Promoting Regional and International Cooperation On Cybersecurity Issues

Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection

February 20, 2008

Mark L. Krotoski
Computer Crime and Intellectual Property Section
U.S. Department of Justice, Criminal Division

Overview

- Challenges
- Objectives
- Importance Of Electronic Evidence
- 24/7 High Tech Crime Network
- Benefits and Case Examples

Challenges

- Computer Crime crosses boundaries
- Perpetrators or key evidence may be in another country
- Electronic evidence is perishable
- Changing technologies

Objectives

- Recognize Interconnectedness
  - Shared issues and problems
- Follow leads across boundaries soon after crime
- Preserve and obtain evidence promptly
- Establish responsive mechanisms
  - Foster collaboration and cooperation
  - Keep current with technological changes
  - Legal framework

Importance Of Electronic Evidence

- Among The Best Evidence
  - Captures Moment
- Consider Early In Investigation
  - Perishable
  - Retention Issues
  - Records May Be In More Than One Place
- Role
  - Instrument of Crime
  - Target of Crime
  - Storage Platform

Importance Of Electronic Evidence

- Question for every case:
  - Do you have Electronic Evidence?
- If so, make preservation request
  - Upon request of governmental entity
  - Retain 90 days
  - 90 day extension
- Process

Preservation Example

- Trade Secret/Economic Espionage Case
- After arrest in December
- FBI preservation request
  - Yahoo and Hotmail accounts
- January E-Mail Search Warrants
- Between December 22nd to January 2nd
  - 966 emails from defendant's email account deleted from PRC

YAHOO!

24/7 High Tech Crime Network

- Point of Contact
  - Available 24 hours, 7 days-a-week
  - Provide immediate attention
    - Investigations or proceedings concerning criminal offenses related to computer systems and data
    - Other criminal cases involving the collection of evidence in electronic form

24/7 High Tech Crime Network

- Nearly 50 member countries
  - Group of 8 (G8) Nations Ministers (1997)
  - Many Asian, European and South American countries
- Network enhances and supplements (but does not replace) traditional methods
- Recent Case Examples

Requirements 24/7 Network

- Identify Point of Contact Who Understands
  - Technology
  - Domestic Law
  - Domestic Law ability to assist other countries
- 24/7 POC Initially Contacts 24/7 Representatives
- Inform Domestic Law Enforcement Of Membership

Joining 24/7 Network

- Contact G-8 Chair, High-Tech Crime Subgroup
  - Christopher.Painter@usdoj.gov
  - Betty.Shave@usdoj.gov
  - Telephone: +1 (202) 514-1026
  - Computer Crime and Intellectual Property Section, USDOJ, Washington, D.C.
- Short Form

Benefits

- “Around-the-clock” capability
  - Respond shortly after crime reported
- Follow, preserve and obtain evidence across boundaries
- Point of Contacts knowledgeable on high-tech matters
- Cases Solved
  - Proven track record

Promoting Regional and International Cooperation On Cybersecurity Issues

Questions ?

Mark L. Krotoski
Computer Crime and Intellectual Property Section
U.S. Department of Justice, Criminal Division
Mark.Krotoski@usdoj.gov