Building an Effective Insider Risk Management Program

Randall Trzeciak

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.

DM21-0744

About the Speaker

Randall Trzeciak

Director – National Insider Threat Center

Deputy Director – CERT Cyber Risk and Resilience Directorate

Program Director – CMU Heinz MS Information Security Policy & Management Program

Randy Trzeciak is Deputy Director CERT's Cyber Risk and Resilience Directorate and the Director of the CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute. The team's mission is to assist organizations in improving their security posture and incident response capability by researching technical threat areas; developing and conducting information security assessments; and providing information, solutions and training for preventing, detecting, and responding to illicit activity. Team members are domain experts in insider threat and incident response. Team capabilities include threat analysis and modeling; building and evaluating insider threat programs; development of insider threat controls, workshops, and exercises. Randy has over 30 years' experience in a wide-range of topics including: insider threat mitigation, risk management, cybersecurity, software engineering, project management, information security, and database design, development, and maintenance. In addition to his role with CERT, he also has a dual appointment as Program Director for the Masters of Science in Information Security Policy and Management (MSISPM) program and CERT professor at Carnegie Mellon's Heinz College, Graduate School of Information Systems and Management. Randy holds an MS in Management from the University of Maryland and a BS in Management Information Systems and a BA in Business Administration from Geneva College.

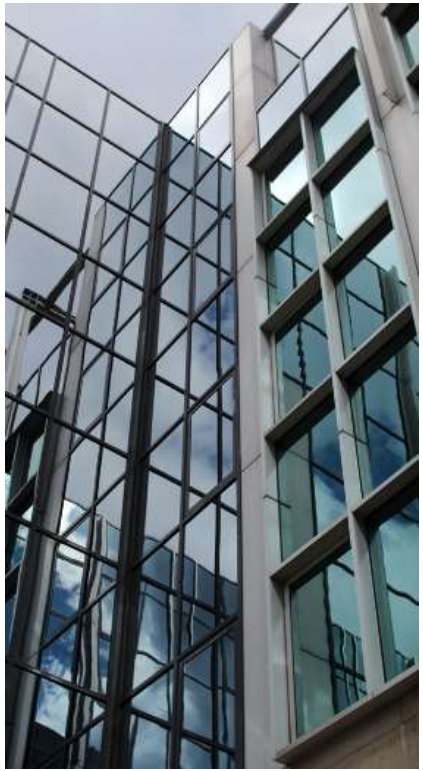
The CERT Insider Threat Center

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 threats

Action and Value: conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats



What / Who is an 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.

The Insider Threat

There is not one “type” of insider threat

Threat is to an organization’s critical assets

- People
- Information
- Technology
- Facilities

Based on the motive(s) of the insider

Impact is to Confidentiality, Availability, Integrity

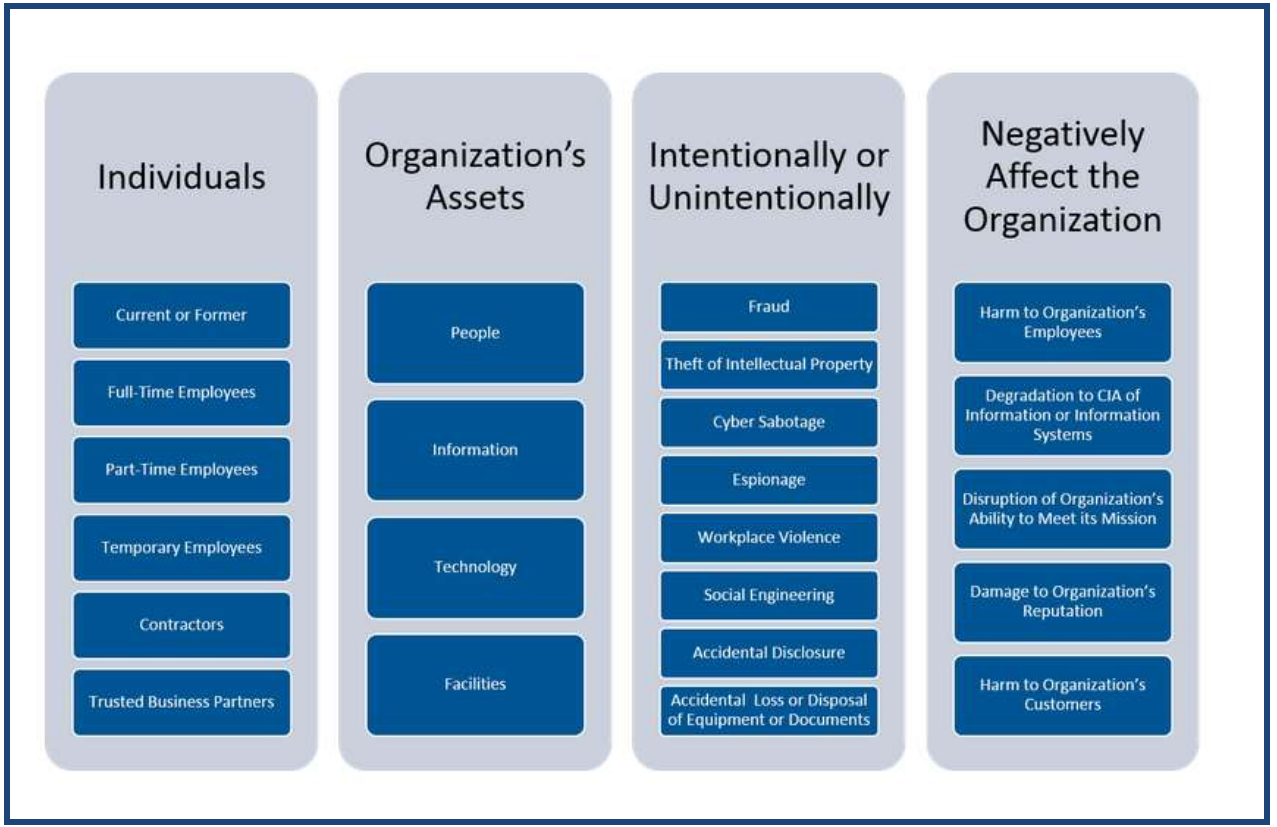
Cyber attack = Cyber Impact

Kinetic attack = Kinetic Impact

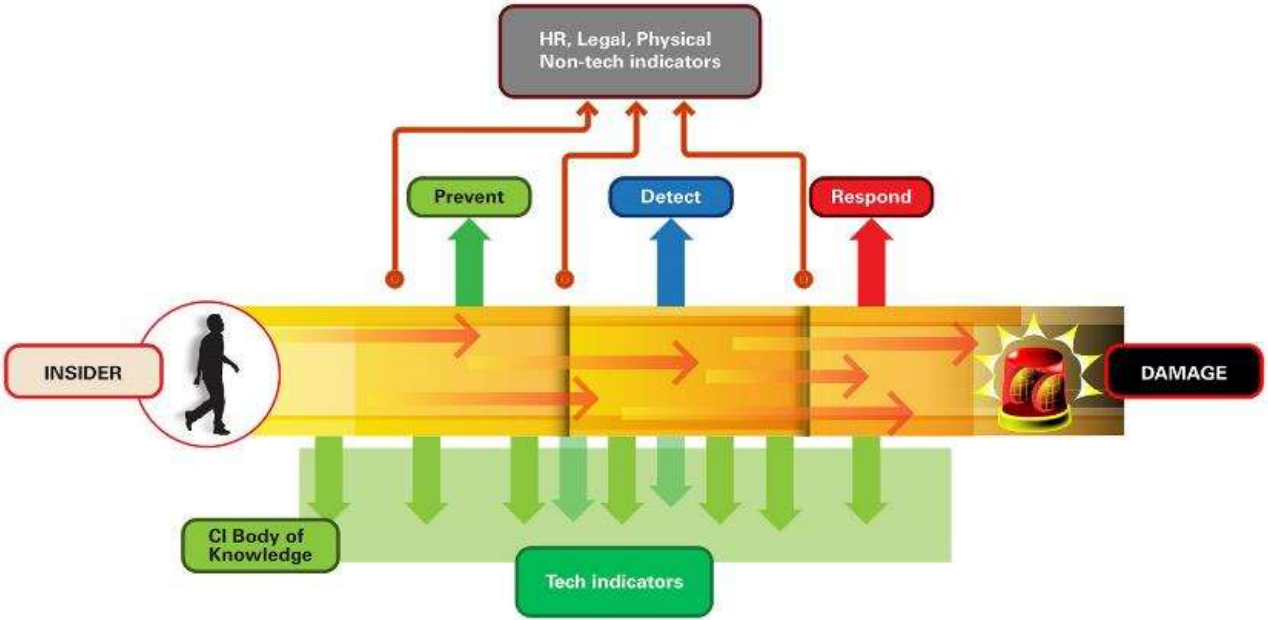
Cyber attack = Kinetic Impact

Kinetic attack = Cyber Impact

What / Who is an Insider Threat?



Goal for an Insider Risk Management Program



Is to reduce insider risks to critical assets to acceptable levels

https://insights.sei.cmu.edu/insider-threat/2020/01/maturing-your-insider-threat-program-into-a-n-insider-risk-management-program.html

Types of Insider Incidents

Types of Insider Activities - 1

Insider IT Sabotage

An insider's use of IT to direct specific harm at an organization or an individual

- Deletion of information
- Bringing down systems
- Website defacement to embarrass organization

Insider Theft of Intellectual Property

An insider's use of IT to steal intellectual property from the organization

- Proprietary engineering designs, scientific formulas, etc.
- Proprietary source code
- Confidential customer information
- Industrial Espionage and Trade Secrets

Types of Insider Activities - 2

Insider Fraud

An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud

- Payroll; Reimbursement

Theft and sale of confidential information

- SSN, PII, Credit Care Numbers, etc.

Modification of critical data for a fee

- Driver's license records; Criminal records

Insider National Security Espionage

The act of communicating, delivering or transmitting information pertaining to the national defense of the United States to any foreign government or faction, with intent or reason to believe that is to be used to the injury of the United States or to the advantage of a foreign nation

- Volunteers
- Recruited in Place
- Dispatched

Types of Insider Activities - 3

Insider Miscellaneous

Unauthorized disclosure (information insider believed should be in the public domain)

Providing address of a person to an acquaintance who physically harmed the individual

Accessing records of high-profile individuals

Non-Malicious:

Unintentional Insider Threat (UIT)

An insider whose actions or lack of action without malicious intent causes harm or the possibility of harm

Types of Insider Activities (Non-Malicious) - 4

UIT - Four Categories:

DISC - accidental disclosure (e.g., via the Internet)

- sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail

PHISHING/SOCIAL - malicious code (UIT-HACKing, malware/spyware)

- an outsider's electronic entry acquired through social engineering (e.g., phishing email attack, planted or unauthorized USB drive) and carried out via software, such as malware and spyware

PHYS - improper/accidental disposal of physical records

- lost, discarded, or stolen non-electronic records, such as paper documents

PORT - portable equipment no longer in possession

- lost, discarded, or stolen data storage device, such as a laptop, PDA, smart phone, portable memory device, CD, hard drive, or data tape

Summary of Insider Incidents

	IT Sabotage	Fraud	Theft of Intellectual Property
Current or former Employee?	Former	Current	Current (within 30 days of resignation)
Type of position	Technical (e.g., sys admins, programmers, DBAs)	Non-technical (e.g., data entry, customer service) or their managers	Technical (e.g., scientists, programmers, engineers) or sales
Gender	Male	Fairly equally split between male and female	Male
Target	Network, systems, or data	PII or Customer Information	IP (trade secrets) or Customer Information
Access Used	Unauthorized	Authorized	Authorized
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At Work

Building an Effective Insider Risk Management Program

Have a Long-Term Roadmap

Source: http://www.insaonline.org/InsiderThreat

Initial Planning

Building a Business Case for an InTP

- Use a risk management thought process
- Include:
  - the problem you are trying to solve
  - the scope and impact of the program
  - the approach to solving the problem (and why it is better than alternatives)
  - the possible positive outcomes of the program
  - the possible risks associated with the program
  - the possible risks associated with *NOT* doing the program

Extracted from Source: http://www.insaonline.org/InsiderThreat

Identify Your Starting Point

Get the right group of people together to start brainstorming and designing the framework and workflows.

Determine:

- what is already there but needs tweaks or improvements
- where the greatest gaps exist that will need to be addressed

Improve existing procedures or workflows for quick wins.

Save large gaps for long-term improvements.

Know the awareness level within your organization.

Know What's in Place

Component	Not Implemented	Partially Implemented	Fully Implemented	Not Applicable
Awareness of Insider Threat as a Problem		X		
Executive Management Support			X	
Organizational Participation	X			
Policies and Procedures	X			
Insider Threat Controls and Defenses		X		
Technical Data Sources Collected			X	
Behavioral Data Sources Collected	X			

Formalizing the InTP -1

A formalized InTP should have policies, procedures, and practices that define:

- the basic functions and services of the InTP
- the day-to-day actions and operations of the InTP team
- the corresponding actions of the investigative teams
- the tools used to perform daily operations

Formalizing the InTP -2

A formalized InTP should also have:

- defined processes for organizational employees to interact with the InTP
- mechanisms and channels for information sharing, communications, and coordination with other organizational components
- guidelines for information disclosure restrictions

Common Documents to Build an InTP

There are a core set of documents that most organizations need in order to formalize the InTP:

- Insider Threat Policy (*you will*)
- Insider Threat Charter (*you will what*)
- Concept of Operations (CONOPS) (*you will how*)
- Implementation Plan (*how you will get there*)
- Incident Response Plan (*what to do when something happens there*)
- Communications Plan (*who/how to tell what happened there*)

Run Everything Through Legal/Privacy

Before creating these documents:

- Work with legal counsel and privacy officers in the development of the InTP
- Make sure both groups have ongoing involvement with process/procedures involving investigations and dispositions of inquiries.
- Ensure that all InTP actions meet legal mandates and protect the rights and privacy of employees.

Compliance with Regulations or Standards

You may already have made progress on InTP requirements depending on your existing compliance requirements:

- NIST 800-53 – Security and Privacy Controls for Federal Information Systems
  and Organizations
  - Payment Card Industry (PCI) Data Security Standard (DSS)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Sarbanes-Oxley Act (SOX)
  - Gramm-Leach-Bliley Act (GLBA)
  - State Data Breach Notification Laws
  - Breach Notification Regulations for Federal Agencies
  - Cybersecurity Maturity Model Certification (CMMC)

Where InTP's Have Succeeded

- Connecting the dots
- Technical detection of blatant policy violations
- Identifying broken business processes

Where InTP's Are Struggling

- Measures of Effectiveness / ROI
- Scoping
- Change management
- Proactive responses to the conditions that precede harmful acts

Where Insider Threat Programs Traditionally Focus

Engineering		
ADM	Asset Definition and Management	
CTRL	Controls Management	★
RRD	Resilience Requirements Development	
RRM	Resilience Requirements Management	
RTSE	Resilient Technical Solution Engineering	
SC	Service Continuity	

Enterprise Management		
COMM	Communications	★
COMP	Compliance	
EF	Enterprise Focus	★
FRM	Financial Resource Management	★
HRM	Human Resource Management	★
OTA	Organizational Training and Awareness	★
RISK	Risk Management	

Operations		
AM	Access Management	★
EC	Environmental Control	
EXD	External Dependencies Management	
ID	Identity Management	★
IMC	Incident Management and Control	★
KIM	Knowledge and Information Management	
PM	People Management	
TM	Technology Management	★
VAR	Vulnerability Analysis and Resolution	★

Process Management		
MA	Measurement and Analysis	★
MON	Monitoring	★
OPD	Organizational Process Definition	
OPF	Organizational Process Focus	

Where Insider Threat Programs Need To Expand

Engineering		
ADM	Asset Definition and Management	★
CTRL	Controls Management	
RRD	Resilience Requirements Development	★
RRM	Resilience Requirements Management	★
RTSE	Resilient Technical Solution Engineering	★
SC	Service Continuity	★

Enterprise Management		
COMM	Communications	
COMP	Compliance	★
EF	Enterprise Focus	
FRM	Financial Resource Management	
HRM	Human Resource Management	
OTA	Organizational Training and Awareness	
RISK	Risk Management	★

Operations		
AM	Access Management	
EC	Environmental Control	★
EXD	External Dependencies Management	★
ID	Identity Management	
IMC	Incident Management and Control	
KIM	Knowledge and Information Management	★
PM	People Management	★
TM	Technology Management	
VAR	Vulnerability Analysis and Resolution	

Process Management		
MA	Measurement and Analysis	
MON	Monitoring	
OPD	Organizational Process Definition	★
OPF	Organizational Process Focus	★

Key Requirements for Program Success

To achieve success requires:

- commitment and sponsorship from all levels of management
- acceptance and buy-in across the enterprise
- recognizing what's already in place in your enterprise
- a long-term vision for the program
- a persistent planning & implementation/working group
- a project plan to track goals and milestones
- iterative short-term tasking and pilot activities

Insider Risk Management Program - Summary

The Insider Risk Management Program of the future is an integrated, proactive, risk-based mission enabler that makes its organization operationally resilient against insider threats.

This future state can be realized by:

- expanding relationships with traditionally under-represented insider threat program stakeholders
- clearly articulating program goals and risk appetite
- placing an emphasis on process institutionalization, yielding more stable processes that produce consistent results over time that are retained during times of stress

Insider Threat Resources

Recommended Best Practices for Insider Threat Mitigation

1 - Know and protect your critical assets.	12 - Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
2 - Develop a formalized insider threat program.	13 - Monitor and control remote access from all endpoints, including mobile devices.
3 - Clearly document and consistently enforce policies and controls.	14 - Establish a baseline of normal behavior for both networks and employees
4 - Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	15 - Enforce separation of duties and least privilege.
5 - Anticipate and manage negative issues in the work environment.	16 - Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
6 - Consider threats from insiders and business partners in enterprise-wide risk assessments.	17 - Institutionalize system change controls.
7 - Be especially vigilant regarding social media.	18 - Implement secure backup and recovery processes.
8 - Structure management and tasks to minimize unintentional insider stress and mistakes.	19 - Close the doors to unauthorized data exfiltration.
9 - Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	20 - Develop a comprehensive employee termination procedure.
10 - Implement strict password and account management policies and practices.	21 - Adopt positive incentives to align the workforce with the organization.
11 - Institute stringent access controls and monitoring policies on privileged users.	

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=540644 or search “cert common sense guide insider threat”

Featured Research from the CERT National Insider Threat Center – 1

The Common Sense Guide to Mitigating Insider Threats, Sixth Edition – a collection of 21 best practices for insider threat mitigation, complete with case studies and statistics

- https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644

Balancing Organizational Incentives to Counter Insider Threat – a study on how positive incentives can complement traditional security practices to provide a better balance for organizations' insider threat programs

- https://ieeexplore.ieee.org/abstract/document/8424655

Featured Research from the CERT National Insider Threat Center – 2

Navigating the Insider Threat Tool Landscape: Low Cost Technical Solutions to Jump-Start an Insider Threat Program – an exploration of the types of tools that organizations can use to prevent, detect, and respond to multiples types of insider threats

- https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_521706.pdf

Insider Threats Across Industry Sectors – a multi-part blog series that contains the most up-to-date statistics from our database on sector-specific insider threats

- https://insights.sei.cmu.edu/insider-threat/2018/10/insider-threat-incident-analysis-by-sector-part-1-of-9.html

Featured Research from the CERT National Insider Threat Center – 3

Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls

- https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=446367

Analytic Approaches to Detect Insider Threats

- https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=451065

Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments

- https://web.archive.org/web/20170122065908/http:/resources.sei.cmu.edu/library/asset-view.cfm?assetid=48668

Featured Research from the CERT National Insider Threat Center – 4

Workplace Violence & IT Sabotage: Two Sides of the Same Coin?

- https://resources.sei.cmu.edu/asset_files/Presentation/2016_017_001_474306.pdf

An Insider Threat Indicator Ontology

- https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=454613

Training from the CERT National Insider Threat Center

Our insider threat program manager, vulnerability assessor, and program evaluator certificate programs and insider threat analyst training courses are now available in live-online delivery formats!

For more information, please visit
www.sei.cmu.edu/education-outreach/courses/index.cfm

For More Information

Over 125 publications are available at our website, www.cert.org/insider-threat

We're updating our blog (www.insights.sei.cmu.edu/insider-threat) weekly this month

Any other questions or comments? Email us at insider-threat-feedback@cert.org.

Point of Contact

Director – National Insider Threat Center

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/