Responding to Cybercrime in the Post-9/11 World

Scott Eltringham

Computer Crime and Intellectual Property Section

U.S. Department of Justice

(202) 353-7848

Crime on the Internet

- The Internet provides a target rich environment for criminals
- Attacks are easy, low risk, hard to trace technically, hard to prosecute, and can have a high payoff
- Sophisticated tools are readily available
- Access can be from anywhere and anonymous

Computer Attacks

- Attacks on:
  - Confidentiality,
  - Integrity or
  - Availability of information or systems
- Theft of information, services, or damage

Typical Criminal Cases

- Fraud
  - Credit Card Fraud
- Economic Espionage
  - Large File Transfers
  - Raiding of Employees/Technical Know-how
- Hacking
  - Denial of Service Attack
  - “Cyber-vandalism”

Impacts of 9-11

- Heightened awareness by businesses of the vulnerability of their information systems and physical plants.
- Companies need to revisit their security procedures in light of changed circumstances.
- Looming threat of CNA

Topics Overview

- What is Being Done
- Why Statistics are Crucial

The USA Patriot Act

- Provided new and clarified existing electronic evidence gathering authorities
- Why the "USA Patriot Act"?
  - Senate: Uniting and Strengthening America (Act)
  - House: Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Act)

Overview

- The Pen Register and Trap and Trace Statute
- The Computer Trespasser Exception
- The Cable Act Fix
- Other Amendments to the Wiretap Statute and ECPA

The Pen/Trap Statute

- Old statute: the term "pen register" means a ***device*** which records or decodes electronic or other impulses which identify the ***numbers dialed*** or otherwise transmitted on the ***telephone line to which such device is attached*** **(18 U.S.C. 3127(3))**
- New statute: Technology-neutral language

The Pen/Trap Statute (cont.)

- New Language: the term "pen register" means a device ***or process*** which records or decodes **dialing, routing, addressing, or signaling information** transmitted by an instrument or facility from which a wire or electronic communication is transmitted ...
- Technology-neutral adjustments made throughout

Computer Trespasser Exception

- Old law: law enforcement often had to get a wiretap order in order to help victims monitor computer hackers
- This made no sense: the wiretap statute protected hackers even where they had no reasonable expectation of privacy in their communications
- New law: new exception to Title III
  - allows interception of "computer trespassers" - i.e. those without authorization to use a computer

Other Amendments

- Voice mail fix
- Scope of subpoenas under 2703(c)
- Voluntary disclosure of information by providers
- Nationwide search warrants for e-mail
- Voice wiretaps in hacker investigations

Why Do Statistics Matter?

- Companies Often Reluctant to Report
- Proof that they are far from unique would be very helpful

Why Companies Don't Report

- Loss of Control
  - Direction of case: LE can't be fired
  - Costs
  - Publicity
- Lack of Confidence
  - Unsure of LE interest
  - Unsure of LE competence

Should companies report to LE?

- YES!
- Federal agents have
  - investigative skills
  - forensic knowledge
  - access to attachés in foreign countries
  - established relationships with Internet players
  - can aggregate your information with data from other cybercrime victims

Other Surveys

- CSI/FBI
  - 503 respondents, a good start
  - 90% had computer security breaches
  - 80% had financial losses as a result
  - only 34% reported to LE
- PWC
  - 44% of British businesses had suffered a "malicious security breach" in the last year

Where To Get More Information

- Computer Crime Section: (202) 353-1787
- My e-mail: scott.eltringham@usdoj.gov
- Computer Crime Section's page on the World Wide Web: