InfraGard

Overview

- Today's FBI
- The FBI's role in cyberspace
  - FBI's Cyber Division
  - Critical Infrastructure protection
  - Sharing with the Department of Homeland Security
- InfraGard
  - Overview
  - Information sharing
  - Initiatives
  - Case study accomplishments

InfraGard

- Overview
- Information sharing
- Initiatives
- Case study accomplishments

InfraGard

Overview

InfraGard Program Mission Statement

To support an information sharing partnership between the private and public sectors for the purpose of protecting the nation's critical infrastructures against attacks or failure caused by either foreign or domestic threats, and to support all FBI investigative programs, especially Counterterrorism, Counterintelligence, and Cyber Crime.

InfraGard: An FBI Program and An FBI Registered Service Mark

- Expanded from 3 cities in 1996 to all Field Offices today
- **84 Chapters** with more than **13,273** members (2/8/06)
- Local Governance
- National perspective

Meeting the Challenge: Build Trust

- Applicants for membership (infragard.net) agree to:
  - Vetting: The FBI conducts record checks on all applicants
    - Crucial towards gaining confidence by information owners
  - Non-Disclosure: Members agree to protect this restricted information to the extent requested by the submitter
    - Admonishments

Formal Structure

- In the beginning, FBI and Industry just met and called the partnership "InfraGard"
  - Problem 1: Industry had to get FBI approval each time it wanted to act under the InfraGard name. Sometimes the FBI could not approve what industry wanted:
    - For example, FBI usually cannot accept gifts from "sponsors" or endorse products, but industry can
  - Problem 2: The need arose to better distinguish between InfraGard's FBI participants and InfraGard's industry participants
    - Members of "FBI InfraGard," some with business cards, began to look like they represented the FBI

The InfraGard Structure:

- For national InfraGard issues, FBI Headquarters works with the INMA Board of Directors.
- The FBI and the INMA have signed a Memorandum of Understanding defining their relationship with each other.
- The INMA may establish relationships with entities other than the FBI.

Annual

- Coordinator/Supervisor Training
  - Program's national perspective
  - Address local Chapter needs
- National Congress
  - Private sector votes for InfraGard National Member Alliance board
  - Conference (August 21 – 24, 2006)
    - www.infragardconferences.com

Examples of Different U.S. Models

- Industry led
  - Information Sharing & Analysis Centers (ISACs): typically exist to promote sharing among businesses in the same industry, and to interact with government.
- Law Enforcement or other Agency led
  - FBI's InfraGard program and FBI Cyber Task Forces
  - US Secret Service Electronic Crimes Task Forces
  - US Department of Homeland Security's US-CERT
- Federally Funded Joint Programs
  - Internet Crimes Complaint Center (IC3): FBI together with the National White Collar Crimes

Why InfraGard?

- Sharing of FBI & DHS threat alerts, advisories & warnings
- Protection requires assistance from owners and operators
- Networking-computer and physical security expertise shared and enhanced – meetings, seminars, forums
  - Discussion groups, listservs, seminars, conferences
- Ongoing relationships establish trust and confidence between members and the FBI/other law enforcement
- Training initiatives and local/national partnerships

InfraGard

Information Sharing

The Need for Cooperation

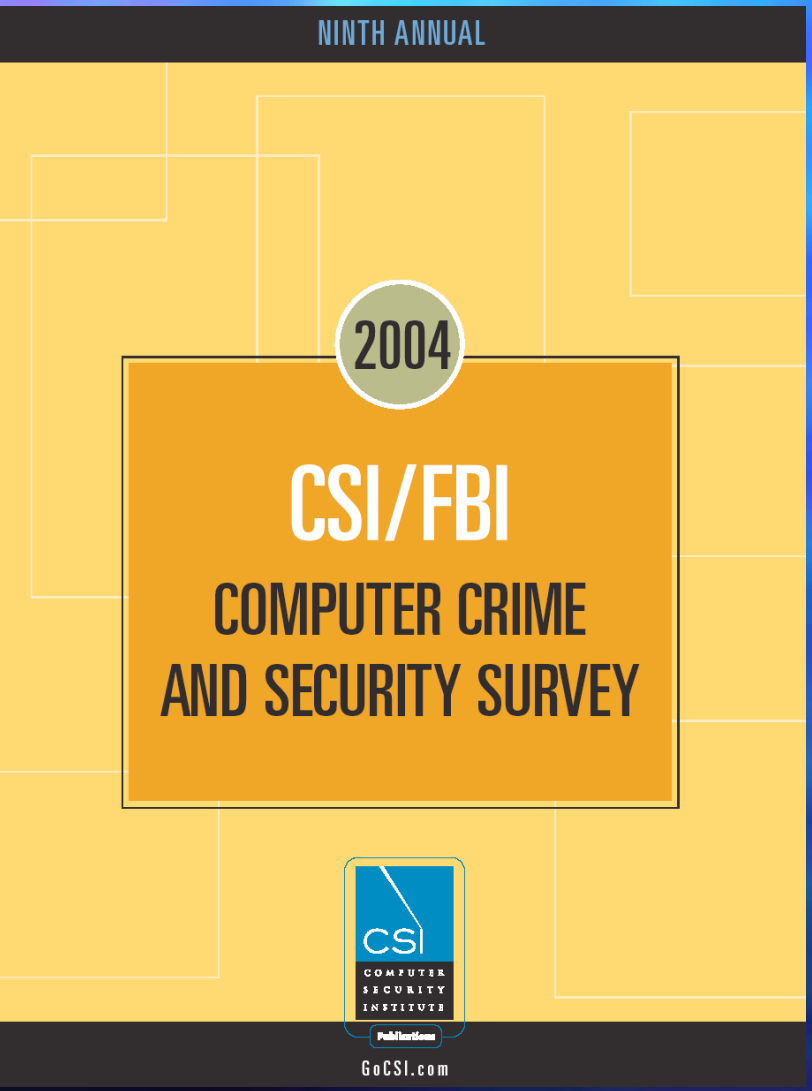
- In the US, industry generally has no legal obligation to report computer crimes to law enforcement
  - Without voluntary industry reporting, law enforcement will be unaware of serious crimes
  - In U.S., roughly 85-90 percent of the critical infrastructure is privately owned and operated
- Crime cannot be addressed by industry acting alone
  - Penalties and deterrent effect from law enforcement
  - Some investigative techniques reserved for law enforcement
  - Global aspects of computer crime make some solutions unlikely or impossible

Reasons Given for Not Sharing

- Reporting crime to law enforcement:
  - Bad publicity will result in loss of consumer confidence
  - Possible civil liability for having poor security
- Sharing vulnerability information with others:
  - Information may get into the wrong hands (including both criminals and competitors)
  - Possible civil liability if shared information is wrong
  - Possible antitrust considerations if sharing is anti-competitive

CSI/FBI Cybercrime Survey

free report: www.gosci.com



- Survey Size: nearly 500
- If you had a computer intrusion, what did you do?
  - Patched holes = 91%
  - Did not report to anyone = 48%
  - **Told Law Enforcement = 20%**
  - Told Legal Counsel = 16%
- Why not report computer crime to law enforcement?
  - **Bad publicity = 51%**
  - Competitors would use = 35%
  - Can handle without police = 20%
  - Think they're not interested = 18%

How accomplished?

- Intelligence product for dissemination to InfraGard secure web
  - Jointly with DHS if possible
  - Produced by owner of information, Analyst/Agent, Field Office and FBIHQ
  - Field Office - Field Intelligence Group
    - Dissemination – locally & to all InfraGard Chapters if requested
  - FBIHQ or Cyber Division – Information Sharing and Analysis Unit
    - Dissemination – for national InfraGard
- Goal: assimilation and sharing of new information for intelligence or case work
- InfraGard intelligence admonishments on secure web

InfraGard

Initiatives

Initiatives

- Cyber Incident Detection Data Analysis Center
- National Cyber Forensics & Training Alliance
- Co-sponsorship Agreement – NIST/SBA/FBI
- NSIE
- Special Interest Groups (Chemical)
- Foreign Affiliate Program
- Philippines “InfraGard” Initiative

Cyber Incident Detection Data Analysis Center (CIDDAC)

- www.CIDDAC.org
- Public/private partnership (Philadelphia InfraGard) formed to establish an automated and actionable real-time cyber threat reporting system
- A complete process for reporting cyber attacks, without risking privacy
  - Real-time Cyber Attack Detection Sensor (RCADS)
- Provide data necessary for research and development institutions
- Provide LE necessary data to identify, locate and neutralize significant threats
  - Law Enforcement Incident Report

CIDDAC Pilot

- Launch date March 15, 2005
  - University of Pennsylvania
  - FBI Philadelphia Field Office & InfraGard Chapter
  - Outreach to other LE
- Participant recruiting and sensor deployment
- Laboratory space and graduate student participation secured at University of Pennsylvania
- DHS/DOD R&D provided $200K toward pilot
- Seeking DHS $400K toward RCAD deployment

National Cyber-Forensics & Training Alliance (NCFTA)

- www.ncfta.net
- Public/private partnership
  - Pittsburgh, Pa
- Academia, Private Sector, Public organizations
- Provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly and where resources can be shared
- Facilitates advanced training, promotes security awareness to reduce vulnerability, and conducts forensic lab simulations

NCFTA

- SLAM-Spam & Digital Phishnet Initiatives
  - 100+ cases submitted to LE
  - Top 15 spammers targeted worldwide
  - Local & regional training delivered
  - Spin-off Projects targeting Phishing/Identity Theft & Online Pharmacy fraud under way
- Operation Web Snare (August 2004)
  - 155+investigations
  - $184,000,000+ in losses
  - 878,560 victims
  - 115+ arrests/convictions
- Asian Tsunami Scams (January 2005)
  - 800+ websites analyzed
  - 100+ sites shut down
  - 50+ matters referred for investigaiton
- Hurricane Katrina Scams (September 2005)
  - 5000+ websites analyzed
  - Pulbic servcie adi

Co-Sponsorship Agreement Computer Security for the Small Organization Seminars

- Begun June 2002: Commerce Department's National Institutes of Standards and Technology, Small Business Administration and FBI
  - Promote computer and information technology security to safeguard their information systems
    - 95% of U.S. businesses, >20 mil, are small and medium size
    - A vulnerability common to most could pose a threat to our Nation's economic base
- 2006: San Diego, Santa Anna, Glendale, CA; Colorado Springs, Denver; Cheyenne/Casper, Wyoming; Rapid City, South Dakota

Network Security Information Exchange

- National Communications System
  - National Security Telecommunications Advisory Committee
- Government and private sector meet to share information
- NSIE Program Manager, InfraGard member
- InfraGard Program participation expands knowledge of how FBI is sharing information
- Fosters protocols with DHS
- Improves FBI technical capabilities:
  - PBX training
  - SME for Boise, Idaho matter

Special Interest Groups

- Chemical InfraGard (infragard.net)
  - December 22, 2005
- FBI Counterterrorism and Cyber Division partnership w/ the Chemical Industry Sector:
  - Communication; information sharing; investigative purposes
- Goal: to be a consortium of chemical industry professionals with aim of protecting chemical plants/industry
- Secure web: features and links
- Must be an InfraGard member
  - InfraGard private sector outreach to FBI
  - Expands FBI's Chemical Outreach Program

Foreign Affiliate Program

- Draft
- InfraGard Members Alliance – may enact individual policies re denying or granting permission for non-IG members to attend meetings
  - Affiliate Application for Non-Members
    - Non-U.S. Citizen lawfully admitted for permanent residence (can serve in U.S. Armed Forces)
    - No records check
  - Same Code of Ethics
    - Not an InfraGard Member/cannot vote
    - Cannot view restricted information
    - Cannot access secure web

Philippine "InfraGard" Initiative

- Critical infrastructure protection mechanism based on InfraGard model – they asked us….
- September/October 2005
  - Cebu, Regional Cyberterrorism Conference
  - Manila: Australian Federal Police; Manila American Chamber of Commerce Information and Communications Technology Committee; Microsoft CIO working group; Asian Development Bank; FBI equivalent in LE; Philippine Computer Technology Center
  - Key interest is information exchange – that trusted relationship
    - August 2005, San Diego InfraGard Coordinator
    - November 2004, presentation for Undersecretary Purugganan
  - Philippine Congressional delegation visited FBIHQ, January 2006

Questions?

John "Chris" Dowd

John.dowd@ic.fbi.gov

(202) 324-1419