FBI AND CYBER SECURITY

SSA John Caruthers
SSA Tom Winterhalter
SSA Ken Schmutz

Mission

- The FBI is the only U.S. agency charged with the authority to investigate both criminal and national security investigations.
- As a law enforcement agency and a full member of the US Intelligence Community, the FBI serves as a vital link between the two groups.
- The traditional distinction between national security and criminal matters is increasingly blurred as terrorists commit crimes to finance their activities, organized crime groups exploit international boundaries and jurisdictions, and computer hackers cause havoc or create vulnerabilities that can be exploited by foreign spies.

Cyber Threats

- Cyber Criminal Threats
  - Botnets (Resources), ACH Fraud, Extortion, Insider Threats
- Cyber Terrorism
  - Internet being used not just to recruit or radicalize, but to incite.
  - Growing use of social network site to collaborate and promote violence.

Cyber Threats

- Counterintelligence and Economic Espionage
  - Espionage used to be spy vs. spy
- Who are they?
  - Nation-State Actors, Mercenaries for Hire, Rogue Hackers, Transnational Criminal Syndicates
- What are they after?
  - Technology, Intelligence, Intellectual Property, Military Weapons, Military Strategy
  - They have everything to gain; we have a great deal to lose

FBI Response

What the FBI can do

- Investigate
  - National and global
  - Combine technical skills and investigative experiences
  - Long-term commitment of resources
- Forensics (RCFL)
- Patterns and Links
- Bring national security concerns to intelligence community

FBI Response

- 56 Field Offices with Cyber Squads.
- 75 FBI Legal Attaché Offices around the world.
  - Cyber Trained Agents embedded with foreign police forces.
  - Promotes joint operations/initiatives with international partners.
- Training provided to international law enforcement community.

FBI Response

- National Cyber Investigative Joint Task Force
- Cyber Action Team
- Groups that are focusing on key threats and trends.
  - These groups consist of agents, officers, and analysts from different agencies.
  - ICS/SCADA TFC – FBI, DHS, and OGA partnering together.
- Establishing cooperative working relationships with regulatory groups and agencies.
    - InfraGard

FBI Response

What the FBI won't do

- Take over your systems.
- Repair your systems.
- Share proprietary information with competitors.
- Provide investigation-related information to the media or shareholders.

- In essence … we will not further victimize the victim.

Cooperation

- The most effective weapon against crime is cooperation … The efforts of all law enforcement agencies with the support and understanding of the American people.
  - J. Edgar Hoover

Cooperation

- Assessments
  - Partnership with DHS ongoing program
  - Free to asset owners across all 18 CIKRs
  - **Optional** FBI participation provides the asset owner an easy transition for investigative handoff
  - **Optional** FBI participation will enhance domain awareness and help to cultivate the FBI Infragard program within the control system community
- Incident Response
  - Fly team:
    - US-CERT
    - ICS-CERT
    - DHS-CSSP
    - FBI **(Optional)**
  - DHS entities focus on operational assurance
  - FBI provides investigative expertise

Reporting Information

- Why should you report to us?
  - You may help prevent/identify an incident or victim.
  - Another piece of the puzzle.
  - How much do you know about the interdependency between the US and Canada:
    - $6.0 billion in trade between Canada and Florida.
    - Nearly 500,000 jobs in Florida depend on trade with Canada.
    - Florida's agricultural sales to Canada amounts to $726 million.
    - Canada is the largest oil and natural gas supplier to the US.
    - Canada is the largest supplier of nuclear fuel to the US.
    - Canada is the largest electricity supplier to the US
      - Canada and the US share an integrated electricity grid and supply almost all of each other's electricity imports.

Stuxnet

- Always worth mentioning …
- Proof of concept
- Stuxnet vs. Aurora … the original Aurora.
  - Is it really a problem?
  - What do your engineers say?
- Unintended Consequences
  - Persistence and a Loss of Revenue.
  - Are you still secure?

Questions?

- SSA John Caruthers
- SA Winterhalter
- SSA Ken Schmutz
- SA Smithmier