Law, Investigations, and Ethics

Ed Crowley CISSP

‘05

Topics

- Computer Crime
- Computer Laws
- Investigations
- Computer Ethics
- Crime determination
- Evidence preservation
- Investigation basics
- Legal liabilities.

Expectations

- A security professional is expected to know and understand:
  - What laws apply to computer crimes
  - How to determine if a crime has occurred
  - How to preserve evidence
  - Basics of conducting an investigation
  - Liabilities under the law

Potential Computer Crimes

- Denial of Service
  - (DoS and DDoS)
- Password theft
- Network Intrusion
- Emanation Eavesdropping
- Social Engineering
- Illegal Content
- Fraud
- Privacy Violations
- Intellectual Property Violations
- Software Piracy
- Malicious Code
- Spoofing
- Information Warfare
- Espionage
- Masquerading
- Embezzlement
- Traditional Crime Facilitated by a computer

Examples

- Feb 2000, Yahoo, Amazon, and ZD-Net, DDOS
- Oct 2000, Microsoft source code theft
- 1989, Kevin Mitnik IP theft
- 1988, Robert Morris Internet Worm

Legal Issues

- Jurisdictional challenges
  - State vs Federal Laws
  - International Scope?
- Rapidly changing environment
  - Case Law is dynamic
  - International LE is forming agreements

Existing legal systems

- Common Law
  - US
  - UK, Australia, and Canada
- Civil or Code law
  - France, Germany, Quebec
- Socialist legal Systems
- Islamic or other religious law

Common Law

- Compiled either as:
  - Case Reporters in chronological fashion or
  - Case Digest arranged by subject matter.
- Three Common Law Categories
  - Criminal Law
  - Civil Law
  - Administrative/Regulatory Law

Common Law Categories

- Criminal
  - Concerned with individual conduct that violates laws enacted for the protection of the public
- Civil (Tort)
  - Concerned with a wrong inflicted upon an individual or organization that results in damage or loss
- Administrative
  - Standards of expected performance and conduct

U. S. Law

Involves three government branches.

- Legislative branch makes
  - Statutory laws
- Administrative agencies makes
  - Administrative laws
- Judicial branch makes
  - Common laws

Statutory Law Format

- Format includes:
  - Code Title Number
  - Abbreviation of the Code
  - Statutory section
  - Date of the edition

Statutory Law

- Collected as session laws
  - Arranged in order of enactment or as statutory codes.
- Arranges laws according to subject matter. For example:
  - Title 12 Banks and banking
  - Title 15 Commerce and Trade
  - Title 18 Computer Fraud and Abuse
  - Title 26 Internal Revenue Code
  - Title 49 Transportation

Administrative Law

- Administrative laws are arranged either:
  - Chronologically in administrative registers
  - By subject matter in administrative codes.
- At the Federal level, arrangements are called:
  - Federal Register
  - Code of Federal Regulations.

Federal Computer Fraud and Abuse Act, 1986

- Title 18, U.S. Code, 1030, outlaws accessing federal interest computers (FIC) to :
  - Acquire national defense information
  - Obtain financial information
  - Deny the use of the computer
  - Affect a fraud
- Also outlaws:
  - Damaging or denying use of an FIC thru transmission of code, program, information or command
  - Furthering a fraud by trafficking in passwords

Electronic Communications Privacy Act

- Title 18 U. S. Code 2510
- Forbids trespass by all persons and businesses, not just government, where they "obtain or alter data, or prevent authorized access"
- Prohibits not just unauthorized intercept of messages, but unauthorized access to stored messages
  - Covers both voice and data (text or images)
  - Does not require intent to defraud
  - Does not require and specified minimum dollar value of damages
- One year in prison and US$ 250K fines if for personal or commercial gain or maliciously

Patriots Act, 2001

- After 9-11, expands reach of law enforcement in efforts to pursue or capture terrorists.
- Authorizes interception of wire, oral, and electronic communications relating to terrorism and to computer fraud and abuse.
- Authorizes sharing of criminal investigative information

Information Privacy Laws

- Goal is the protection of information on private individuals from intentional or unintentional disclosure or misuse.

European IP Laws

- Without consent, information may not be disclosed.
- Records should be accurate and up to date.
- Data should be used for the purposes for which it was collected.
- Individuals are entitled to their reports.
- Transfer of personal information from the EU to the United States when equivalent personal protections are not in place is prohibited.

Kennedy-Kassenbaum, 1996

- Health Insurance Portability and Accountability Act (HIPAA)
- Addresses issues of health care privacy and plan portability in the US.
- First federal policy to govern the privacy of health information in electronic form.

HIPAA

- Addresses:
  - Rights of the individual over information about them
  - Procedures for the execution of such rights
  - The uses and disclosures that should be authorized
- Entity must have in place:
  - Standard Safe Guards - must have appropriate administrative, technical and physical safeguards
  - Implementation of Standard Safe Guards - A covered entity must protect health care information from intentional or unintentional disclosure

HIPAA

- Defines Four Security Categories:
  - Administrative procedures
  - Physical safeguards
  - Technical data security services
  - Technical security mechanisms
- Compliance date for HIPAA Standards is April 14, 2003.

Graham-Leach-Bliley, 1999

- Regulates sharing of personal information about individuals who obtain financial products or services from financial institutions.
- Attempts to inform individuals about financial institution's privacy policies and practices.
  - Consumers can make choices about financial institutions with whom they wish to do business.
- Opt-out option of how financial institutions use and share the consumers personal information.
  - aka Financial Modernization Act

Sarbanes-Oxley Act 2002

- Address many data retention and preservation issues arising from the Enron and Arthur Andersen debacles.
  - Mandates retention of electronic documents
  - Imposes strict criminal penalties for altering or destroying records, including those kept in electronic form
  - Mandates production of electronic records and other documents when summoned by the new Oversight Board.

Sarbanes-Oxley Act 2002

- Section 802 imposes fines up to $25 million and/or imprisonment of up to 20 years against “whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence” any government investigation or official proceeding.

Sarbanes-Oxley Act 2002

- Section 103 requires public accounting firms to “prepare, and maintain for a period of not less than 7 years, audit work papers and other information related to an audit report, in sufficient detail to support the conclusions reached in [the audit report].”

Computer Crime Challenges

- Rules of Property
  - Digital information lacks tangible assets
- Rules of Evidence
  - Lack of Original Documents
- Threats to Integrity and Confidentiality
  - Beyond normal definition of a loss
- Value of Data
  - Difficult to Measure.
- Terminology:
  - Statutes have not kept pace. Is Computer Hardware "Machinery"? Does Software qualify as "Supplies?".

More Computer Crime Challenges

- Crimes may be hard to define
- Compared with rapidly changing technology, laws evolve slowly.
- Multiple Computers may be:
  - Object of a Crime: Target of an Attack
  - Subject of a Crime: Used to attack (impersonating a network node)
  - Medium of a Crime: Used as a Means to Commit a Crime (Trojan Horse)

Prosecution Difficulties

- Potential lack of understanding
  - Judges, Lawyers, Police, Jurors
- Potential lack of tangible evidence
- Forms of Assets: e.g., Magnetic Particles, Computer Time
- Many perpetrators are juveniles
  - Adults may not take juvenile crime seriously

Intellectual Property Laws

- Patent
  - Provides owner with a legal right to exclude others from practicing the invention
- Copyright
  - Protects “original works of authorship”
- Trade Secret
  - Secures confidentiality of proprietary information
- Trade Mark
  - Establishes a word, name, symbol, color, sound, product shape, device, or combination of these that will be used to identify goods and to distinguish them from those made or sold by others

Electronic Monitoring

- Must be conducted in a lawful manner.
  - Consistent
- Organizations monitoring should:
  - Inform all that email is being monitored
  - Ensure that monitoring is uniformly applied
  - Explain what is considered acceptable use
  - Explain who can read e-mail
  - Not provide a guarantee of e-mail privacy
- Without an appropriate policy stating otherwise, employees can reasonably expect privacy.

Computer Security, Privacy, and Crime Laws

- 1996 U.S. National Information Infrastructure Protection Act
  - Address protection of data and systems confidentiality, integrity, and availability
  - Addresses industrial and corporate espionage.
  - Extends the definition of property to include proprietary economic information

Computer Security and Crime Laws

- 1994 U.S. Communications Assistance for Law Enforcement Act
  - Requires communications carriers to make wiretaps possible
- 1994 Computer Abuse Amendments Act
  - Changed federal interest computer to computer used in interstate commerce or communication
  - Includes viruses and worms
  - Includes intentional damage as well as reckless disregard
  - Limited imprisonment for unintentional damage to one year

U.S. Federal Sentencing Guidelines, 1991

- Degree of punishment is a function of demonstrated due diligence (due care or reasonable care) in establishing a prevention and detection program
  - Specifies Levels of Fines
  - Mitigation of fines through implementation of precautions

Liability

- In 1997, the Federal Sentencing Guidelines were extended to apply to computer crime.
- Management has the obligation to protect the organization from losses due to natural disaster, malicious code, compromise of proprietary information, damage to reputation, violation of the law, employee privacy suits, and stockholder suits.

Due Care

- Corporate officers must institute the following protections:
  - Means to prevent the organization's computer resources from being used as a source of attack on another organization's computer system
  - Principle of proximate causation
  - aka Downstream Liability

Criteria

- The criteria for evaluating the legal requirements for implementing safeguards is to evaluate the cost (C) of instituting the protection versus the estimated loss (L) resulting from exploitation of the corresponding vulnerability.
- If C<L, then a legal liability exists.

Computer Security Act, 1987

Requires federal government to:

- Provide security-related training
- Identify sensitive systems
- Develop security plan for sensitive systems
- Developed Sensitive But Unclassified (SBU) designation

Computer Security Act, 1987

Requires federal government to:

- Split responsibility between National Institute of Standards and Technology (NIST) and National Security Agency (NSA)
- NIST
  - Commercial and SBU
- NSA
  - Cryptography and classified government and military applications

OCED/GASSP

- Generally Accepted Systems Security Principles
- Foundation in the Organization for Economic Cooperation and Development (OECD) Guidelines
  - Computer security supports the mission of the organization
  - Computer security is an integral element of sound management
  - Computer Security should be cost effective

OCED and later NIST 800-14.

GASSP

- System owners have security responsibilities outside their organizations
- Computer security responsibilities and accountability should be made explicit
- Computer security requires a comprehensive and integrated approach
- Computer security should be periodically reassessed
- Computer Security is constrained by societal factors

Investigation

- Computer Forensics is the name for the field of investigating computer crime.
- Unique issues associated with computer criminal cases include:
  - Compressed investigation time frame
  - Intangible information
  - Potential interference with the normal conduct of the business

Evidence

- Evidence must be carefully handled and controlled throughout its entire life cycle.
- Chain of evidence must be followed. Includes:
  - Location where obtained
  - Time evidence obtained
  - Identification of individual who discovered it
  - Identification of individuals who secured evidence

Evidence Life Cycle

- Discovery and recognition
- Protection
- Recording
- Collection
- Identification
- Preservation
- Transportation
- Presentation in court
- Return to owner

Evidence Admissibility

- Evidence must be:
  - Relevant
  - Legally permissible
  - Reliable
  - Properly identified
    - Printouts must be labeled with permanent marker
  - Properly preserved
    - Evidence is not subject to damage or destruction

Types of Evidence

- Best evidence -- Original or primary evidence
- Secondary evidence -- A copy or oral description
- Direct evidence -- Proves or disproves a specific act through oral testimony
- Conclusive evidence -- Incontrovertible: overrides all other evidence

Types of Evidence

- Opinions
  - Expert
  - Non Expert
- Circumstantial evidence
  - Inference of information from other, intermediate relevant facts
- Hearsay evidence
  - (3rd party) not generally admissible in court

Hearsay Rule

Key for Computer Generated Evidence

- Second Hand Evidence
- Admissibility Based on Veracity and Competence of Source

- Exceptions: Rule 803 of Federal Rules of Evidence Business Documents created at the time by person with knowledge, part of regular business, routinely kept, supported by testimony.

Hearsay Exceptions

- Computer generated records and other business records fall into this category
- Exceptions if records:
  - Are made during the regular conduct of business and authenticated by witnesses familiar with them
  - Relied upon in the regular course of business
  - Made by a person with knowledge of the records
  - In the custody of the witness on a regular basis

Searching and Seizing Computers

- Jan 2001 DOJ, in the Computer Crime and intellectual Property Sections (CCIPS), published “Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations”
- Comprehensive guide for federal law agents

Export Issues and Technology

- July 2000, U.S. announced a relaxation of its encryption export policy to certain countries.
- “Under the new policy American companies can export any encryption product to any end user in the European Union and eight other trading partners.”

Incident Handling

- Any adverse event that impact an organization's security or ability to do business is an incident.
- Incident Handling
  - Addressed by establishing a Computer Incident Response Team (CIRT).
- Many incidents are the result of incompetent employees, malicious employees, other insiders, accidental actions, and natural disasters.
  - See Carnegie Mellon's CERT

Investigations

- In a corporate environment, investigations should involve management, corporate security, human resources, the legal department, and other appropriate staff members.
- Organizational procedures should define when and how law enforcement will be contacted.

Law Enforcement Liaison

- An appropriate committee needs to:
  - Establish a prior liaison with law enforcement
  - Decide when and if to involve law enforcement
  - Establish computer crimes reporting procedures
    - Establish procedures for handling and processing reports of computer crime
  - Plan for and conduct investigations
  - Involve senior management and others
  - Ensure proper evidence collection

Investigation

- Critical
  - Must determine if disclosure to legal authorities is required by law or regulation
- Without a warrant, private individuals can conduct a search for possible evidence.
- If a private individual is asked by a law enforcement officer to search for evidence, a warrant is required.
  - Individual is acting as a law enforcement agent and different rules apply.

Timing

- Too Early
  - In regard to searching for and gathering evidence, law enforcement investigators are held to a stricter standard than an organization's employees.
- Too Late
  - Improper handling of the investigation and evidence by untrained organization employees may reduce or eliminate the chances for a successful prosecution.
  - Improper handling of information may make it unacceptable as evidence.

Ethics

- Ethics should be incorporated into an organizational policy and further developed into an organizational ethical computing policy.
- Differences Between Law and Ethics:
  - Must vs. Should

IAB Ethics and the Internet

- Access to and use of the Internet is a privilege and should be treated as such by all users of the system.

(ISC)2 Code of Ethics

- Certified Information Systems Security Professionals (CISSPs) shall:
  - Conduct themselves in accordance with the highest standards of moral, ethical, and legal behavior.
  - Not comment on or be a party to any unlawful or unethical act that may negatively affect their professional reputation or the reputation of their profession.

(ISC)2 Code of Ethics

- Appropriately report activity related to the profession that they believe to be unlawful and shall cooperate with resulting investigations.
- Support efforts to promote understanding and acceptance of prudent information security measures throughout the public, private and academic sectors of our global information society.
- Provide competent service to their employers and clients, and avoid conflicts of interest.

(ISC)2 Code of Ethics

- Execute responsibilities in a manner consistent with the highest standards of their profession.
- Not misuse the information in which they come into contact during the course of their duties and they shall maintain the confidentiality of all information in their possession that is so identified.

Questions?

NIST (National Institute of Standards and Technology) Introduction to Computer Security Handbook can be downloaded from:
http://csrc.nist.gov/publications/nistpubs/800-12/

Current Federal Cases
http://www.cybercrime.gov/cccases.html

Dan Ryan's Page
http://www.danjryan.com/papers.htm

New Laws from the International Journal of Digital Evidence
http://www.ijde.org/docs/03_spring_art2.pdf