The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Insider Threat Awareness Virtual Roundtable

September 18, 2012

Homeland Security

Caitlin A. Durkovich

Assistant Secretary for Infrastructure Protection

- Leads the Department's efforts to strengthen public-private partnerships and coordinate programs to protect the Nation's critical infrastructure, assess and mitigate risk, build resilience, and strengthen incident response and recovery
- Has more than 13 years of homeland security-related expertise covering a wide range of activities including continuity of operations and business continuity planning, cybersecurity, institutional transformation, and communications

Homeland Security

Jonathan Richeson

Security Specialist, Department of Homeland Security

- Jon Richeson currently works for the Department of Homeland Security, in the Office of Infrastructure Protection, Commercial Facilities Section
- Former U.S. Air Force Security Forces officer, with a Bachelor's Degree in Justice Administration from the University of Louisville and a Master's Degree in Homeland Security from the American Military University

Homeland Security

Dawn Cappelli

Technical Manager, CERT Insider Threat Center, Carnegie Mellon University

- Technical Manager, Enterprise Threat and Vulnerability Management and the CERT Insider Threat Center, CERT Program, Software Engineering Institute, Carnegie Mellon University
- Team 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
- More than 30 years of experience in software engineering, technical project management, information security, and research

Homeland Security

Dave B.

Supervisory Special Agent, Federal Bureau of Investigation

Insider Threat Investigations Unit (CD-4D)

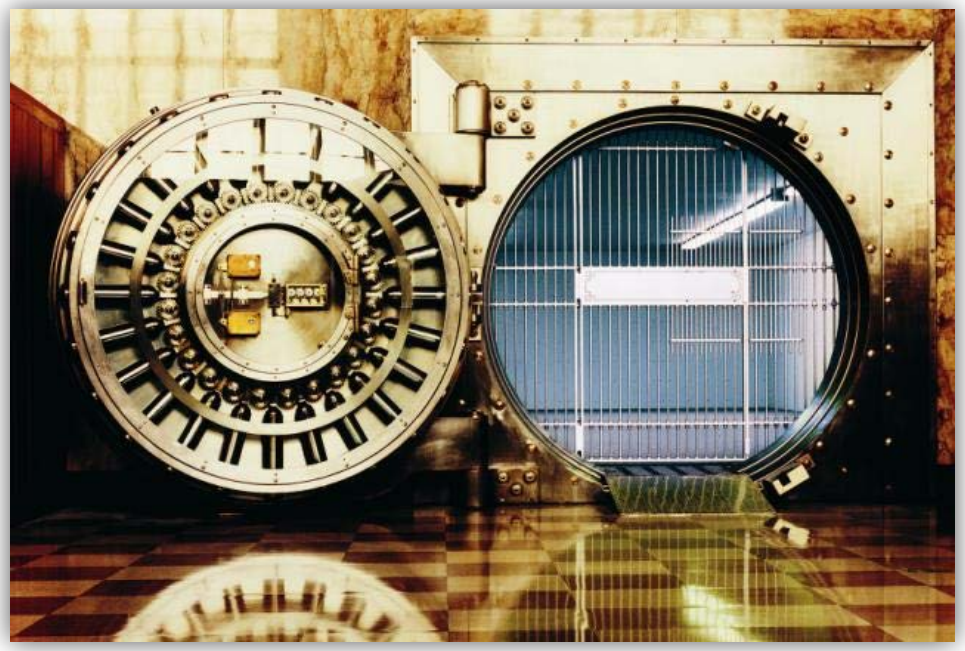
- Investigates FBI personnel suspected of engaging in:
  - Espionage or related activity
  - Unauthorized disclosure of classified information
  - Media leaks
- Provides insider threat-related outreach and awareness training to FBI personnel, the U.S. intelligence community, the U.S. government, cleared defense contractors, friendly foreign partners, business, and academia

Homeland Security

What Is an Insider Threat?

The insider threat to critical infrastructure is one or more individuals with the *access and/or inside knowledge* of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.

—The National Infrastructure Advisory Council Final Report and Recommendations on the Insider Threat to Critical Infrastructures (2008)



Homeland Security

Objectives

- To help critical infrastructure owners and operators to understand the importance of:
  - What **malicious insiders** are and how they impact organizations
  - What an organization can do to **deter and detect** insider threats
  - What **defense and response strategies** are available to mitigate the insider threat

Homeland Security

Polling Question

- What percentage of companies do you think have been victims of Insider Threats?

Homeland Security

How Big Is the Threat?

- Very little preexisting data, partially because 70% of insider incidents are handled internally and without legal action, per the 2011 CyberSecurity Watch Survey
- 43.2% of security practitioner respondents representatively surveyed attributed some loss to malicious insiders, per the 2010 / 2011 Computer Security Institute / FBI Study
- FBI case load for economic espionage has doubled; indictments increased five-fold, convictions risen eight-fold
- Average cost per data breach event was $5.5 Million per the Ponemon Institute study reported in the 2011 U.S. Cost of Data Breach Study

Homeland Security

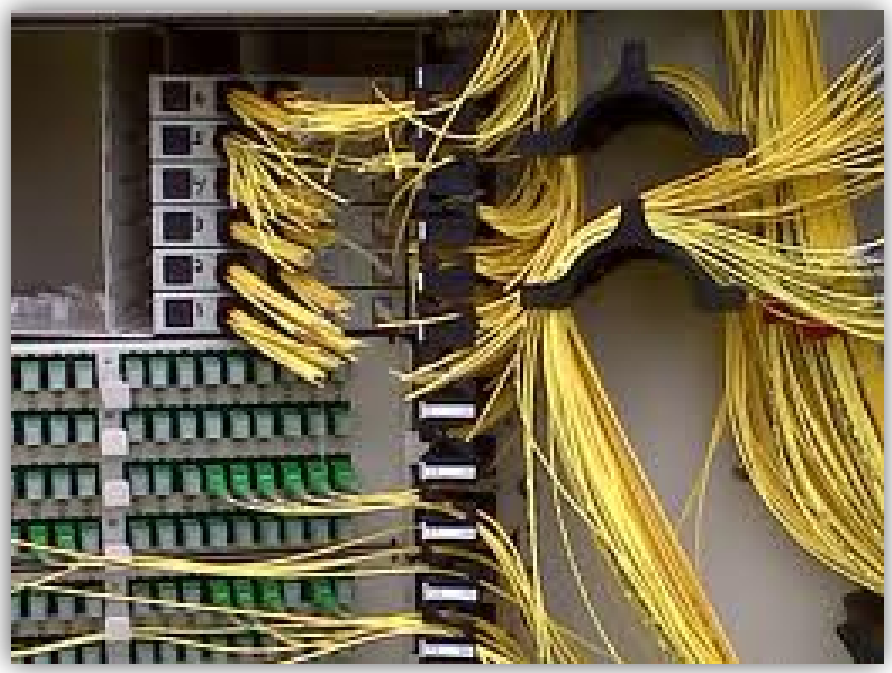
Types of Insider Threats

- Physical and Information Technology (IT) Sabotage
- Theft of Intellectual Property
- Fraud
- National Security Espionage (*Not included in this presentation*)

Homeland Security

Physical and IT Sabotage: What Is It?

- A current or former insider misuses systems with the intent to cause harm to an individual or organization
- Case studies:
  - Supervisory Control and Data Acquisition (SCADA) sabotage releases 800,000 liters of raw sewage into parks and rivers
  - Employee brings down his former employer, a global retailer, for a week during the busiest shopping days of the year
  - Contractor uses physical access to shut down operations at a power generation facility after being suspended by his company on Friday afternoon



Homeland Security

Physical or IT Sabotage: Profile

- Disgruntled former employee
- Often already on Human Resources (HR) radar
- Leaves under unfavorable circumstances
- Sets up attack before leaving

Physical or IT Sabotage	
Current or former employee?	Former
Type of position	Technical (e.g., systems administrators, programmers, or DBAs)
Target	Network, systems, or data
Access used	Unauthorized
When	Outside normal working hours
Where	Remote access

Homeland Security

Physical or IT Sabotage: Mitigation

- Communication between HR / management / security / IT, when problem insider is identified
- Audit for online activity that could be setting up an attack
- Monitor employees who have been identified as insider threat risks
- Ensure that access is revoked immediately once an employee leaves the organization or is terminated

Homeland Security

Theft of Intellectual Property: What Is It?

- An insider steals intellectual property, which includes trade secrets, strategic plans, and source code (often scientific or engineering information)
- Case studies:
  - A programmer took source code and schematics for a nuclear power plant back to home country of Iran
  - A Boulder, Colorado software company went bankrupt after an employee stole its source code and took it to China to set up his own business

Homeland Security

Theft of Intellectual Property: Profile

- Some crimes benefit a foreign government or organization
- Can involve financial difficulties, underperforming, at risk (or perceived to be) for layoff/termination
- Steal on the way out the door

Theft of Intellectual Property (IP)	
Current or former employee?	Current (within 30 days of resignation)
Type of position	Technical (e.g., scientists, programmers, engineers) or sales
Target	IP (trade secrets) or customer information
Access used	Authorized
When	During normal working hours
Where	At work

Homeland Security

Theft of Intellectual Property: Mitigation

- Identify most critical assets
  - Surround those assets with higher levels of security
  - Limit access to most critical assets/information
- Audit anomalous activities (e.g., large data transfers)
- Report foreign travel
- Do not allow company assets to be taken outside the U.S. (laptop, blackberry, etc.)
- Remind employees about company policies and property ownership upon hire, periodically, and upon resignation

Homeland Security

Fraud: What Is It?

- Insider theft or modification of information for personal gain – not always financial (e.g., students changing grades)
- Case studies:
  - Three meter reader employees scheme with customers to eliminate $800,000 in utility bills
  - An undercover agent who claims to be on the “No-Fly” list buys a fake driver’s license from a ring of DMV employees who sold more than 200 fake licenses for more than $1 Million

Homeland Security

Fraud: Profile

- Lower level employees (or their managers)
- Usually separation of duties (someone who cannot make a change without someone else's approval)
- Financial difficulties
  - Need turns to greed
- Social engineering
- Often recruited into the group/ring

Fraud	
Current or former employee?	Current
Type of position	Non-technical (e.g., data entry, customer service) or their managers
Target	PII or customer information
Access used	Authorized
When	During normal working hours
Where	At work

Fraud: Mitigation

- Pay attention to employees with financial difficulties
- Think like a “bad guy”
- Learn from past mistakes
- System checks for anomalies

Homeland Security

Video

- Indicators
  - Review of indicators
- Analysis
  - Mitigation strategies
  - Practical application (examples as they relate to the video)

Homeland Security

Polling Question

- Would you feel comfortable reporting a potential insider threat in your current work environment?

Homeland Security

Call to Action: Form a Team

- Form an Insider Threat Mitigation Team

Homeland Security

Call to Action: Develop Policies

- Develop policies for how to protect against and address insider threat

Homeland Security

Call to Action: Provide Training

- Train employees to recognize and report suspicious behavior

Homeland Security

Polling Question

- Does your organization have a formal process for dealing with these three types of insider threats?

Homeland Security

Resources

Insider Threat Center (http://www.cert.org/insider_threat/)

- *Common Sense Guide to Prevention and Detection of Insider Threats* (http://www.cert.org/archive/pdf/CSG-V3.pdf)
- *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)* (http://www.sei.cmu.edu/library/abstracts/books/9780321812575.cfm?wt.ac=hpLibrary)
- Insider threat workshops
- Insider threat assessments
- Insider threat exercises
- New controls from CERT Insider Threat Lab

CERT | Software Engineering Institute Carnegie Mellon

Homeland Security

Resources (cont.)

FBI's public Web site (http://www.fbi.gov)

- FBI Counterintelligence Strategic Partnerships (http://www.fbi.gov/about-us/partnerships_and_outreach/investigate/counterintelligence/strategic-partnerships)
- InfraGard (www.infragard.net)
- Links to:
  - Local FBI Field Office
  - *The Insider Threat*
  - *Intellectual Property Protection*
  - *Safety Tips for Students Traveling Overseas*
  - *Safety Tips for Businessmen/Women Traveling Overseas*
  - *Social Networking Risks*
  - *Risks & Mitigations of Visitors*
  - *Elicitation Techniques*
  - Past FBI counterintelligence/espionage cases

Homeland Security

Resources (cont.)

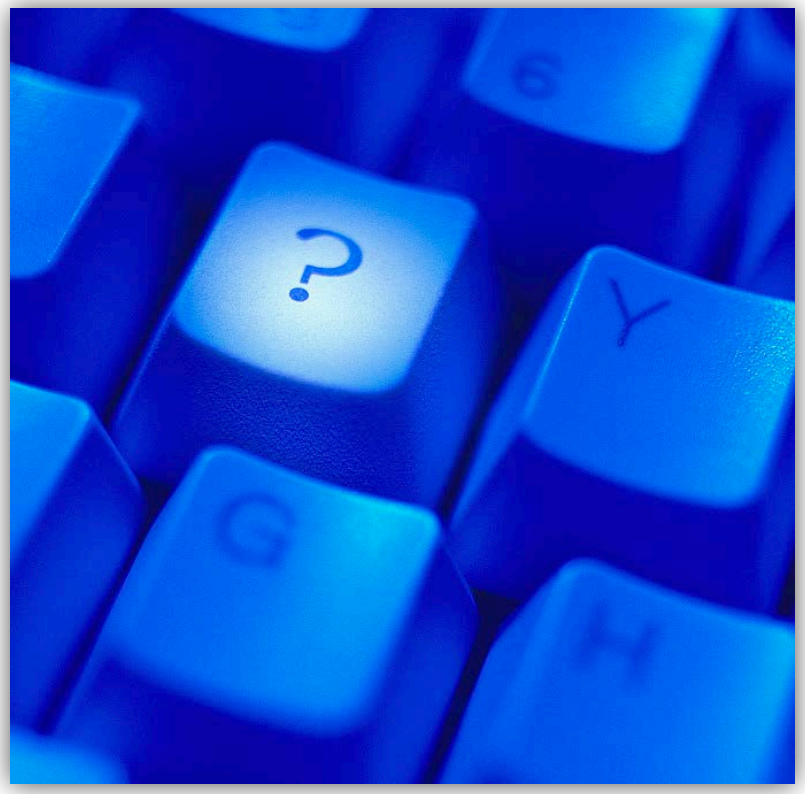
Department of Homeland Security (http://www.dhs.gov/criticalinfrastructure)

National Risk Estimate on Insider Threat

- The DHS Office of Infrastructure Protection developed the National Risk Estimate (NRE) on Insider Threat, a comprehensive assessment of insider risks and trends related to critical infrastructure
- The NRE on Insider Threat:
  - Assesses risk scenarios to all critical infrastructure sectors
  - Incorporates significant input from private and public sector partners and stakeholders from a series of red team/blue team exercises
  - Includes consultation from the foremost experts of insider threat analysis
- Results are available now, upon request
  - Contact: Dennis.Deziel@hq.dhs.gov or Brandon.Wales@hq.dhs.gov

Homeland Security

Question and Answer Session



Homeland Security

Homeland Security

For more information visit:
www.dhs.gov/criticalinfrastructure

Insider Threat Awareness Virtual Roundtable

For additional information contact:

stopinsiderthreat@hq.dhs.gov