


Working with Law Enforcement

CSH5 Chapter 61

David Land




1

Copyright©2014 M. E. Kabay. All rights reserved.

Topics

- Introduction
- Relevant Laws
- Plan Ahead
- Memorandum of Agreement
- Handling Evidence & Chain of Custody
- Issues of Liability
- Ask Law Enforcement to Give Back
- The Knock at the Door
- Keeping Your Operation Running During and Investigation
- Nonelectronic Records and the Insider Threat
- Information Sharing (The Human Factor)


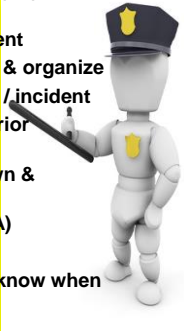


2

Copyright©2014 M. E. Kabay. All rights reserved.

Introduction

- Collaborating with law enforcement (LE) important element of security
- Prepare good relations *before* incident
 - ❑ Know what information to collect & organize
 - ❑ Know whom to call in emergency / incident
 - ❑ Recognition by LEOs based on prior discussions
 - ❑ Rapid response from LE for known & trustworthy people
 - ❑ Memorandum of agreement (MOA)
 - ❑ Join InfraGard (see later)
- Private sector *are not* LEOs – must know when to call in professionals





3

Copyright©2014 M. E. Kabay. All rights reserved.

Relevant Laws (1)

- Work with corporate counsel
 - ❑ Identify state and federal laws applying to jurisdiction
- What must be reported (Exhibit 61.1)
 - ❑ Intrusions / attacks on major networks
 - ❑ Intrusions / attacks resulting in \$\$\$\$ losses
 - ❑ Suspected state-sponsored / industrial espionage
 - ❑ Child pornography
 - ❑ Email or other digitally transmitted threats
 - ❑ Suspected terrorist activities
- Internet fraud *may* be reported to various agencies but *does not have* to be reported





4

Copyright©2014 M. E. Kabay. All rights reserved.

Relevant Laws (2)

- What *not* to report to LE
 - ❑ Port scanning & other non-intrusive activities
 - ❑ Malware (viruses, Trojans, worms, spyware....)





5

Copyright©2014 M. E. Kabay. All rights reserved.

Plan Ahead

- Checklists
- FBI
- USSS & Other Agencies
- USPIS



6

Copyright©2014 M. E. Kabay. All rights reserved.

Checklists




EXHIBIT 61.3 Computer Crime Reporting Checklist: Where to Report

- **Local/State Law Enforcement:** Call your local police department, county sheriff's agency. Do not call 9-1-1. Ask for the agency's high tech crimes unit or, its smaller investigation division.
- **FBI Computer Crimes Squad:** nccs@fbi.gov or 202-324-9164
- **FBI Tips site:** <https://tips.fbi.gov/>
- **US Secret Service Form 401 – Cyber Threat/Network Incident Report:** http://www.secretservice.gov/net_intrusion_forms.shtml
- **Internet Fraud Complaint Center:** <http://www.ifccfbi.gov/index.asp>
- **National White Collar Crime Center (NW3C):** <http://www.nw3c.org/>
- **FTC Identity Theft Web site:** <http://www.consumer.gov/idtheft/index.html>

Source: http://i.i.com/cnwk.1d/i/tr/downloads/home/computer_crime_reporting_checklist.pdf.

CSH5 Chapter 61 p 61.4

7
Copyright©2014 M. E. Kabay. All rights reserved.

FBI




- Lead LE agency for investigating foreign cyberattackers
- Fights criminals, sexual predators, fraudsters
- Jurisdiction over national security investigations



8
Copyright©2014 M. E. Kabay. All rights reserved.

USSS & Other Agencies




- US Secret Service
 - ❑ Counterfeiting, identity theft, computer fraud
 - ❑ Attacks on Treasury Dept
 - ❑ Attacks on other targets not covered by FBI
- Other agencies may be involved
 - ❑ Customs
 - ❑ Commerce
 - ❑ Naval Criminal Investigative Service
 - ❑ US Army Intelligence
 - ❑ US Army Criminal Investigation Division




9
Copyright©2014 M. E. Kabay. All rights reserved.

USPIS




- US Postal Inspection Service
- Enforce > 200 laws affecting or using postal system
 - ❑ Auction fraud
 - ❑ Multilevel marketing scams
 - ❑ Payment or delivery via US mail
 - ✓ Work from home / money laundering




10
Copyright©2014 M. E. Kabay. All rights reserved.

Memorandum of Agreement



- MOA with appropriate law-enforcement authorities
- Prudent measure
 - ❑ Both sides know what to expect
 - ❑ Specific points for details
 - ❑ Discuss public disclosure in advance
- DoJ computer-crime resources (see next slide)



11
Copyright©2014 M. E. Kabay. All rights reserved.

THE COMMON LAW IS THE WILL OF *Manfred* ISSUED FROM THE *Life* OF THE *People*

THE UNITED STATES DEPARTMENT OF JUSTICE

SEARCH THE SITE

HOME ABOUT AGENCIES BUSINESS RESOURCES NEWS CAREERS CONTACT

Home > Agencies > Criminal Division > Organizations > Computer Crime & Intellectual Property Section

CCIPS DOCUMENTS AND REPORTS

Manuals

- Computer Crime & Intellectual Property Section
- About CCIPS
- Press Releases
- Documents and Reports
- Career Opportunities
- Report Crime
- Contact CCIPS
- Criminal Division Home

Manuals

- Prosecuting Computer Crimes manual
- Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations manual
- Prosecuting Intellectual Property Crimes manual

Reports

- IP Enforcement Coordinator's 2010 Annual Report (February 2011)
- FT 2010 Pro IP Act Report
- FT 2010 Joint Strategic Plan on IP Enforcement

Testimony

Archives

GENERAL INFORMATION

COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION

LEADERSHIP

John Lynch
Chief, Computer Crime & Intellectual Property Section

CONTACT

Department of Justice Main switchboard
(202) 514-2000

STAY CONNECTED

Sign up for E-Mail Updates


Subscribe to News Feeds

Facebook MySpace Twitter YouTube

<http://www.justice.gov/criminal/cybercrime/documents.html>

Handling Evidence & Chain of Custody

- Examine media systematically
- Keep detailed notes about possible evidence
- Document all procedures and processes
 - ❑ Especially note variations/deviations from standards
- Mark (label) all output from exploratory processes
 - ❑ Unambiguous
 - ❑ Consistent with law-enforcement agency's standards
- Note resources on previous screen shot
 - ❑ *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*
 - ❑ *Prosecuting Computer Crimes*
 - ❑ *Prosecuting Intellectual Property Crimes*



13 <http://www.justice.gov/criminal/cybercrime/documents.html>

Issues of Liability

- Keep track of discovery, theft or damage of
 - Proprietary information
 - Business-sensitive information
 - Export-controlled information*
 - Downloaded copyrighted music/videos
 - National-defense information




*Export Administration Regulations (EAR)
 Bureau of Industry and Security, US Department of Commerce
<http://www.bis.doc.gov/policiesandregulations/ear/index.htm>

14

Ask Law Enforcement to Give Back


- LE may ask for all conceivable evidence
- Can also provide services
 - ❑ Training for key personnel
 - ❑ Information on crimes
 - ❑ Suggestions for combating crimes



15

The Knock at the Door

- Prepare for unannounced appearance of LE with warrant
- Stay cool
- Express willingness to comply/ cooperate
- Read warrant carefully
- Inform upper management & legal counsel
- Help officers to secure evidence; try to get backups if possible/ necessary for business continuity
- If servers to be searched/seized, get sysadmins involved to prevent data loss & operational damage
- Rarely is entire network brought down
- Retain "officer's return" listing all seized property



16


Keeping Your Operation Running During an Investigation

- Schedule meetings for continuity of operations & test plans before anyone knocks on your door with a warrant
- See if outages can take place after peak processing hours
- Be sure logs/audit files easily accessible for LEOs
- Never allow removal of data without backup! Arrange BU strategies to include possibility of removal by LEOs
- Limit discussion among uninvolved personnel (reduce wasted time, worry, disruption)
- Maintain open communications with LEOs – establish good relations *before* incident
- Encourage on-site bit-for-bit copies of data in real time at all times or at least schedule for non-peak hours (thus avoiding loss of data when the primary disks removed)

17

Non-electronic Records and the Insider Threat


- More than half of computer crimes thought to be committed by insiders
- Maintain careful archives of surveillance data
 - ❑ Paper sign-in sheets, surveillance video, proximity-card records, access-control
 - ❑ Anomalies may highlight collusion or other criminal activity
 - ✓ Theft of user credentials
 - ✓ Unauthorized transfer of data-storage devices
- Some crimes are *cold* cases discovered [long] after incident occurred – records valuable



18

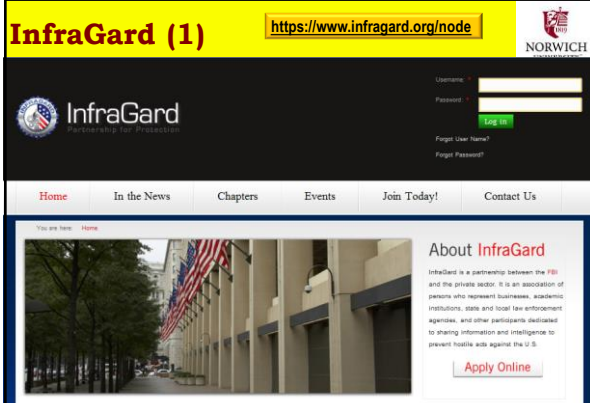
Information Sharing (The Human Factor)

- Improved cybercrime training in many LE agencies
- InfraGard
 - ❑ Information-sharing organization
 - ❑ Industry/academia/government & LE
 - ❑ Many open meetings
 - ❑ Some member-only discussion groups & meetings
 - ❑ Background check for formal membership
 - ❑ >60 chapters across USA (Mar 2014)
 - ❑ 54,677 members (2013-03-12 – couldn't find later data)
- See next slides



<https://www.infragard.net/about.php?mn=1&sm=1-0>

InfraGard (1) <https://www.infragard.org/node>



20

InfraGard (2) <https://www.infragard.org/node>

16 Critical Infrastructures

 Chemical Sector	 Financial Services Sector
 Commercial Facilities Sector	 Food and Agriculture Sector
 Communications Sector	 Government Facilities Sector
 Critical Manufacturing Sector	 Healthcare and Public Health Sector
 Defense Industrial Base Sector	 Information Technology Sector
 Dams Sector	 Nuclear Reactors, Materials, and Waste Sector
 Emergency Services Sector	 Transportation Systems Sector
 Energy Sector	 Water and Wastewater Systems Sector

21

Find a Chapter Near You



With over 60 chapters, InfraGard has a chapter for you to belong to. Chapters conduct local meetings pertinent to their area.

<http://preview.tinyurl.com/19y826d>

22

Paranoid Conspiracy Theories About InfraGard

- Try < infragard conspiracy > using Internet search engine for lunatic beliefs:
 - ❑ InfraGard members have shoot-to-kill authorization (!) [not true]
 - ❑ Special privileges (!!)
 - ❑ Early warnings in emergencies (!!!) [not true]
 - ❑ InfraGard members snoop on neighbors!!!! [not true]
- See M. E. Kabay's "InfraGard is not a deodorant" < http://www.mekabay.com/nwss/406_infragard.pdf > [Originally published in 2005 in *Network World Security Strategies*]

23

DISCUSSION

24