

Keeping Up with the Joneses: How Does Your Insider Threat Program Stack Up?

SESSION ID: HUM-W02

Dawn M. Cappelli

Director, Insider Risk Management
Rockwell Automation
@DawnCappelli

Randall F. Trzeciak

Technical Manager, Insider Threat Center at CERT
Software Engineering Institute
Carnegie Mellon University
rft@cert.org



Notices

Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by DHS; U.S. Secret Service; CMU CyLab under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0000857

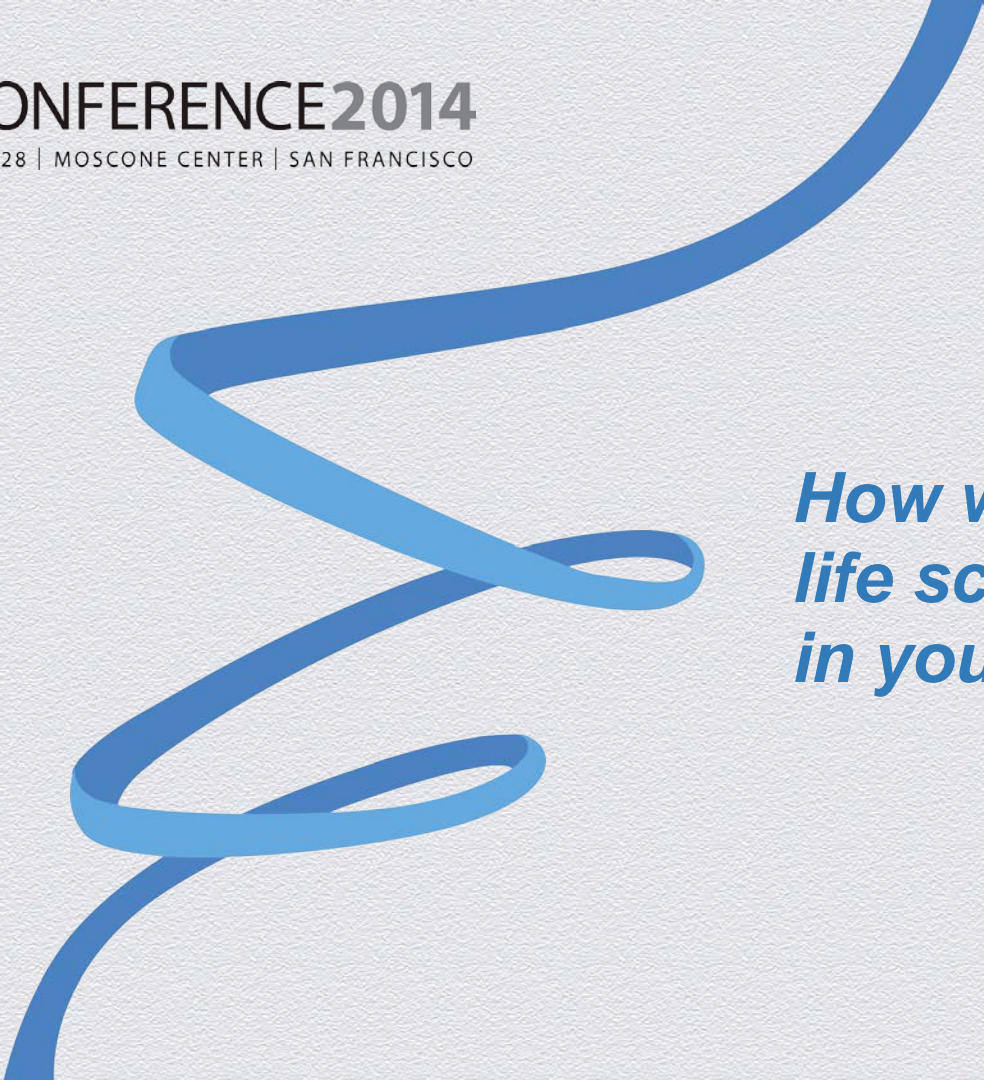


Software Engineering Institute
Carnegie Mellon University



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



How would this real-life scenario play out in your organization?

Could this happen to you??

A director and 4 accomplices downloaded information valued at over \$100M from an energy research and development facility to take with them to a competing organization.

Insider signed NDA and "no-solicitation" clause

Accepted offer from competitor

Downloaded tens of thousands of customer files and confidential information to external storage devices

1 week later left the company

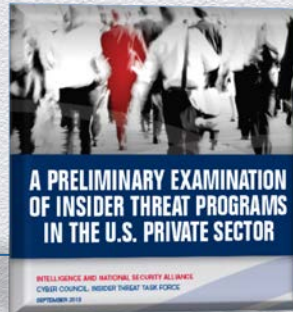
Recruited 4 other employees

They attached external storage devices and downloaded more IP, then left the company

One of them forwarded e-mail from the company to his personal e-mail after he left

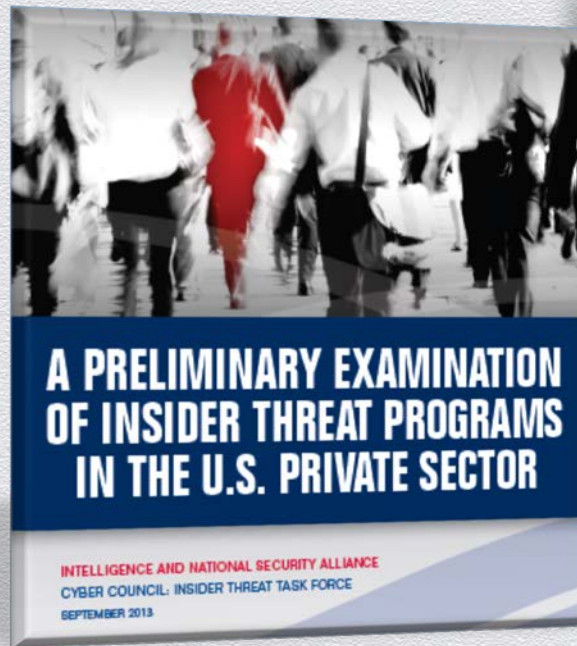
Purpose of this Presentation

- ◆ Present the state of over 90 insider threat programs in the U.S. private sector; provide guidance on how to build a program
- ◆ Why: So you can benchmark your organization, and build or enhance a program in your organization
- ◆ How: Based on our collective experience working on insider threat since 2001, as well as our participation on the following projects:



INSA Insider Threat Task Force

- ◆ *A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector*
- ◆ Intelligence and National Security Alliance (INSA) Insider Threat Task Force, September 2012
- ◆ Provides preliminary benchmark of private sector insider threat programs



INSA Insider Threat Task Force Members



- ◆ **Dawn Cappelli**, CERT Insider Threat Center of the SEI at Carnegie Mellon University (Lead)
- ◆ **Zalmai Azmi**, CACI International, Inc.
- ◆ **Steve Coppinger**, CACI International, Inc.
- ◆ **Christopher King**, CERT Division of the SEI at Carnegie Mellon University
- ◆ **Kevin Lawrence**, Accenture
- ◆ **Terry Monahan**, Lockheed Martin Corporation
- ◆ **Shannon Peterson**, Accenture
- ◆ **James Robinson**, Websense, Inc.
- ◆ **Robin Ruefle**, CERT Division of the SEI at Carnegie Mellon University
- ◆ **Jim Simon**, Intelligence Enterprises LLC
- ◆ **Roccie Soscia**, Lockheed Martin Corporation
- ◆ **Douglas Thomas**, Lockheed Martin Corporation
- ◆ **Randall Trzeciak**, CERT Insider Threat Center of the SEI at Carnegie Mellon University



Process – INSA Insider Threat Task Force



- ◆ Interviewed 13 companies - mostly large, national or global:
 - ◆ IT services and consulting firms
 - ◆ Financial institutions
 - ◆ Technology vendors
 - ◆ Aerospace and defense organizations
 - ◆ Research institutions
 - ◆ Data analytics providers
- ◆ Conducted online survey of 71 organizations from the financial sector

Major Findings



- ◆ Just over half of the organizations interviewed and 25% in the financial sector have an insider threat program; many are technology-focused
- ◆ A program cannot succeed without senior leadership support
- ◆ Only 5 companies interviewed and less than half in the financial sector have an insider threat incident management plan
- ◆ Over half of the organizations have an awareness program related to insider threat

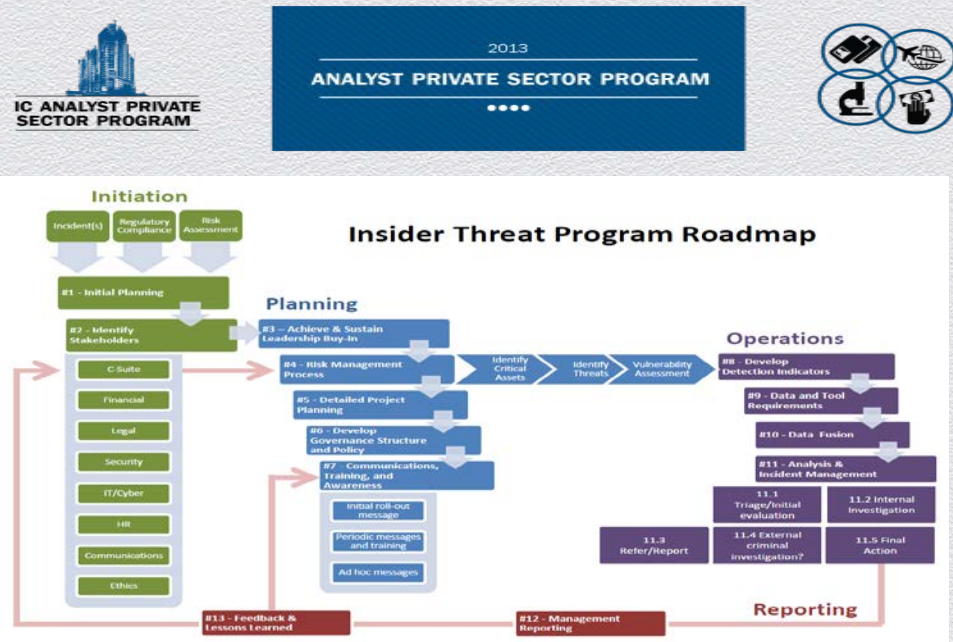
Major Findings - 2

An effective insider threat program requires the entire organization working together:

Information Security	Information Technology
Human Resources	Public Relations
General Counsel	Ethics
Counterintelligence	Executive Management

DHS / ODNI Intelligence Community Analyst-Private Sector Partnership Program

- ◆ *Identifying & Countering Insider Threats Study*
- ◆ Intelligence Community (IC) Analyst-Private Sector Partnership Program
- ◆ Sponsored by the Department of Homeland Security's Office of Intelligence and Analysis (DHS/I&A), on behalf of the Director of National Intelligence (ODNI)



IC Analyst-Private Sector Partnership - Insider Threat Team Members



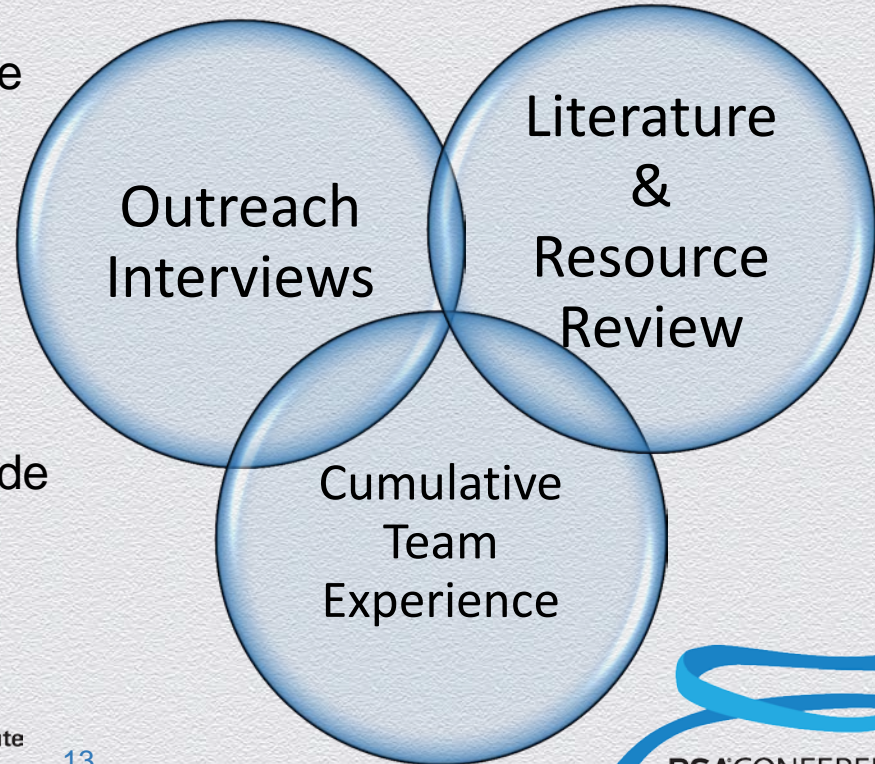
- ◆ **Moon-Hui Choi**, Office of the National Counterintelligence Executive & FBI (Team Champion)
- ◆ **Charlie Meyer**, Office of Personnel Management – Federal Investigative Services
- ◆ **Dan Donohue**, Caterpillar, Inc.
- ◆ **Dawn Cappelli**, Rockwell Automation & Carnegie Mellon/SEI/CERT
- ◆ **Jay Boggs**, PricewaterhouseCoopers
- ◆ **Jeffrey Taylor**, DHS / I&A
- ◆ **Jordan Greene**, FBI
- ◆ **Randy Trzeciak**, Carnegie Mellon/SEI/CERT
- ◆ **Ray Weldon**, Defense Security Services
- ◆ **Stephen Thompson**, Leidos

IC Analyst-Private Sector Partnership Insider Threat Study



◆ Goals:

- ◆ Develop roadmap and resource guide for insider threat practitioners
- ◆ Share highlights and lessons learned from mature private sector programs
- ◆ Identify knowledge gaps to guide research & inform US government outreach efforts

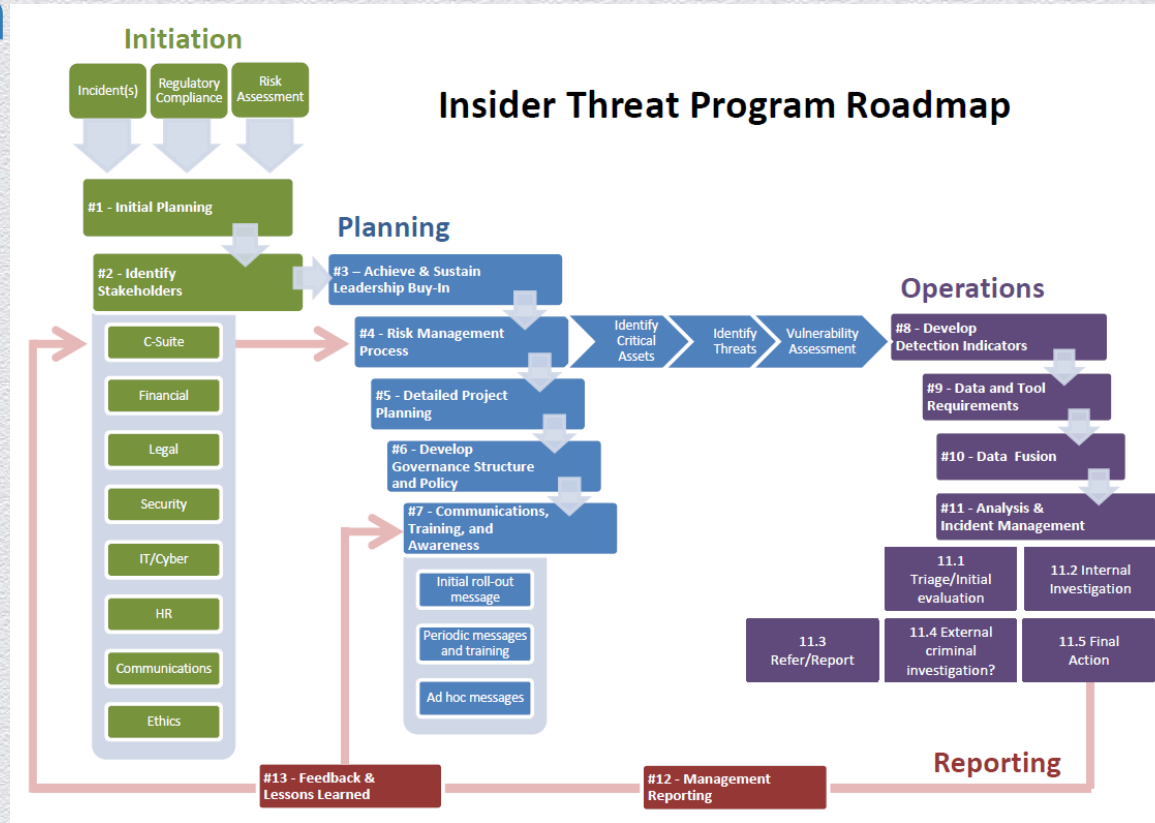


Components of Robust Insider Threat Programs



- ◆ The team interviewed six companies representing critical manufacturing, defense, financial, telecommunications sectors and two trade groups that support small and mid-sized businesses
- ◆ Highlights follow...

Essential Elements of an Insider Threat Program



Initiation of an Insider Threat Program



Why are all of those organizations necessary?

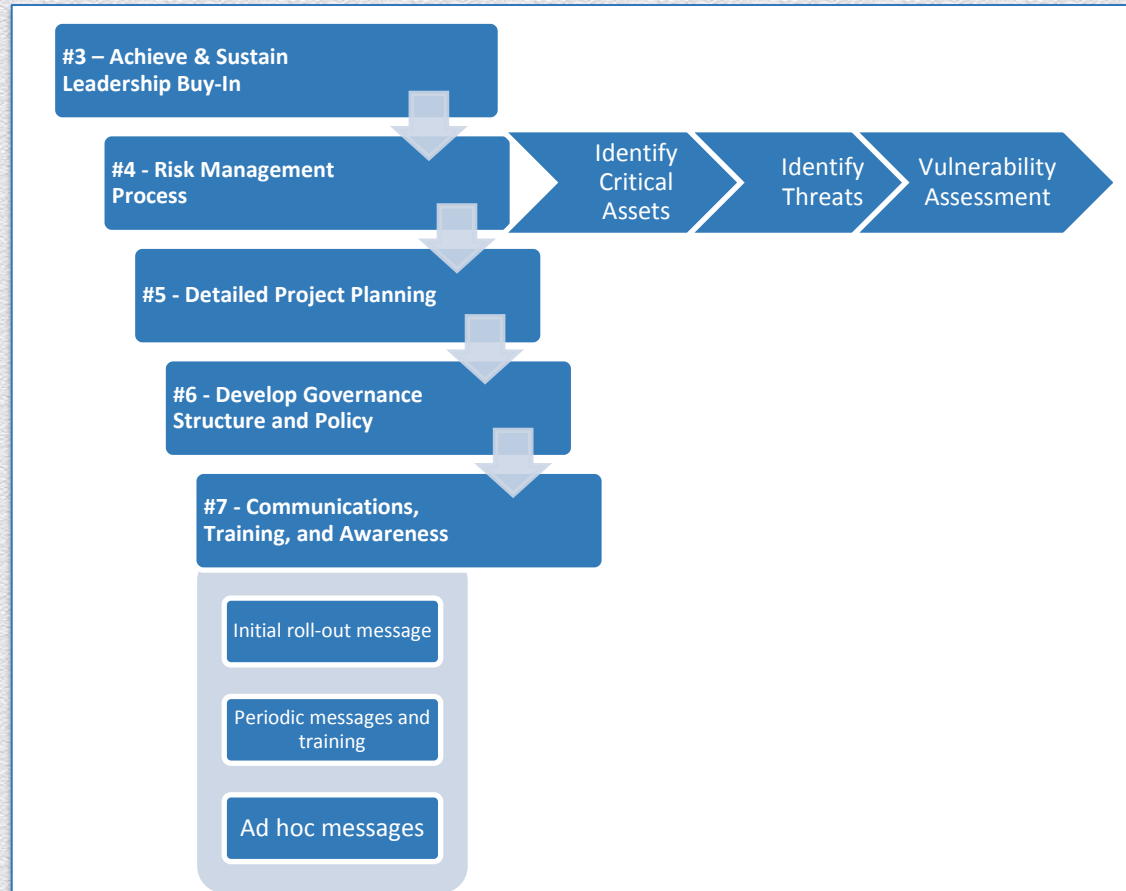
TRUE STORY:

A computer programmer at a hospital, before resigning, deployed a logic bomb, which detonated 2 months after departure...

The insider worked on a computer based training program for hospital employees



Planning



Why is the Risk Management Process Important?

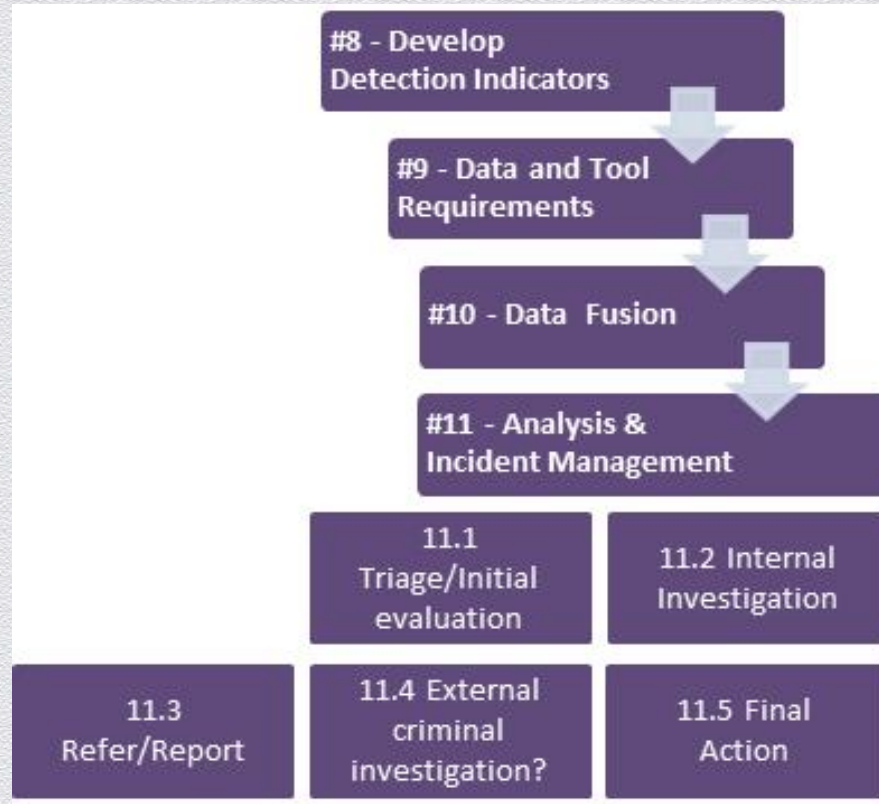
TRUE STORY:

A contractor at a government organization falsified information to obtain legal documents for illegal immigrants...

Over a 3 month period he altered personal information in a database, charging between \$1,000 and \$4,000 per person.



Operations



Why are well planned operations essential?

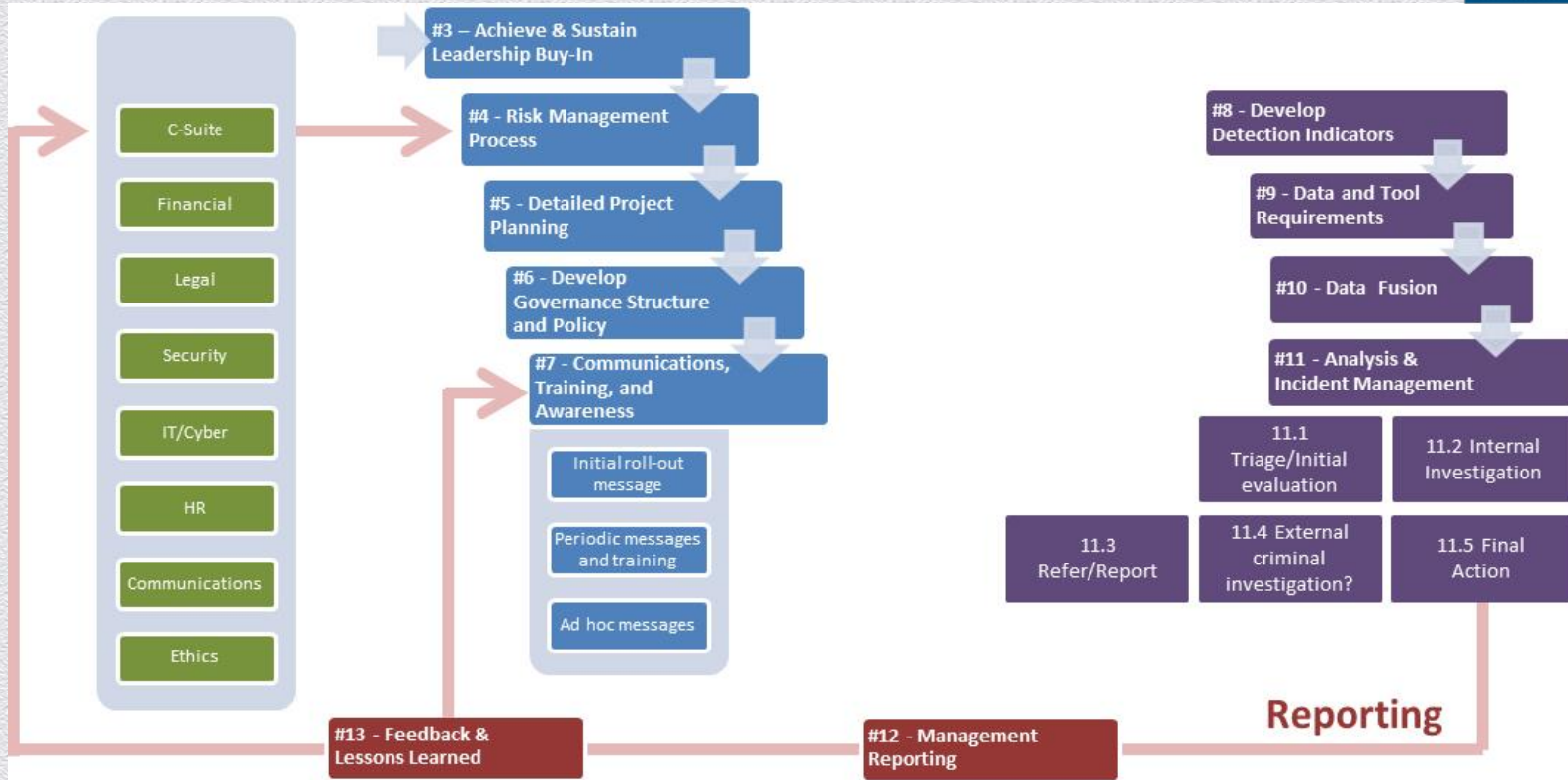
TRUE STORY:

A software engineer at a U.S. software development company sold stolen source code to the highest bidder, outside the U.S....

One day after signing a contract with the foreign organization and submitting his resignation, the insider transferred the source code to the bidder.



Reporting



Similar to INSA Findings



- ◆ Robust insider threat programs are both human and technology-focused
- ◆ Successful programs have strong senior leadership support
- ◆ Strong programs have a proactive insider threat incident management plan and work closely with their Legal department
- ◆ These organizations have formal insider threat communications plans

Similar to INSA Findings - 2



◆ Effective programs involve:


◆ Information Security	◆ Information Technology
◆ Human Resources	◆ Public Relations
◆ General Counsel	◆ Ethics
◆ Counterintelligence	◆ Executive Management

Highlights from Robust Programs




- ◆ Big losses can drive strategic change
- ◆ Leverage existing resources
- ◆ Pilot and full-scale approaches are both viable
- ◆ Employees themselves are stakeholders
- ◆ Real world examples resonate in obtaining leadership support
- ◆ Asset identification and prioritization is key
- ◆ Prioritize threats into a high risk group
- ◆ Someone needs to “watch the watchers”
- ◆ Expanding outside the U.S. is a challenge

Website Resource Guide



2013
ANALYST PRIVATE SECTOR PROGRAM
....



Identifying and Countering Insider Threats

[Home](#) | [Insider Threat Roadmap](#) | [Terms of Reference](#) | [Domain Gaps](#) | [Insider Threat Resources](#) | [Contact Us](#)

Background: The IC Analyst-Private Sector Partnership Program, sponsored by the Department of Homeland Security's Office of Intelligence and Analysis, on behalf of the Director of National Intelligence, facilitates collaborative partnerships between members of the private sector and teams of experienced Intelligence Community (IC) analysts. The areas of focus selected for this year's program, based on intelligence priorities, were: Energy Security, Money Laundering, Identifying and Countering Insider Threats, Air Domain Awareness, Identity Theft and Illicit Activity, Game Changing Biotechnology. Our group, based on individuals experience and expertise, was selected to work on the Insider Threat topic.

Deliverable: Our group set out to develop a resource that provides the essential elements required to initiate an insider threat program. To accomplish this, our group relied on several sources including: personal experience in the public and private sectors, interviews with industry experts, overviews of insider threat programs and countless discussions among team members. The 13 essential elements were developed to follow a timeline from the first step (Initial Planning) to the last (Feedback/ Lessons Learned). In practice the processes required are iterative and will require coordination and communication throughout.

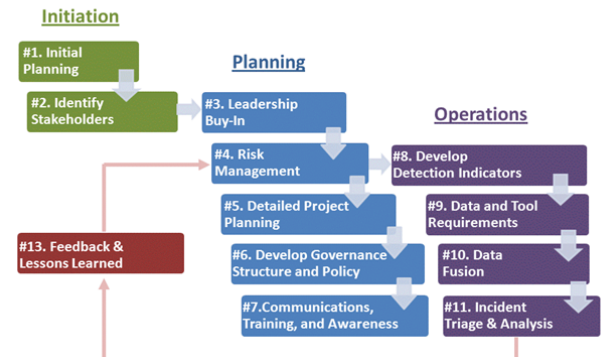
1). Initial Planning

This first step includes the development of an initial strategic plan, scope, high-level requirements (money, people, equipment) and the timeline/ schedule.

Outreach Highlight:
Pilot vs. Full Scale- One company decided to pilot the program and successfully used suspicious activity they identified as justification for further investment. A second company went for full program investment up front. While both approaches worked for their respective programs, an organization's approach is influenced by the availability of resources and their adversity to risk.

Resources:
[Project Initiation Document](#) (www.Mindtools.com)
[Common Sense Guide to Mitigating Insider Threats](#) (www.SEI.CMU.edu)

Insider Threat Program Roadmap (Click image for detailed version)



```
graph TD
    subgraph Initiation
        I1[#1. Initial Planning] --> I2[#2. Identify Stakeholders]
    end
    subgraph Planning
        P3[#3. Leadership Buy-In] --> P4[#4. Risk Management]
        P4 --> P5[#5. Detailed Project Planning]
        P5 --> P6[#6. Develop Governance Structure and Policy]
        P6 --> P7[#7. Communications, Training, and Awareness]
    end
    subgraph Operations
        O8[#8. Develop Detection Indicators] --> O9[#9. Data and Tool Requirements]
        O9 --> O10[#10. Data Fusion]
        O10 --> O11[#11. Incident Triage & Analysis]
    end
    F13[#13. Feedback & Lessons Learned] --> I1
    F13 --> P3
    F13 --> O8
```

7). Communication, Training & Awareness

The importance of employee awareness and training cannot be underestimated. Employees need to understand the intent of the program and the role they play towards achieving program goals.

Outreach Highlight:
Several companies highlighted the importance of corporate communications. One CSO noted that "an internal corporate communications strategy is absolutely vital." The CSO stated that you can't afford an ill thought-out comms plan as it will destroy employee support for the program just as much as "false positives."

Resources:
[Developing a Successful Governance Strategy - Chpt. 4](#) (www.isaca.org)
[Traveling Overseas with Mobile Phones, Laptops, PDAs, and Other Electronic Devices](#) (www.NCIX.gov)



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

<http://www.insaonline.org/InsiderThreat>



Final Takeaway: Benchmarks

What should you do?

According to studies of the U.S. private sector, you should consider these benchmarks:

1. Overall, over half of the organizations interviewed and 25% in the financial sector have an insider threat program.

Recommendation: Obtain leadership buy-in for an insider threat program.

2. Organizations with effective insider threat programs stress that the entire organization needs to work together.

Recommendation: Create an insider threat team consisting of representatives from across the company.

What should you do? (2)

3. Many programs are technology-focused, using existing tools.

Recommendation: Use existing tools to prevent / detect malicious insider activity.

4. Over half of the organizations have an insider threat awareness program.

Recommendation: Include insider threats in existing security awareness and ethics training.

***After implementing those 4 recommendations, you will
“Keep up with the Joneses”.***

Maturing Your Program

Companies with mature, robust insider threat programs recommended the following:

1. Develop a formal governance structure for your program.
2. Develop a detailed communications plan.
3. Take the time to identify critical assets and use a risk management approach to protect those assets.
4. Implement insider threat technology for automated data fusion and analysis.
5. Develop an insider incident management process.

Summary

- ◆ Quote from a CEO in the U.S. private sector:
“There is not a technological silver bullet in a people-centric business like ours.”
- ◆ Current state of U.S. private sector insider threat programs appears to be immature compared to programs focused on external cyber threats
- ◆ Likelihood of potential regulation is growing in the U.S. – industry leaders are paying attention and getting ahead of the game!
- ◆ Insider threat experts are beginning to build formal collaboration mechanisms to work together to raise the bar for Insider Threat Programs in the U.S. private sector – JOIN US!!

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Discussion /
Questions

Contact Information

Dawn Cappelli

Director, Insider Risk Management
Rockwell Automation
+1 (414) 323-0404
dmcappelli@ra.rockwell.com

Randall Trzeciak

Technical Manager, Insider Threat
Center at CERT
+1 (412) 268-7040
rft@cert.org