The Law Enforcement Response to Crime on the Internet

Law Enforcement’s Roles and Responsibilities on a Unique Frontier

Special Agent Brad Sheafe
FBI - Springfield Division
"Frankly, I miss the old days of John Dillinger and Al Capone."
A Little History…

- The Western Wilderness…
- The Wild West…
- The Modern West…

A truly unique frontier, especially for law enforcement
Right!

- **The WWW**
  - 1990: 1st commercial dial-up ISP
  - 1993: 600 sites
  - 1994: 10,000 sites
  - 1995: 100,000 sites
  - 1997: 1,000,000 sites
  - Today: $130.3 Billion projected in ‘06

- **The F-22 Raptor**
  - 1990: 1st prototype flight
  - 1993: 648 - $84M per A/C
  - 1994: 442 - $91M per A/C
  - 1995: 1st A/C Build
  - 1997: 10 Test Flights
  - Today: One operational F-22 squadron
The Other Side of the Coin

- Although never designed to be, the Internet has become critical infrastructure.
  - Its security is in the public interest.
- As a matter of fact, it is the critical infrastructure of critical infrastructures.
  - Gov’t Ops, Gas & Oil, Water Supply, Banking & Finance, Transportation, Electricity, Telecommunications, Emergency Services
- 80-90% of the Internet’s backbone infrastructure is privately owned.
  - With ownership, comes stewardship, and …
  - Stewardship costs money.
A (Brief) Case for Law Enforcement

• The Internet’s security is in the public interest.
  – Who usually protects the public interest (and spends money on it)?

• Free Enterprise v. Governance
  – The “Flood Insurance” Model
  – What happens when the system is abused, or attacked?

Law enforcement can fill the gap between free enterprise and governance.
Crime Comparison

A Physical Crime V. A Cyber Crime

Choice…
But For How Long?

Disclosure Legislation

• Sarbanes-Oxley Act of 2002

• Specter-Leahy: Personal Data Privacy And Security Act Of 2005
  – To date, has not been enacted.

• California SB 1386
  – Over a dozen other States.
Industry’s Concerns

Reasons for Not Reporting Cybercrime to Law Enforcement

What affects your choices?
Law Enforcement’s Interests

• **Infrastructure Protection**
  – Terrorism
  – Information Warfare
  – Criminal activity

• **Crime Intervention, Mitigation and Prevention**
  – Unauthorized Network/Host Access
    • Espionage
    • Theft
    • IPR Violations
    • Sabotage
    • Cut-out
  – Fraud/Prohibited Content
When to Call Law Enforcement

• An attack is potentially targeted at your infrastructure and not your data.
  – Why? Is it a DDoS, or something more complex?
  – Is the DDoS a feint?
  – Where’s the source?

• Your data is compromised.
  – Accessed remotely or physically?
  – Stolen, or destroyed (or both)?
  – Who’s got it?
  – Have you received demands?

• You experience a significant business loss.
  – $5,000.00 (Be creative….)
Why to Call Law Enforcement

A Cybercrime Agent will:

• Combine technical skills and investigative experience.
• Provide local, national and global coverage.
• Apply traditional investigative techniques.
• Provide long-term commitment of resources.
• Integrate law enforcement and national security concerns.
• Provide deterrent effect . . . even if hacker not prosecuted.
• Help to ensure compliance with federal statutes.
Preparing for the Inevitable

An ounce of prevention is worth a pound of cure.

-Ben Franklin

And is certainly better than being pounded by the cure.

-Brad Sheafe
Living on the ‘Net:
Minimizing the Incident, Maximizing the Response

• Develop and implement security policies and procedures.
  – Know what you want to protect, and who will do it.

• Build some walls…
  – Create a perimeter and guard it (border routers, firewalls, IDS, AV, DMZ). Then, inspect the guards (audit policy).

• Educate your users.
  – The importance of security (personal & corporate data/devices), strong passwords, encryption, etc.
Living on the ‘Net:
Minimizing the Incident, Maximizing the Response

• Login banners.
  – Put users on notice, you will be watching!
  – Seek legal counsel’s input

• Ensure the security policy is enforced:
  – Log, and secure the logs
    • Logging server, offline storage
  – Monitor
    • IDS, AV, Address, Port & Protocol Analysis (know what’s weird)
  – Test
    • Run the occasional IT “fire drill”
Living on the ‘Net:
Minimizing the Incident, Maximizing the Response

• Maintain backups.
  – OS software
  – All important system/user data

• Scrub user accounts upon their departure.

• Develop a solid, well thought-out recovery plan.
  – One accepted by, and involving, all necessary levels of management.
Post-Incident Evidence Handling:
It Might Not Make the Case, but It Sure Can Lose It

• If possible, freeze the machine for forensics.
  – No? Then freeze the storage (drive/RAID).
  – Still no? Make an image.
  – Last resort: incident handler’s notes

• Secure the logs
  – Firewall, IDS, AV
  – Any server facing the ‘net (RADIUS, email, web, etc.)
  – Victim server/host (Windows “Events”)

• Secure the backups
  – Determine “last known good” and make copies
When the Agents Arrive...

- They will *participate* in the investigation, not take it over.
- They will want to:
  - Talk to someone who knows the security policy.
  - Talk to someone who knows what happened.
  - Talk to someone who knows the network.
  - Acquire “Best Evidence”
    - Digital Forensics
    - Logs
    - Backups
- **Identify the organization’s POC(s) for the investigation.**
However, They Won’t...

- Take over your network.
- Become involved in civil action.
  - But a companion criminal investigation may be possible.
- Provide you with classified investigative information.
  - Information that would damage national security if released.
- Provide investigation-related information to the media.
- *May not* react with the speed you want or expect.
Are We Successful?

Were you satisfied with the actions of law enforcement?

Source: 2005 FBI Computer Crime Survey

- Yes 85.5%
- Not applicable (We did not report a computer security incident) 6.0%
- Not sure yet 4.6%
- No 3.9%
Questions?
SA Brad Sheafe
bradlee.sheafe@ic.fbi.gov
Office: 217-353-7216
Cell: 217-841-6897