RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HUM-R02

# A FRAMEWORK TO EFFECTIVELY DEVELOP INSIDER THREAT CONTROLS

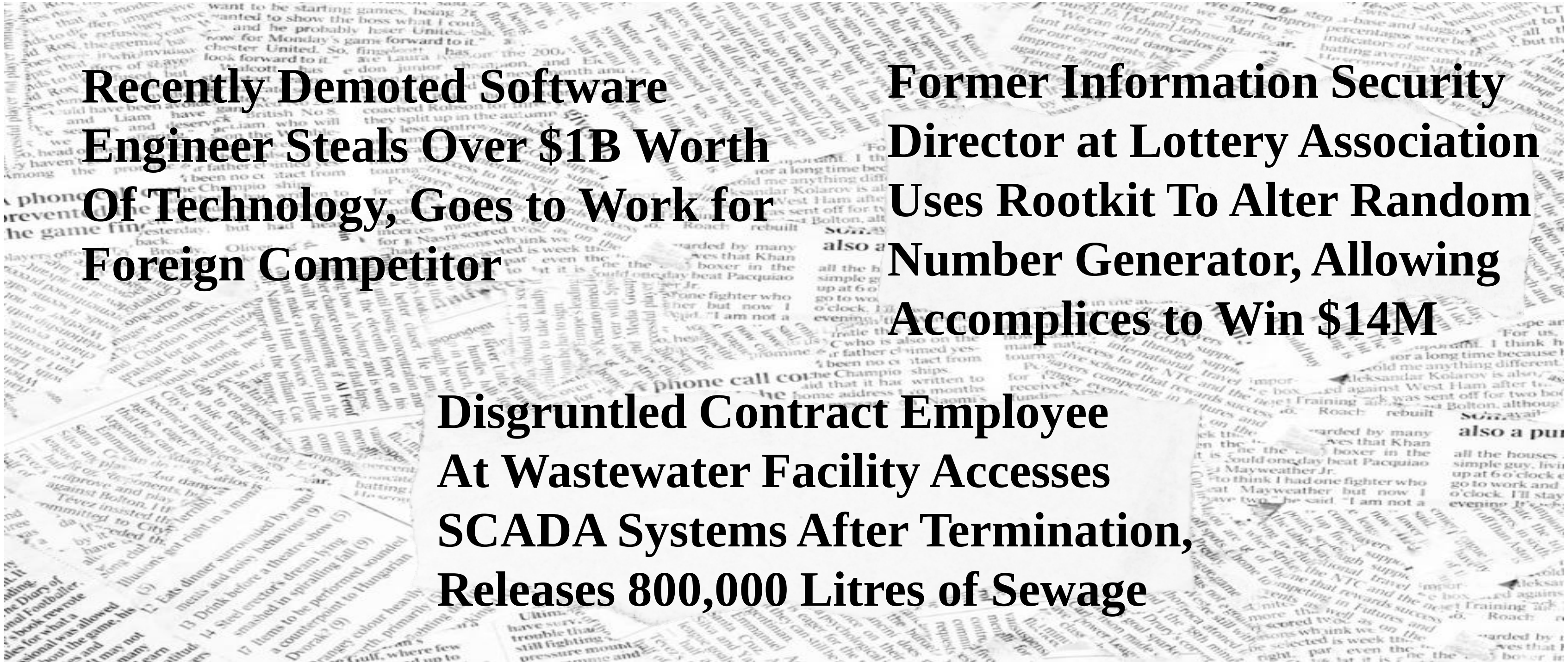
**Randy Trzeciak**

Director
CERT National Insider Threat Center
Software Engineering Institute
Carnegie Mellon University

**Dan Costa**

Technical Solutions Team Lead
CERT National Insider Threat Center
Software Engineering Institute
Carnegie Mellon University

# Can This Happen to Your Organization?

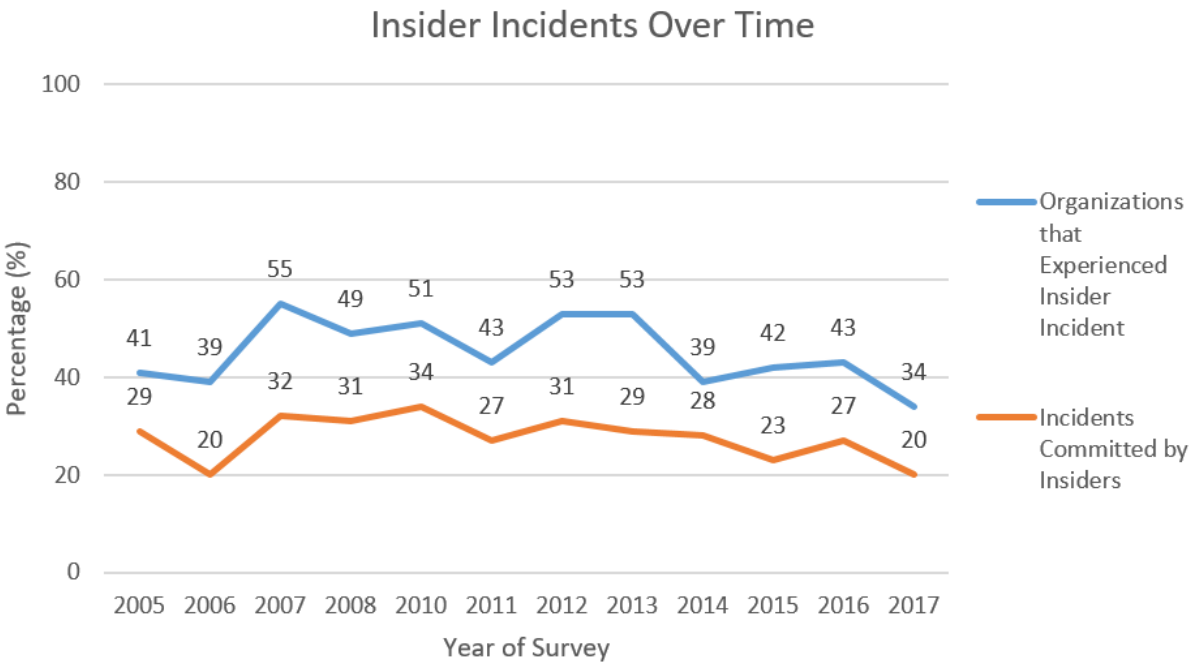


**Recently Demoted Software Engineer Steals Over $1B Worth Of Technology, Goes to Work for Foreign Competitor**

**Former Information Security Director at Lottery Association Uses Rootkit To Alter Random Number Generator, Allowing Accomplices to Win $14M**

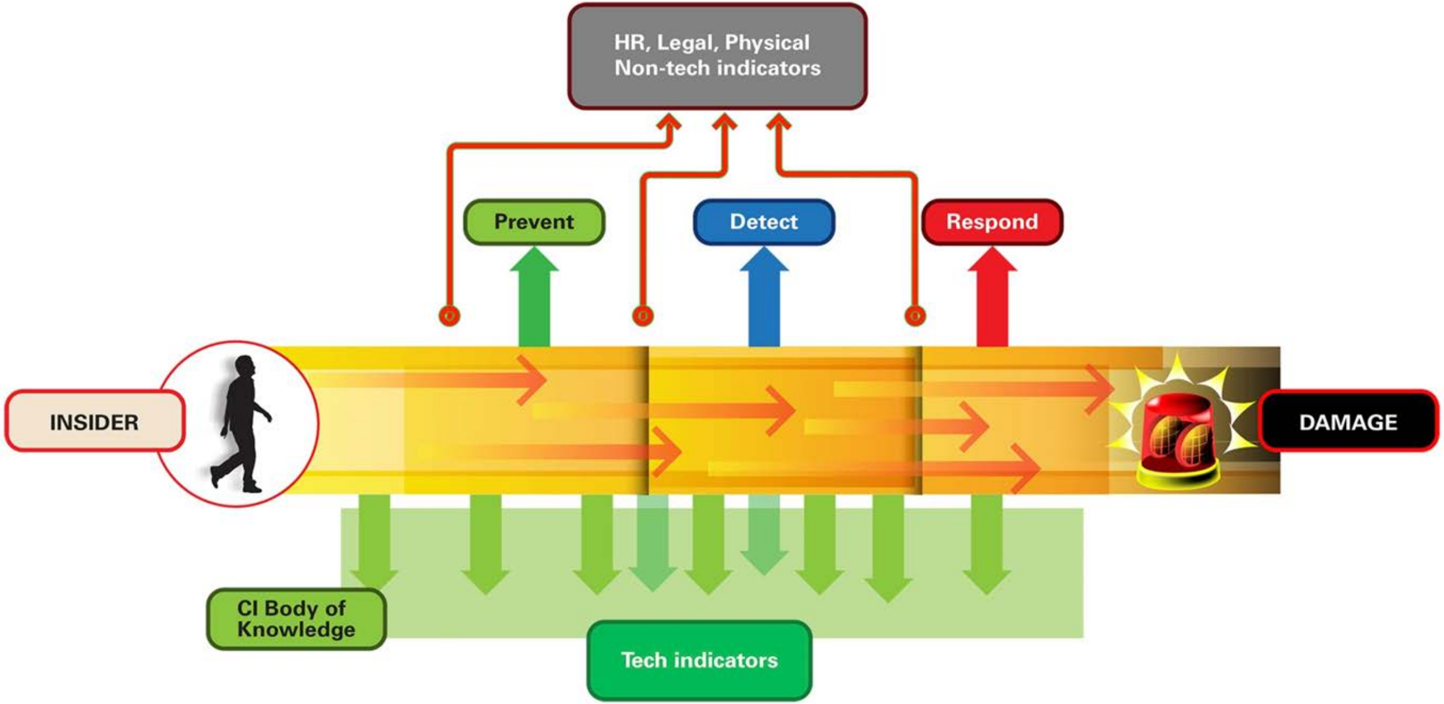
**Disgruntled Contract Employee At Wastewater Facility Accesses SCADA Systems After Termination, Releases 800,000 Litres of Sewage**

# How Pervasive is the Issue?



Source: U.S. State of Cybercrime Surveys, 2005-2017, CSO Magazine, USSS, Carnegie Mellon Software Engineering Institute, Price Waterhouse Cooper, ForcePoint

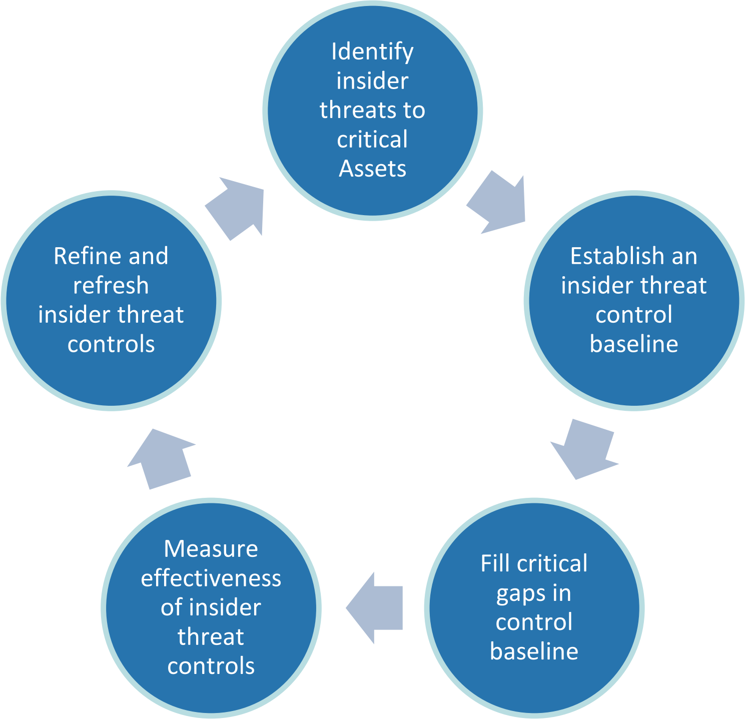
# What Can You Do?



# Presentation Objectives

- Help you:
  - identify, select, develop, and implement insider threat controls
  - navigate the insider threat control landscape
  - measure the effectiveness of your insider threat controls

# A Process for Insider Threat Control Implementation and Operation



Identify insider threats to critical Assets

Establish an insider threat control baseline

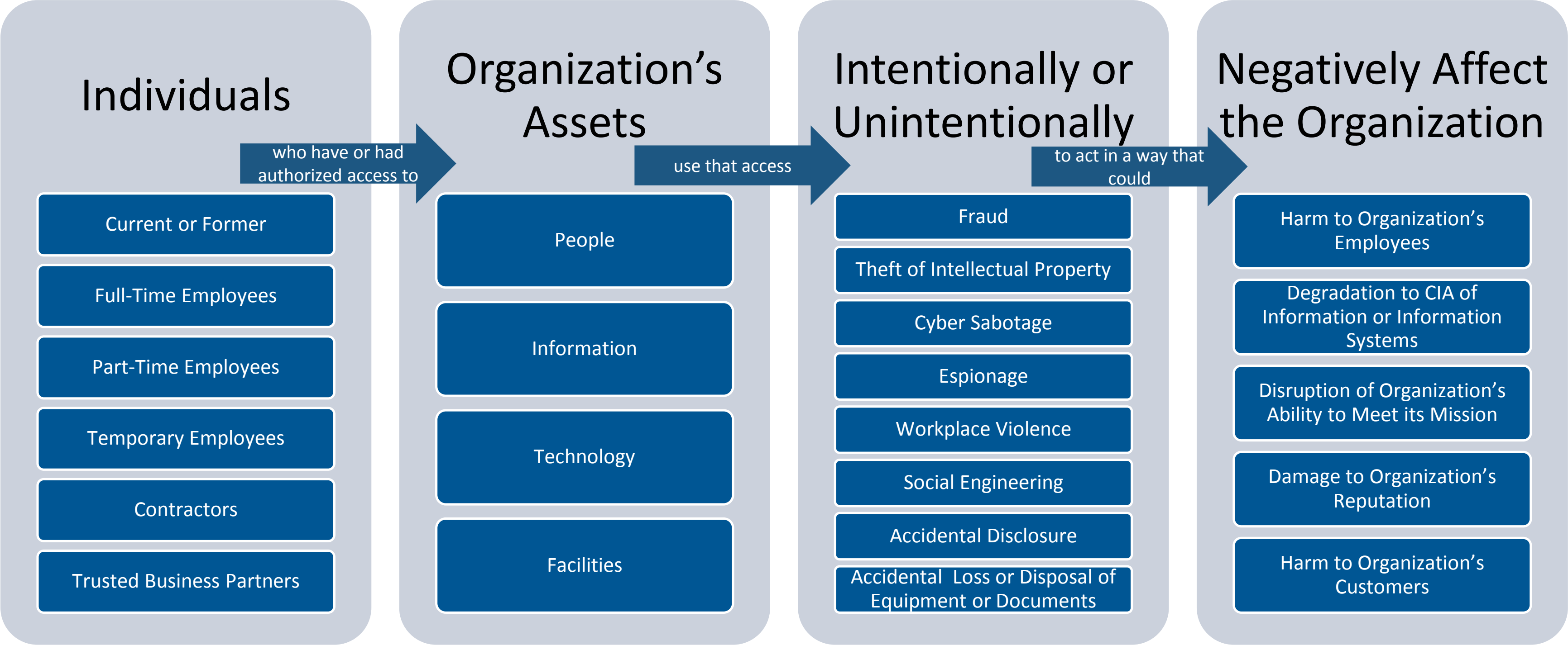
Fill critical gaps in control baseline

Measure effectiveness of insider threat controls

Refine and refresh insider threat controls

# IDENTIFYING INSIDER THREATS TO CRITICAL ASSETS

# Insider Threats to Critical Assets



## Individuals

who have or had authorized access to

- Current or Former
- Full-Time Employees
- Part-Time Employees
- Temporary Employees
- Contractors
- Trusted Business Partners

## Organization’s Assets

use that access

- People
- Information
- Technology
- Facilities

## Intentionally or Unintentionally

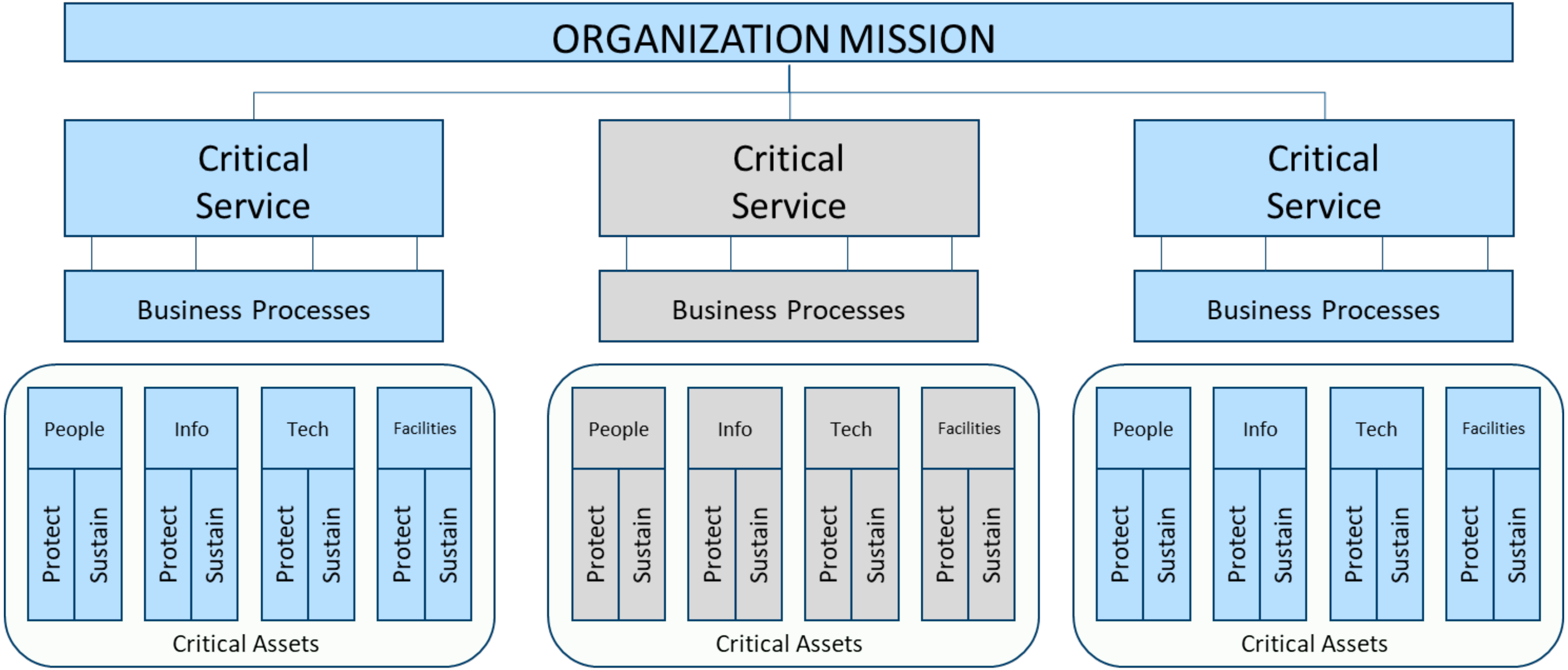
to act in a way that could

- Fraud
- Theft of Intellectual Property
- Cyber Sabotage
- Espionage
- Workplace Violence
- Social Engineering
- Accidental Disclosure
- Accidental  Loss or Disposal of Equipment or Documents

## Negatively Affect the Organization

- Harm to Organization’s Employees
- Degradation to CIA of Information or Information Systems
- Disruption of Organization’s Ability to Meet its Mission
- Damage to Organization’s Reputation
- Harm to Organization’s Customers

# Identifying Insider Threats Within Your Organization - 1



ORGANIZATION MISSION

# Identifying Insider Threats Within Your Organization - 2

- Don’t guess! Get the right people involved
  - Enterprise risk management
  - Business process owners
  - Executive leadership team
  - Board of directors
- Prioritize threats relative to potential impacts / priorities of your organization
  - What’s more important: your organization’s reputation, or its intellectual property?
    - Who makes this call?

# ESTABLISHING AN INSIDER THREAT CONTROL BASELINE

# Insider Threat Controls

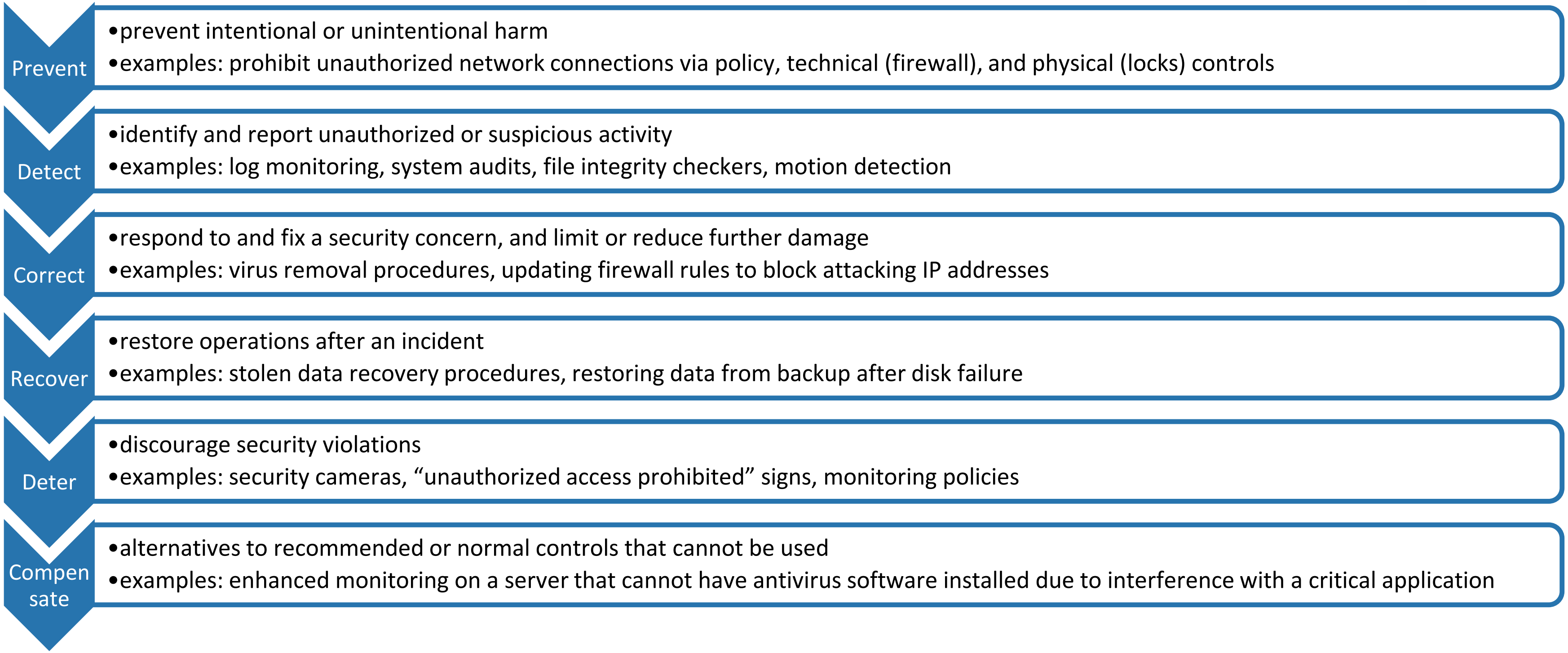
## Steps to Success

- Figure out what you need
  - Standards can help
- Figure out what you already have
  - Traditional cybersecurity controls provide a solid foundation of capability
  - Consider technical, physical, and administrative controls
  - Engage other key parts of your organization!

## Control Areas by Stakeholder

| Data Owners | Human Resources | Information Technology | Legal | Physical Security | Software Engineering |
|---|---|---|---|---|---|
| Access Control | Recruitment | Access Control | Agreements to Protect Sensitive Information | Facility Security | Technical Policies and Agreements |
| Modification of Data, Systems, Logs | Policies and Practices | Modification of Data or Disruption of Services / Systems | Restrictions on Outside Employment | Physical Asset Security | Modification of Data or Systems |
| Unauthorized Access, Download, or Transfer of Assets | Training, Education, and Evaluation | Unauthorized Access, Download, or Transfer of Assets | Employee Behaviors in the Workplace | | Asset Management |
| Incident Response | Policy and Practice Monitoring and Enforcement | Incident Response | Contractor / Trusted Business Partner Agreements | | |
| Termination | Termination | Termination | | | |

# Different Control Functions



Prevent

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

Detect

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

Correct

- 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

Recover

- restore operations after an incident
- examples: stolen data recovery procedures, restoring data from backup after disk failure

Deter

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

Compensate

- 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 - 1

- IR-4 (6) INCIDENT HANDLING | INSIDER THREATS – SPECIFIC CAPABILITIES
- IR-4 (7) INCIDENT HANDLING | INSIDER THREATS – INTRA-ORGANIZATION COORDINATION
- MP-7 MEDIA USE
- PE-2 PHYSICAL ACCESS AUTHORIZATIONS
- PS-3 PERSONNEL SCREENING
- PS-4 PERSONNEL TERMINATION
- PS-5 PERSONNEL TRANSFER
- PS-8 PERSONNEL SANCTIONS
- SC-5 (1) DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS
- SC-7 BOUNDARY PROTECTION
- SC-7 (9) BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC
- SC-7 (10) BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION
- SC-38 OPERATIONS SECURITY
- SI-4 (12) INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS

# NIST SP 800-53 Revision 4 Insider Threat Controls - 2

- PM-12 (0) INSIDER THREAT PROGRAM
- PM-1 INFORMATION SECURITY PROGRAM PLAN
- PM-14 TESTING, TRAINING, AND MONITORING
- AC-6 (9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS
- AT-2 (2) SECURITY AWARENESS | INSIDER THREAT
- AU-6 (9) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INPUT FROM NON-TECHNICAL SOURCES
- AU-7 AUDIT REDUCTION AND REPORT GENERATION
- AU-10 NON-REPUDIATION
- AU-12 AUDIT GENERATION
- AU-13 MONITORING FOR INFORMATION DISCLOSURE
- CA-2 (2) SECURITY ASSESSMENTS | TYPES OF ASSESSMENTS
- CA-7 CONTINUOUS MONITORING
- CP-2 (1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS
- IA-4 IDENTIFIER MANAGEMENT

# Tools for Detecting, Preventing, and Responding to Insider Incidents

## User Activity Monitoring (UAM)

- Provide host-based audit, monitoring, and preventative controls Observe and record host-based activities of (applications executed, file access and modification, clipboard activity)
- Key capabilities: rule-based alerting, screen capture / video recording, analyst interface

## Data Loss Prevention (DLP)

- Detect and prevent sensitive information from leaving authorized locations
- Key capabilities: data tagging, content inspection, active monitoring of print jobs, removable media, file systems, and networks

## Security Information Event Management (SIEM)

- Log aggregation and analysis capability typically found in security operations centers (SOC's)
- Key capabilities: data visualization, rule-based alerting, reporting, data normalization

## Analytics

- Broad range of tools that perform advanced analytics for insider threat prevention and detection
- Key capabilities: anomaly detection, risk scoring, predictive analytics, text analytics, analyst interface

## Forensics

- Tools that provide incident responders with detailed low-level views of user activity
- Key capabilities: storage medium acquisition, forensic artifact extraction, forensic artifact management and analysis

# Policies and Procedures for Insider Threat Mitigation

## Reminder

- Don’t forget your administrative controls!
  - Policies, procedures, documentation codify “normal” behavior - important for anomaly detection

## Exemplars

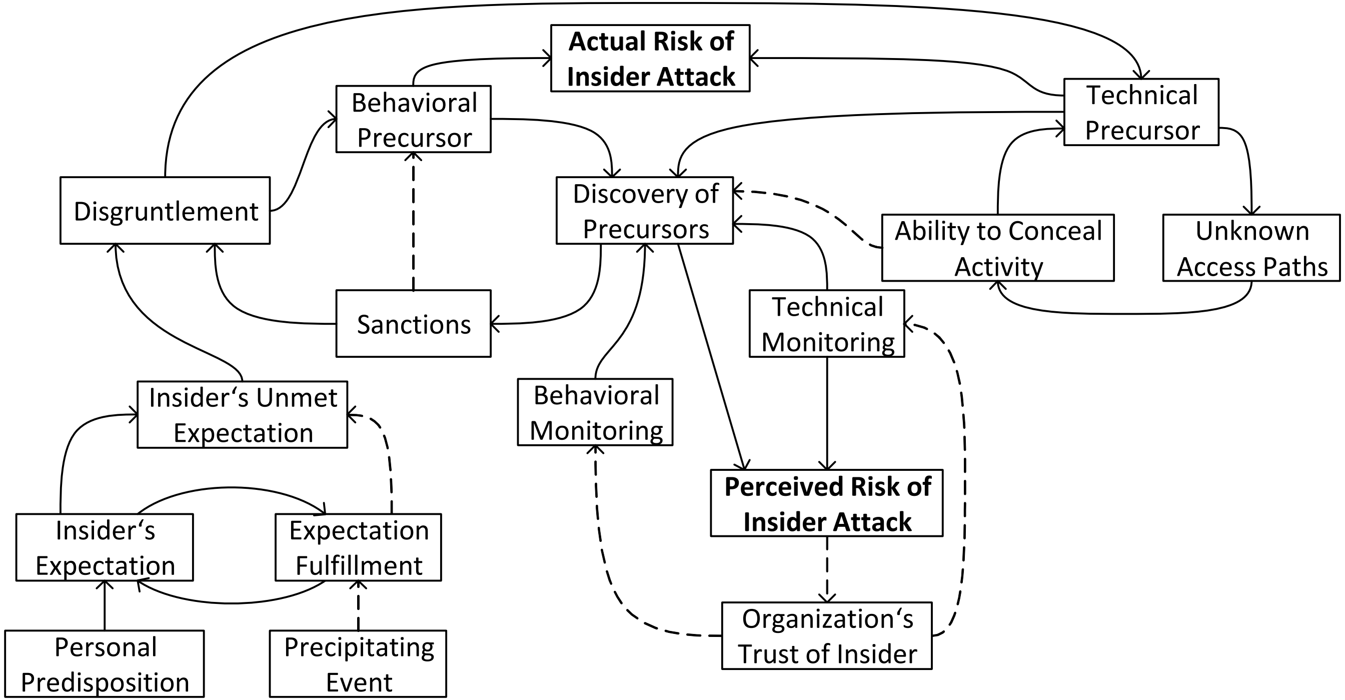
- IT Acceptable Use Policy
- Intellectual Property Policy
- Data Handling and Classification Policy
- Change Control and Configuration Management Policy
- Employee Onboarding Procedures
- Incident Response Plan
- Disciplinary Action Procedures
- Employee Separation Handling
- Trusted Business Partner Agreements

# SELECTING AND IMPLEMENTING ADDITIONAL 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 components to observables
- Map observables to controls
  - Select controls of varying functions (preventative, detective, corrective, deterrent, etc.) for a defense-in-depth strategy

# Example – IT Systems Sabotage Model



# 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 |

| Model Component | Associated Observables |
|---|---|
| Technical Precursors | Creating backdoor, shared, non-attributable, or unauthorized accounts |
| | 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 |
| | Inserting malicious code into system |

# Mapping Observables to Controls - 1

| 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 |
| | Background Checks | 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 |

# Mapping Observables to Controls - 2

| Observable | Associated Control | Control Type |
|---|---|---|
| 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 |
| 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 |

# Mapping Observables to Controls - 3

| Observable | Associated Control | Control Type |
|---|---|---|
| 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 |

# MEASURING EFFECTIVENESS OF INSIDER THREAT CONTROLS

# Measures of Effectiveness

- Coverage
  - % of endpoints monitored
- True/False Positive/Negatives for Detective Controls
  - Important to understand the difference between a faulty detective control (cameras record black and white video) and a bad insider threat indicator (insiders wear blue shirts)
- Impact
  - Reduced latencies in processes (IR, investigations, etc.)
  - # of malicious actions prevented / recovered before harm done

# Insider Threat Control Testing Techniques

- Tabletops
  - Exercise stakeholder’s abilities to execute on policies / procedures and identify any critical gaps
- Penetration Testing
  - Exercise controls’ abilities to prevent / detect / respond to technically sophisticated attacks
- Advanced Techniques
  - Wallnau et. al – insert synthetic threat data into operational data sets, measure detective controls’ abilities to differentiate threat data from benign activity
  - Greitzer et. al – measure predictive models against known incident data

# REFINE AND REFRESH

# Insider Threats are Dynamic

- The threat landscape changes
  - Disruptive technologies
  - Organization-level events
    - Mergers, acquisitions, reductions in force, etc.
  - Current events
  - The workforce changes
- Your organization’s appetite for risk changes
- Stuff breaks
  - “Why isn’t that data in the SIEM anymore?”

# … So Your Insider Threat Control Set Must Be Dynamic

- Implement periodic:
  - Re-assessments of the highest priority insider threats to your organization's critical assets
  - Tests designed to measure the effectiveness of the deployed insider threat controls
  - Improvements to deployed controls based on testing and feedback from insider threat program stakeholders

# WRAP-UP

# Summary

- Insider threat control selection should be driven by an enterprise-wide effort to identify and prioritize the biggest threats to the organization’s mission-critical assets
- Insider threat control baselines should be informed by existing standards, and should leverage as much existing capability as possible
- Insider threat controls run the gamut of control types, control functions, and require input, operation, and feedback from across the organization
- There is overlap in the features and functionality of the main types of insider threat controls – fine line between defense-in-depth and buying the same thing twice

# Applying What You Have Learned Today

For immediate action:

- Identify if your organization has a prioritized list of its critical assets
- Map the threats insiders pose to those critical assets, and start to think about what controls are in place that mitigate those threats

Within 3 months:

- Establish an insider threat control baseline within your organization
- Enumerate the observables associated with the threat scenarios for which you have control coverage gaps
- Establish measures of effectiveness you can use to test proposed new controls

# QUESTIONS

# Presenter Contact Information

**Randy Trzeciak**

Director, CERT National Insider Threat Center

rft@cert.org

**Dan Costa**

Technical Solutions Team Lead, CERT National Insider Threat Center

dlcosta@cert.org