Insider Threat with a CI Focus
The Road to a Successful Program

Trevor Odell
Director, IT Security & Assurance

May 1, 2016
...The more they stay the same

• When did someone know something?
• The person was too big / too important / too valuable
• Who did they tell?
• What was the climate for telling?
• What’s the trust in leadership?
• How do we handle poor performers?
• What’s the professionalism of the HR and Security teams?
• Is there a communication barrier at the Manager / Supervisor level?

There remains a fundamental issue regardless of the business:

TRUST and COMMUNICATION

What do I Know? Who else Needs to Know? Have I told them?
“If only we knew…” but we do!

Our ability to detect, and respond, is limited only by our visibility

• Employees can be educated as part of Security Awareness Training

  [There is a chance that an insider threat may be created by any] person who is tuned out, angry, apathetic, better than the rest, doesn’t have feeling for his or her teammates and countrymen, is convinced that “If I created it I can do with it what I want”, and is able to say, with conviction “the rules don’t apply to me”

  [Our adversaries look to compromise] someone who NEEDS money, who’s life is a train wreck, or who might have ties with or sympathy for another country. Then if that person tends to lose control because of alcohol or could be blackmailed because of drugs we should be able to turn up the pressure.

  [Tell someone who can follow up if] you notice someone’s behavior changing significantly for the worse - obsessing over perceived slights, making overt threats, expressing thoughts that make no sense, becoming verbally abusive, taking unnecessary risks, or significantly changing appearance or behavior (not a new haircut, unless it was a do-it-yourself job accompanied by a sudden lack of concern for personal hygiene)

• These and other potential indicators are known by the business functions:
  • WARN notice recipients as well as those potentially impacted by a RIF
  • HR Records and security data, manager concerns, and staff complaints
  • Resistance to share information due to concerns of sensitivity, privilege, unintended release, and resulting conclusions
Program Elements

- Suspicious Activity Reports
- Foreign Visitor Checks & Visitor Control
- SAP/SCI Access Process
- Security Clearance & Adverse Reporting
- Commercial Background Investigations
- Government Agency Briefings & DSS Technology Trend Reports
- Terminating Employment Controls
- Suspicious Network/Email Activity
- Personnel Trends & Behavioral Analysis
- Physical Security/Parameter Controls
- Foreign Travel Briefing/Debriefings
- Social Networking Training & Monitoring *
- Classified Network Controls
- Liaison & Partnerships

Information Assurance
Personnel Security
Insider Threat Awareness
Government Liaison

* Selected use during investigations

Source: ASIS International
NI SPOM Program Requirements/Options

Insider Threat Program [1-202]

Contractors must establish an Insider Threat Program to Gather, Integrate & Report relevant information indicative of a Potential or Actual insider threat.

Individual Facility Program

Must have an Insider Threat Program Senior Official (ITPSO) who is:

- US Citizen
- Cleared in connection with each (or all) FCL
  - Can be the FSO
  - If not FSO, then FSO must be an “integral member” of the program

Corporate Program

Must have an Insider Threat Program Senior Official (ITPSO) who is:

- US Citizen
- Cleared in connection with each (or all) FCL
- Designated as the ITPSO by each Legal Entity (if more than one)
More Requirements

**Reporting Requirements**  [1-300]
You must report events that:

- Impact the status of the FCL
- Impact the status of an Employee’s PCL
- May indicate the employee poses an Insider Threat
- Affect Proper Safeguarding of Classified Information, or indicate that classified information has been lost or stolen

**Training Requirements**  [3-103]
Insider Threat Program Personnel (Including the Senior Official) must be trained in:

- CI and Security Fundamentals, including applicable Legal issues
- Procedures for conducting insider threat response actions
- Applicable Laws and Regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information
Insider Threat Program Overview

Program stood up in May 2013

- Part of an overall corporate effort
- Mission is the detection, deterrence and defeat of insider threats
  - Accomplished via automated and manual monitoring, analysis, and reporting
- Leverages our existing Counterintelligence Program
- Under Continual Improvement

Current Data Sources Include:

- Network Data Loss Prevention
- Host Data Loss Prevention
- System Logs
- Custom E-mail Filters (Inbound and Outbound)
- HR & Ethics Data
- Manager/Supervisor and Employee/Co-worker Reporting
- Ethics Hotline (Anonymous reporting)
Integrated Program Design

C-Suite Supported
Government Mandate
Transparency in Actions

Cross Functional Support
IT Participation

Use what you Have
Build what you Don’t Have
Invest where Needed

Process & Policy Driven
Tools are Important
Communicate all Decisions
Our Approach

Build a Cross Functional Strategic Team – at the C-Suite Level

- Build a Cross Functional Tactical Team
  - IT, HR, Legal, Comms, Procurement/Contracts, Security and Ethics along with Key Senior and Sector Executives

Understand where risk exists and how to measure it

- People, Process, Suppliers, Competitors, Foreign Nation States, Systems

Understand Employee & Contractor Communication Patterns

- Customers, Partners, Suppliers
  - Leverage what Employees know about Their Environments!

Balance Employee Needs with Company Needs

- Mandatory Government & Customer Requirements
  - Business Operations

Evaluate what you already have – that you can use to support the effort
Insider Threat Operations (ITROPS) escalates suspected/potential threats to IT Security & Assurance (ITSA) for evaluation. ITSA performs a Risk Analysis, advises the Sector Security Leadership and recommends additional monitoring or formal investigation.
Motivations, Behaviors, Rationale & Actions Taken

- Intentional
- Inadvertent
- Negligent
- Indifferent
- Not Applicable

- Policy Violation
- Disgruntled / Disaffected
- Behavioral Issue
- Performance Issue
- Self Focused
- Disregard for Authority

- Mental Illness
- Substance Abuse

- Anti-US Sentiment
- Terrorist Affiliation
- Military Espionage
- Economic Espionage
- Religious Extremism
- Social Activism

- WARN Notice Recipient
- Career Change
- New Hire
- Personal Financial Gain
- Financial Distress
- Coercion
- Blackmail

- System Detected
- Employee Reported
- Manager Reported
- Customer Reported
- 3rd Party Reported
- Not Discernable

- Economic Espionage
- Suspected FIS Activity
- Theft
- Destruction of Property
- Pending RIF Recipient
- Contractor
- Manager Directed
- Customer Directed
- Program Directed
- Excessive Foreign TVL
- Alcohol/Drug Abuse
- Unreported Affluence
- Unreported Foreign Affiliation/Contacts

- Bomb Threat
- Active Shooter
- Dangerous Material Release

- No Action Taken
- Escalated to Authorities
- Re-Education

© 2016 BAE Systems
Taxonomy

Before you can effectively report on incidents you must have a Taxonomy to describe them.

Initial Observations
- Criticality
  - Low, Medium, High, Critical
- Source
  - System Tools, SOC, Employee, Manager, Customer, External Party, Unknown, Other
- Content/Activity
  - Immediate Threat, Policy Violation, Data Release, Data Mishandling, System Abuse, Unauthorized Access, Work / Performance Issue, Behavioral Issue, Other

Case Closure
- Type
  - Intentional, Inadvertent, Negligence, Indifference, Not Applicable
- Motivation / Rationale
  - Espionage, Ideology, Personal Gain, Malice, Workforce Reduction, Directed Activity, Anti-Government Sentiment
- Outcome / Action
  - Employee / Contractor – Educated, Disciplined, Terminated, Escalated; No Action Taken
- Escalated / Reported To
  - Customer, Government, Law Enforcement, Partner, Supplier, Vendor, HR, Ethics, Management
- Triggers / Indicators
## Special Monitoring

<table>
<thead>
<tr>
<th>Tier</th>
<th>Criteria</th>
<th>Approval</th>
<th>IT Security Action</th>
<th>Data Source</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>New hires within first 90 days of employment; employees identified for RIF (include entire decisional unit); employees given WARN notice; employees on major program at risk; voluntary resignations.</td>
<td>No specific approval needed for each instance of monitoring done in the ordinary course of business.</td>
<td>Increase risk score factor for automated anomaly detection through Securonix. Escalate identified possible threats to HR VP and Sector Chief Counsel (SVP HR and General Counsel for HQ)</td>
<td>Spreadsheet sent from HR to IT Security on daily or weekly basis (underlying data obtained from Sector HR). (Automation in 2016)</td>
<td>90 days with an option to renew for additional periods as necessary. Renewal must be approved by HR VP in consultation with Sector Chief Counsel (SVP HR and General Counsel for HQ)</td>
</tr>
<tr>
<td>2</td>
<td>Investigations; request made by manager, HR BP, ethics officer, or FSO in response to behavioral indicators such as: ethics complaint, IT traffic irregularities; office conflict; substance abuse; reckless financial behavior; or unexplained affluence.</td>
<td>HR VP in consultation with Sector Chief Counsel. (Inc. approval by SVP HR and General Counsel) Notification to: VP Security; VP HR; Inc. Ethics; Inc. Assoc. Gen. Counsel Employment</td>
<td>Tier 1 IT Security Action and: (a) content collection and the use of controls to block certain usage of Company IT Assets; and (b) additional forensic analysis of data and Company IT Assets as necessary and approved.</td>
<td>Specific request from manager, HR BP, ethics officer, or FSO. Ethics will key information into their Tracking DB</td>
<td>15 days with an option to renew for additional period(s) as necessary. Renewal must be approved by HR VP in consultation with Sector Chief Counsel (SVP HR and General Counsel for HQ)</td>
</tr>
</tbody>
</table>
Insider Threat communications

- All-employee email message from VP Security
- E-mail message to people managers with PPT slide for re-use
- Drum beat of Intranet articles and image banners
  - What’s too much of a good thing? - On social media, the answer depends
  - Personal information is everywhere — and so are people who want to steal it
  - Potential security threats are everywhere - Could you be among them?
  - When something just isn’t right, you can tell
- Related all-employee messages and Intranet stories
  - OPM announces steps to protect federal workers and others from cyber threats, establishes incident resource center
  - Spear-phishing targets your online accounts
  - OPM issues notification letters to personnel affected by data breaches
- Supporting digital signage and flyers for Intranet stories
The credible threats are needles in a haystack of events

- System Log Events (Automated)
- System Generates Alerts (Automated) and Applies Custom Algorithms
- Analysts Triage Potential Threats and Escalate to IT Ops Director
- IT Ops Director Analyzes Threat, Reviews/Changes Risk Assessment and Escalates to Sector Security VP's
Keys to a Successful Program

• Use automation appropriately and effectively
  • It is Not the sole answer

• Observe Information Flow
  • How data moves in and out of the company

• Leverage the Existing Confidential Reporting Process
  • Established as the Ethics Hotline to protect accuser and accused

• Recognize Organizational Cultural Differences
  • Leverage what people know about their environment and what looks wrong

• Leverage the Existing “Acceptable Use” and “Security” Policies
  • You probably have all of the policy tenets in existing documents

• Write “Incident Escalation” Policies/Standards/Procedures
  • The Operational workflows to authorize investigations into employees

Above all - develop together and implement together
CI Connections

Reported to DSS and the FBI
The Second Time it was a shorter Process....

Reported to DSS and the FBI
CI Connections 3

Reported to DSS and the FBI
Insider Threat Indicators you might not think about

- Excusing violence against Americans – because it was provoked by America or American Policy
- Conspiracy theories about 9/11 etc. as attempts by USG to destroy others
- Support for a system of Religious Law to replace existing US Legal System
- Support for anarchy, secession or revolution or their advocates
- Tacit approval for illegal behavior (polygamy, retribution killings, discrimination etc.)
- Attacks on mainstream religions and their belief systems (declaring the practitioners Apostates etc.)
- Flashing unique hand signs or wearing/posting criminal or extremist tags or tattoos
- Professing immunity from US Law (Federal, State, Tribal etc.)
- Advocating the legitimacy of extralegal courts (citizen grand juries, common law courts, sharia courts, etc.)
- Disparaging the way of life in America and favoring alternate ideological systems (Anarchy, White Supremacy, Islamism)
- Showing disrespect to the National Anthem or National Colors
- Defaming the President of the US
- Refusal to pay Taxes, Register Motor Vehicles, or engage in any “Government Contract”
- Advocating the use of Lynching as a “Suitable Punishment” for specific racial or gender groups
- Bumper stickers showing support for anarchist, quasi legal or extralegal groups
- Pens, mouse-pads, ornaments, jewelry from extremist groups
Useful Resources

## Tools

- **Securonix** Security Analytics [http://www.securonix.com](http://www.securonix.com)
- **Veriato** * Recon 360/Monitor [http://www.veriatio.com](http://www.veriatio.com)
- **ObserveIT** Insider Threat Detection [http://www.observeit.com](http://www.observeit.com)
- **SureView** ** SureView Insider Threat [http://www.forcepoint.com](http://www.forcepoint.com)
- **Lockheed Martin** LM Wisdom ITI [http://cyber.lockheedmartin.com](http://cyber.lockheedmartin.com)
- **SRC** Personnel Risk Assessment Tool [http://srcinc.com](http://srcinc.com)
- **Haystax** Carbon [http://haystax.com](http://haystax.com)

* Spectorsoft has been re-branded as Veriato
** Raytheon/Websense has been re-branded as Forcepoint

## Web Resources

- **FBI / CERT** [http://www.cert.org/tech_tips/FBI_investigates_crime.html](http://www.cert.org/tech_tips/FBI_investigates_crime.html)
- **CERT** [https://www.cert.org/insider-threat/tools/](https://www.cert.org/insider-threat/tools/)
- **DoJ** [http://www.usdoj.gov/criminal/cybercrime/searching.html](http://www.usdoj.gov/criminal/cybercrime/searching.html)
Thank you

- Restrictions on use:
- Re-Distribution Not Permitted without consent of Author
- Not Export Controlled

trevor.odell@baesystems.com