Law, Investigations, and Ethics

Ed Crowley
ISC2 Key Areas of Knowledge

Understand legal issues that pertain to information security internationally.

1. Computer crime
2. Licensing and intellectual property (e.g., copyright, trademark)
3. Import/Export
4. Trans-border data flow
5. Privacy
ISC2 Key Areas of Knowledge

Understand and support investigations

1. Policy
2. Incident handling and response
3. Evidence collection and handling (e.g., chain of custody, interviewing)
4. Reporting and documenting
ISC2 Key Areas of Knowledge

Understand forensic procedures
1. Media analysis
2. Network analysis
3. Software analysis

Understand compliance requirements and procedures
1. Regulatory environment
2. Audits
3. Reporting
Topics

- Legal Frameworks
- Computer Laws including:
  - HIPAA
  - DCMA
- Ethics
- Computer Crime
- Investigations
- Crime determination
- Incident response and computer forensics
- Evidence preservation
- Investigation basics
- Legal liabilities.
Expectations

- Security professionals need to have an awareness of:
  - Criminal, Civil, and Regulatory Law
  - Legal liabilities
  - Incident response process
    - Investigative process
    - Digital forensics processes
      - Evidence basics

- Behave Ethically
Existing Legal Systems

- Common Law (Judges)
  - US, UK, Australia, and Canada
- Civil or Code law
  - France, Germany, Quebec, South America
- Islamic or other religious law, Middle East, East Africa, Indonesia
- Socialist legal Systems
US Common Law Categories

- **Criminal**
  - Concerned with individual conduct that violates laws enacted for public protection (imprisonment)

- **Civil (Tort)**
  - Concerned with a wrong inflicted upon an individual or organization that results in damage or loss (financial penalty)

- **Administrative (Regulatory law)**
  - Standards of expected performance and conduct
  - (Imprisonment or financial penalties)
From three government branches.

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

- 1974 US Privacy Act
  - Protection of PII on federal databases
- 1980 Organization for Economic Cooperation and Development (OCED)
  - Provides for data collection, specifications, safeguards
  - Trafficking in computer passwords or information that causes a loss of $1000 or more or could impair medical treatment
Laws

1986 Electronic Communications Privacy Act
- Prohibits eavesdropping or interception without distinguishing private/public

1987 US Computer Security Act
- Security training, develop a security plan, and identify sensitive system on govt. agencies

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 (1986)

- 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” (no eavesdropping)
- 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 $250,000 fines if for personal or commercial gain or maliciously
Laws

- 1996 US Economic and Protection of Propriety Information Act Industrial and corporate espionage
- 1996 US National Information Infrastructure Protection Act Encourage other countries to adopt similar framework
- 1996 Health Insurance and Portability Accountability Act (HIPPA)
Health Insurance Portability and Accountability Act (HIPAA)

- Codifies the right of individuals to control and protect their own health information.
  - 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
    - Appropriate administrative, technical and physical safeguards
  - Implementation of Standard Safe Guards
    - A covered entity must protect health care information from intentional or unintentional disclosure
Information Privacy (IP) Laws

Goal

- Protection of information on private individuals from intentional or unintentional disclosure or misuse.
Intellectual Property Laws

Patent
- Grants ownership of an invention and provides enforcement for owner to exclude others from practicing the inventions. (20 years)

Copyright
- Protects the expression of ideas but not necessarily the idea itself
Intellectual Property Laws

Trade Secret
- Something that is propriety to a company and important for its survival and profitability

Trademarks
- Words, names, product shape, symbol, color, used to identify products and distinguish them from competitor products
European IP Laws

- Without consent, information may not be disclosed.
- Records should be accurate and up to date.
- Data should not be used for the purposes other than for which it was collected.
- Individuals 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.
Safe Harbor Privacy Principles

- Framework that allows U.S. entities wishing to do business in the EU to meet the minimum EU privacy controls. Includes:
  - Notice
  - Choice
  - Onward transfer
  - Security
  - Integrity
  - Access
  - Enforcement
Sarbanes-Oxley (SOX) 2002

- Address many data retention and preservation issues arising from Enron/Arthur Andersen.
  - 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.
SOX 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.
SOX 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].”
Electronic Monitoring

- Must be conducted in a lawful manner.
  - Consistent, communicated, punitive, clear

- 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 provide potential for wiretaps
- 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

- 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

- 1997, 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.
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

- Splits federal computer security responsibilities 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
Ethics

- Ethics should be incorporated into an organizational policy.
- Further developed into an organizational ethical computing policy.
- Differences Between Law and Ethics:
  - Must vs. Should
ISC² Code of Ethics Canons

- Protect society, the commonwealth, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals
- Advance and protect the profession.

https://www.isc2.org/ethics/default.aspx
Ethics and Internet (RFC 1087)

Access to and use of Internet is a privilege and should be treated as such.

It is defined as unacceptable and unethical if you for example gain unauthorized access to resources on the Internet, destroy integrity, waste resources or compromise privacy.
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
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

- Through its entire life cycle, evidence must be carefully handled and controlled.
- Chain of evidence must be followed. Includes:
  - Location where obtained
  - Time obtained
  - Identification of discovering individual
  - Identification of securing individuals
  - At all times, positive, secure, evidence possession
Evidence Life Cycle

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

Evidence must be:

- Sufficient – persuasive enough to convince one of the validity of the findings
- Reliable – consistent with fact
- Relevant
- Legally permissible
- Properly identified
  - Printouts must be labeled with permanent marker
- Properly preserved
  - Evidence is not subject to damage or destruction
Evidence Types One

- Best evidence -- Original or primary evidence
- Secondary evidence -- A copy or oral description. Note that copy is not permitted if original is available.
- Direct evidence -- Proves or disproves a specific act through oral testimony. Does not need support.
- Conclusive evidence -- Incontrovertible: overrides all other evidence. Requires no other corroboration.
Evidence Types Two

- Opinions
  - Expert
  - Non Expert
- Circumstantial evidence
  - Inference of information from other, intermediate relevant facts. Cannot stand on its own.
- Hearsay evidence
  - (3rd party) not generally admissible in court
Evidence Rules

- **Exclusionary rule**
  - If evidence isn’t gathered legally, it can't be used.

- **Best evidence rule**
  - Concerns limiting potential for alteration.

- **Hearsay rule**
  - Concerns computer-generated evidence, which is considered second-hand evidence.
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 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
Incident Handling

- Any adverse event that impacts an organization’s security or ability to do business is an incident.

- Incident Handling
  - Addressed by 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
  - Legal department
  - Other appropriate staff

- Organizational procedures should define when and how outside law enforcement will be contacted.
Incident Response Issues

- An appropriate committee needs to:
  - Establish a prior law enforcement liaison
  - 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 acting as a law enforcement agent. 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.
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