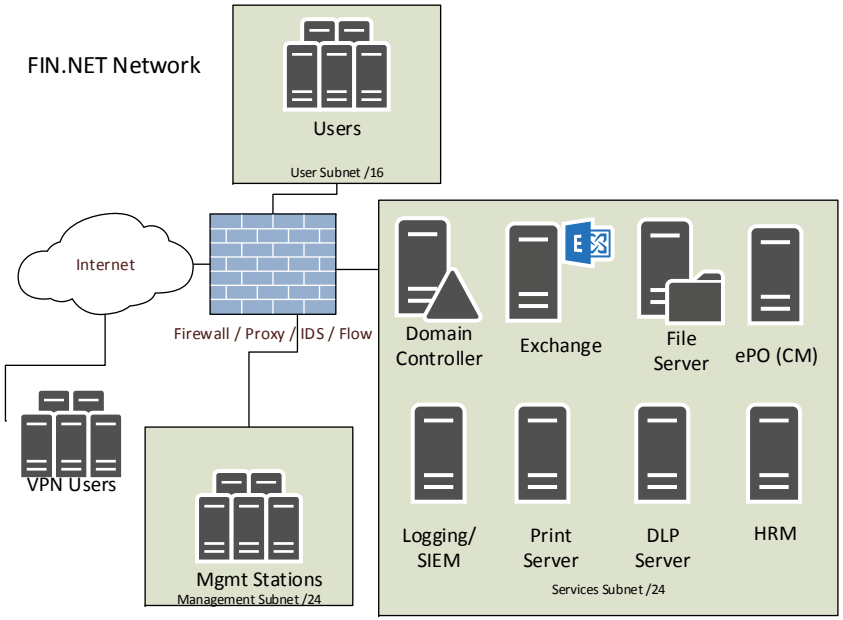
- example: percentage of recommended / required (NIST SP 800-53, NITTF Minimum Standards) controls implemented

Impact

- example: number of incidents prevented, reduction in time to resolve allegations, reduction in number of incidents over time

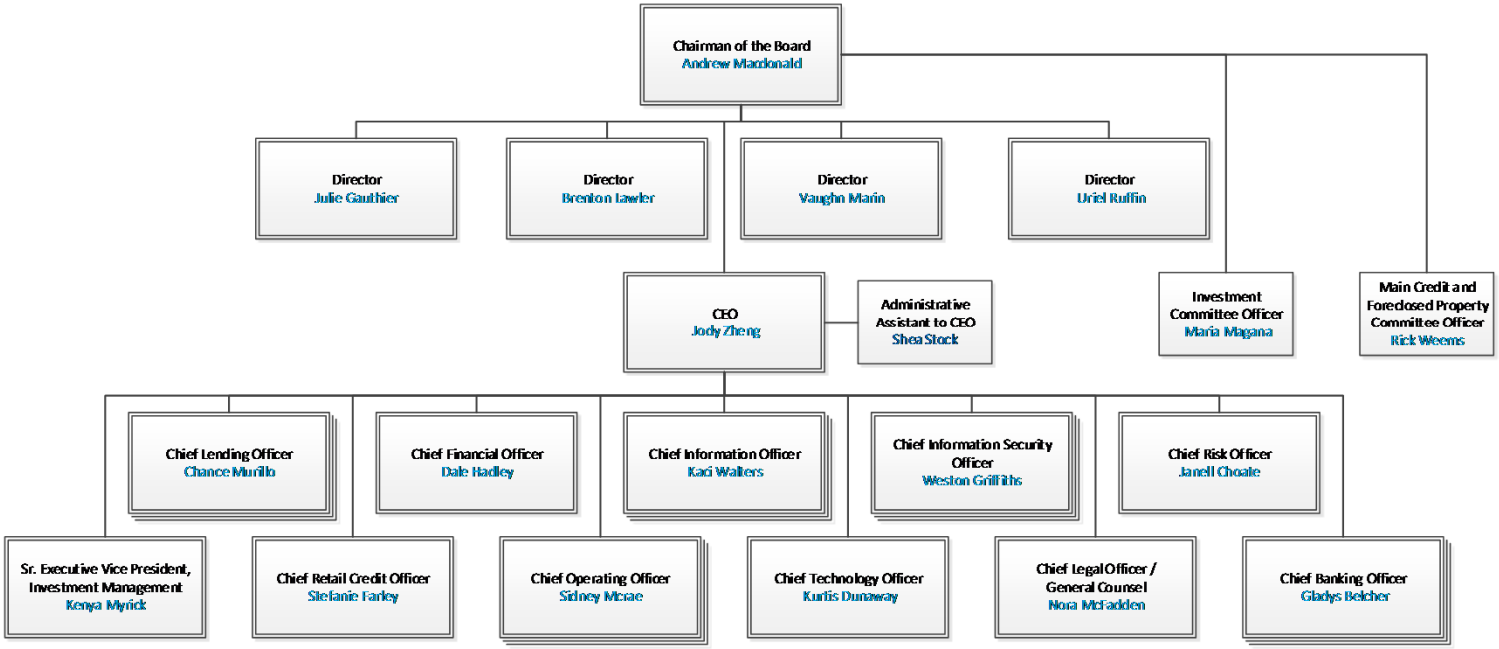
Insider Threat Control Deployment – A Reference Implementation

NeedleStack



- Virtual lab for insider threat
  - Tool testing (current)
  - Analyst training (FEB 2018)
  - Indicator testing (Summer 2018+)
- Exercise instance on the CERT STEPfwd platform
- Foundation of the CERT National Insider Threat Center

Current Simulated Environment



Fin.Net

- Small organization in the banking and finance sector
- 100 Employees
- Policies for:
  - Data classification
  - Acceptable Use

Auditable User Activity

Sending and receiving email

- To and from internal and external accounts
- Using work and personal accounts
- Using Outlook and Webmail services

Browsing the web

- To internal and external sites
- To work-related and non-work-related sites

Creating, reading, updating, and deleting files

- Stored locally and on network drives
- .docx, .xlsx, .pptx, .pdf, .zip, log files
- Modify file extensions and headers
- Encrypting files
- Taking screenshots

Using:

- Cloud-Based Storage
- Removable Media
- VPN
- Scanners
- Printers
- Remote Access Protocols (RDP,SSH)

Auditable Human Resource Management System Incidents

Incident Type	Description
Drug or Alcohol Violation	Consuming alcoholic beverages during work hours, except at approved company functions, or the possession or consumption of illegal drugs.
Information Integrity Violation	Intentional falsification of personnel records, payroll reports or other company records.
Property Violation	Theft, intentional destruction, or defacing of company or other employee property.
Violent Behavior	Abusive, threatening or coercive treatment of another employee or client. Aggressive, hostile or violent behavior, such as intimidation of others; or subjecting others to emotional distress.
Gambling Violation	Gambling, lottery, or any other game of chance on the employer's premises during working hours.
Confidentiality Agreement Violation	All employees must hold any confidential information in confidence, and not use or disclose it, except as necessary in the performance of duties or as required by law or contract.
IT Policy Violation	Excessive violation of company IT policies.
Legal Violation	Violation of local, state, or federal law which causes unfavorable publicity to the company, impairs the ability to perform the employee's job or is connected to company employment.
Insubordination	Employees must obey company directives issued by their supervisor. A refusal to obey a supervisor's order or a lack of respect will subject employee to progressive disciplinary actions.
Employee Leave Policy Violation	Employees are responsible for notifying supervisors of absences, late arrivals, or early departures each day of the absence, tardiness or early departure, in accordance with company policy.
Hostility	Behavior that creates an environment considered intimidating, hostile, or offensive to a reasonable person.
IP Policy Violation	Property violation infringing on intellectual property agreement

Other Auditable Personnel Events

- Salary Changes
- Promotions
- Promotion Applications
- Demotions
- Terminations
- Suspensions
- Job Performance Reviews

NeedleStack Data Sources

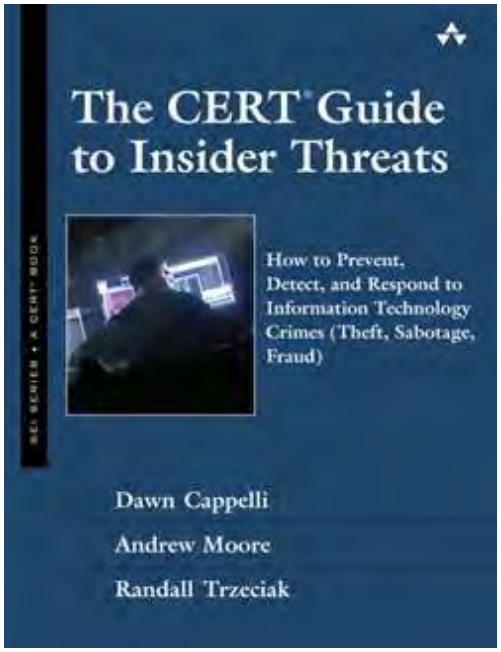
Data Type	Source/Sensor	Format	In SIEM?
Web Traffic	Squid Proxy 3.4 (pfSense)	Syslog (via pfSense)	Yes
Document Traffic	Microsoft File Services Audit Logging	Windows Event Log	Yes
Email	Microsoft Exchange 2010	Windows Event Log Exchange Message Tracking	Yes
SIEM	ArcSight Logger 6.2.0 ArcSight ESM 6	ArcSight CEF	N/A
Configuration Management	McAfee ePO 5.1.1 (HBSS) McAfee Solidcore 7.0.1 (HBSS)	ArcSight CEF via McAfee Database SmartConnector	Yes
Data Loss Prevention	Comodo MyDLP	Syslog	Yes
Anti-Virus	McAfee Endpoint Protection (HBSS)	ArcSight CEF via McAfee Database SmartConnector	Yes
IDS	Snort (pfSense)	Syslog (via pfSense)	Yes
Netflow	pfSense – Netflow v9	ArcSight CEF via Netflow SmartConnector	Yes
Firewall	pfSense	Syslog	Yes
Human Resource Management	Open Source HRM - Sentrifugo	Custom syslog format or Custom MySQL ODBC	Yes

Best Practices for Mitigating Insider Threats

Recommended Best Practices for Insider Threat Mitigation

1 - Know and protect your critical assets.	11 - Institute stringent access controls and monitoring policies on privileged users.
2 - Develop a formalized insider threat program.	12 - Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
3 - Clearly document and consistently enforce policies and controls.	13 - Monitor and control remote access from all endpoints, including mobile devices.
4 - Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	14 - Establish a baseline of normal behavior for both networks and employees
5 - Anticipate and manage negative issues in the work environment.	15 - Enforce separation of duties and least privilege.
6 - Consider threats from insiders and business partners in enterprise-wide risk assessments.	16 - Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
7 - Be especially vigilant regarding social media.	17 - Institutionalize system change controls.
8 - Structure management and tasks to minimize unintentional insider stress and mistakes.	18 - Implement secure backup and recovery processes.
9 - Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	19 - Close the doors to unauthorized data exfiltration.
10 - Implement strict password and account management policies and practices.	20 - Develop a comprehensive employee termination procedure.

CERT Insider Threat Resources and Services



- Insider Threat Awareness Training
- Insider Threat Certificate Programs
- Insider Threat Analyst Training
- Insider Threat Vulnerability Assessments
- Insider Threat Program Evaluations
- Technical Reports
  - CERT Common Sense Guide to Mitigating Insider Threats
  - Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector
  - Unintentional Insider Threats: A Foundational Study
- Technical Controls
  - Using Plagiarism Detection Algorithms to Prevent Data Exfiltration in Near Real Time
  - Using a SIEM signature to detect potential precursors to IT Sabotage
  - Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources
- Insider Threat Blog
- Insider Threat Data Analytics and Hub Development
- Customized Insider Threat Research

Contact Information

Presenter / Point of Contact

Randy Trzeciak

Director, CERT Insider Threat Center

Email: rft@sei.cmu.edu

412.268.7040

Daniel Costa

Technical Solutions Team Lead, CERT Insider Threat Center

Email: dlccosta@sei.cmu.edu

412.268.8006