INSIDER THREAT: DETECTING THE BAD ACTORS?

INTRODUCTION & BACKGROUND

Education:
• Fordham University, BA
• University of Maryland, MS

Career Experience:
• Air Force Office of Special Investigations (AFOSI), Special Agent
• CACI, Contract Intelligence Analyst (U.S. Intelligence Community Customer)
• Lockheed Martin Counterintelligence & Insider Threat Operations, Intelligence Analyst

INSIDER THREAT PHENOMENON
INSIDER THREAT DEFINITION

- Intelligence & National Security Alliance (INSA) definition:
  - “The threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who, willingly, or unwittingly, commits: acts in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace.”
- Based upon commonly shared behaviors preceding acts of workplace violence, suicide, and espionage
- A program built around behavioral analysis allows for applicability for a variety of threats
- Allows for education of employees based on broad observable behaviors

SHIFTING THREAT LANDSCAPE

- Government
  - Classified Information
  - National Security
  - Foreign Nations
  - Espionage
- Private Industry, Financial Institutions, Universities, Law Firms
- Corporate Proprietary, Intellectual Property, Pre-Classified Research
- US Technological Edge, Financial Prosperity, Brand Preservation
- Industry Competition, Self Interest
- Workplace Violence, Sabotage, Theft of Trade Secrets

ENVIRONMENTAL FACTORS

- The incidence of employee financial hardships during economic downturns
- Employer affordability initiatives
  - Reduction of benefits and pension plans, lay-offs, etc.
- The global economic crisis
  - Foreign nations more eager to acquire new technologies, R&D
  - Mergers, acquisitions, divestitures, joint ventures
  - Ease of stealing anything stored electronically
  - Increased exposure to foreign intelligence entities (FIE) presented by the reality of global business
  - Increase in FIE recruitment of students
  - Widespread data breaches
INDIVIDUAL MOTIVATING FACTORS

- "I was angry all the time...I had an overwhelming need to lash out at the FBI...and strike out...I wanted to hurt them." - Earl Edwin Pitts
- "I needed the money: Plus, well, I was extremely angry." - David Sheldon Boone
- "I obeyed my conscience rather than the law. I believe our government’s policy towards Cuba is cruel and unfair, profoundly un-neighborly, and I felt morally obliged to help." - Ana Montes
- "I used examples based on my B-2 experiences and knowledge. At that time I knew it was wrong and I did it for the money." - Noshir Gowadia
- "I think he’s just a man, and that flattery does much to their ego, and he’s just fallen into it." - Witness re: Benjamin Bishop
- "I tried to serve two countries at the same time. That does not work. There can be no justification for violating the trust given an intelligence officer." - Jonathan Pollard
- "No one held a gun to my head. There was a lot of psychological pressure." - Joseph Helmich

DETECTION & MITIGATION

ORGANIZATIONAL STRUCTURE
# INSIDER THREAT DETECTION PROGRAM

<table>
<thead>
<tr>
<th>Planning</th>
<th>Development</th>
<th>Implementation</th>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting Leadership</td>
<td>Tool Procurement / Development</td>
<td>Data Ingestion &amp; Tool Calibration</td>
<td>Oversight</td>
</tr>
<tr>
<td>Peer Benchmarking</td>
<td>Establishment of Potential Risk Indicators</td>
<td>Roll-out Message to Employees</td>
<td>Metrics</td>
</tr>
<tr>
<td>Identification of Program Stakeholders</td>
<td>Identification of Required Data Sets</td>
<td>Establishment of Incident Management Procedures</td>
<td>Red Team</td>
</tr>
</tbody>
</table>

## Proactive alignment with Executive Order 13587

## Over and above government requirements

## Identifies indicators of persons at risk & potentially malicious activity

## Analyzes data for behavioral patterns

## Applications beyond traditional Insider Threat

## Government interest in approach

## Recipient of 2014 CSO40 Award

## 2011, 2013 & 2016 Defense Security Service Award for Excellence in Counterintelligence

## 2017 Lockheed Martin NOVA Award

## INSIDER THREAT TOOL

- Evaluation of employee attributes, behaviors and actions according to analyst-defined models
- Automated link analysis
- Analyst defined categories and attributes of interest
- Weighted categories and attributes
- Models run against an entire population or subsets
- Based on Big Data technologies (petabyte+)
- Notifications and alerts
- Data encryption
- NO PROFILING
PROGRAM GOVERNANCE

• Oversight
  • Board of Directors
  • Corporate Risk & Compliance Committee
  • Internal Audit
  • Corporate Sustainability
  • Insider Threat Steering Committee
  • Security, Legal (Privacy), HR, Ethics, Corporate Information Security
  • Quarterly briefings on results, successes, challenges, etc.
  • Manage company policy updates
• National Industrial Security Program requirements
• System Audit Logging

PRIVACY CONSIDERATIONS

• Communications plan to properly introduce program to employees
  • Provide appropriate mechanism to voice concerns
• Proper adoption of local restrictions applicable to foreign and expatriated employees
• Access to automated tool heavily restricted
• “Red team” exercises to ensure highest level of system defenses
• Continual coordination with Chief Privacy Officer (General Counsel)
• Member of CI team privacy certified through international association of privacy professionals (IAPP) – (in progress)
• NO PROFILING!

QUESTIONS?