



CCIPS



## Incident Response and the Role of Law Enforcement

Kimberly Kiefer  
Computer Crime &  
Intellectual Property Section  
Department of Justice

1

---

---

---

---

---

---

---

---



CCIPS

## Computer Crime & Intellectual Property Section (CCIPS)



- DOJ's Experts on Cybercrime
- Prosecute cybercrime/IP
- Support and train the nationwide network of cybercrime-savvy prosecutors
- International policy

2

---

---

---

---

---

---

---

---



CCIPS

"The most important conclusion one must draw from the survey remains that the risk of cyber attacks continues to be high."

-- 2003 CSI/FBI Computer Crime Survey (8th Annual)

"Governments need to implement a criminal justice system that will deter hackers."

-- Steve Ballmer  
April 7, 2004

3

---

---

---

---

---

---

---

---



## Agenda

- Law enforcement's dual role
- Myths/concerns of reporting
- Success stories
- Working with law enforcement
- And benefits!

---

---

---

---

---

---

---

---



## **Law Enforcement's Dual Role**

### (1) Responding to Security Incidents

- Preserving digital evidence that can be used to track and identify an intruder.
- Identifying perpetrators after a cyber incident to help determine the appropriate governmental response (e.g., demarche or prosecution).




---

---

---

---

---

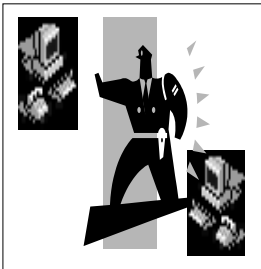
---

---

---



## **Law Enforcement's Dual Role**



### (2) Preventing future security incidents

- Prosecuting computer intrusion cases to discourage would-be intruders
- Training prosecutors and investigators
- Coordinating with companies to improve their security and intrusion detection capabilities.

---

---

---

---

---

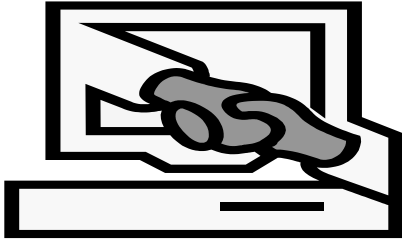
---

---

---



## We need you to share!



---

---

---

---

---

---

---

---



## Victim reporting - statistics

- No reliable statistics – under-detection and under-reporting
- 2003 CSI/FBI Computer Crime Survey
  - 30% reported intrusions to law enforcement
  - Consistent with past five years
- DOD Tiger Team Attacks
  - 8,932 computers attacked, 7,860 broken into
  - 390 detected the attack
  - Only 19 reported

---

---

---

---

---

---

---

---



## Reasons for not reporting

- Negative publicity
  - 70%
- Competitors would use to advantage
  - 61%
- Unaware that could report
  - 53%
- Civil remedy seemed best
  - 56%

---

---

---

---

---

---

---

---



CCIPS

### Concern #1 – Publicity - YIKES!

“If it’s out, competitors will use it against me!”

But, law enforcement tries to be discrete with company information.

And, the fact of the attack may be learned of through other sources.



---

---

---

---

---

---

---

---



CCIPS

### Concern #2 - Competency

“Law enforcement won’t understand intrusions”

But, number of law enforcement agencies prepared to respond has increased at the national, state, and local levels!



---

---

---

---

---

---

---

---



CCIPS

### Concern #3: Hackers will Target Me!

“If they know I’m vulnerable, they’ll attack me again ...”

But, Harvard University study: companies that share data about network attacks are less attractive targets and thus less likely to be attacked!

And, companies that share hinder hacker’s ability to attack other systems

And, “This intruder’s in my system and keeps reappearing every few months!”

---

---

---


---

---



---

---

---

 **CCIPS**

**"I don't know who to call"**

13

---

---

---


---

---

---

---

---

 **CCIPS**

**Who to call?**

- Local law enforcement (sheriff, police)
- Cybercrime investigatory units
  - G-8 Network of 24/7 Contacts
  - Over 35 countries are members
- Computer crime prosecutors
  - High-tech crime units
- CERTs (after incident)

14

---

---

---


---

---

---

---

---

 **CCIPS**

**"I didn't know I could report that"**

When to report: If it looks like criminal activity, consider getting law enforcement involved.

Some indications that the incident involves criminal conduct include:

- An unauthorized user logged into the system
- Abnormal processes are running on the system that use an abnormally high amount of system resources
- A virus or worm has infected the system

15

---

---

---

---

---

---

---

---



## Success Stories

**Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion (July 1, 2003)**

**Hacker Sentenced to Four Years in Prison for Supervising Criminal Enterprise Dedicated to Computer Hacking, Fraud and Extortion and Victimizing Glen Rock Financial Services Company**

---

---

---

---

---

---

---

---



## Success stories

**Cyber Sleuthing Snares Suspected Serial Killer**

JIM SUHR  
Associated Press Writer

**ST. LOUIS** - Perhaps it was cockiness that got the best of Maury Troy Travis. Maybe it was his naivety about cyberspace.

Investigators say Travis didn't emerge as a suspect in the killings of black prostitutes around St. Louis until he sent a computer-drafted letter to the St. Louis Post-Dispatch. More importantly, he sent a map off the Internet.

**Southern California Man Who Hijacked Al Jazeera WebSite Agrees to Plead Guilty to Federal Charges (June 13, 2003)**



---

---

---

---

---

---

---

---

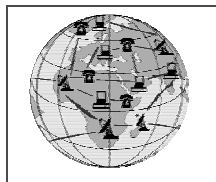


## Benefits to You!

**#1 – Deterrence  
Stop his friend!**



**#2 – Global culture  
of cybersecurity**



---

---

---

---

---

---

---

---



**CCIPS**

**Kimberly B. Kiefer**  
**Department of Justice**  
**Computer Crime & Intellectual Property**  
**Section**

**Phone: (202) 353-4249**

**E-mail: [kimberly.kiefer@usdoj.gov](mailto:kimberly.kiefer@usdoj.gov)**

**DOJ website:**



**[WWW.CYBERCRIME.GOV](http://WWW.CYBERCRIME.GOV)**

Computer Crime and Intellectual Property Section (CCIPS)  
of the Criminal Division of the U.S. Department of Justice

---

---

---

---

---

---

---

---

---

---