

## Class Ten

### Topics:

- **Introduction to Law**
- **Federal Laws & Computer Security**
- **Computer Crime**
  - Evidence
  - Investigation
- **Ethics and the Security Professional**

8/24/2007

Class 10

1

## Basic Legal Concepts

- Common Law vs. Civil Law Jurisdictions
- Common Law
  - Heritage of English legal system
  - More common in former British colonies (including the USA)
  - Tradition of non-statutory law formed by centuries of judicial precedence
- Civil Law
  - Influenced by ancient Roman law
  - Based on written codes, such as the French Napoleonic code
  - Legislation, not the courts, are the source of law
  - Used in Continental Europe, Latin America, and the State of Louisiana and the Canadian Province of Quebec

8/24/2007

Class 10

2

## Basic Legal Concepts

- Types of “Common Law System Categories”
  - Criminal, concerned with individual conduct
  - Civil, concerned with financial awards to compensate injuries
  - Regulatory, standards of performance and conduct
  - Note: not the same as court-made Common Law described previously
- Aspects of Civil Law:
  - Tort Law
  - Contract Law
  - Property Law

8/24/2007

Class 10

3

## Tort Law

- A civil “wrong” (other than breach of contract) for which the law provides a remedy
- Compensation for economic damages:
  - Compensatory damage – actual cost
  - Punitive – intended to punish culpable negligence
  - Statutory – other damages established by law
- Damages are awarded based on “preponderance of evidence”, a less restrictive standard than criminal cases
- Loss of liberty (jail, imprisonment) NOT part of tort law redress
- Types of Tort
  - Negligence - Harm resulting from lack of due care on the part of another. Requires finding fault.
    - Breach of “Due Care” duty, resulting in economic harm
  - Strict Liability - Liability without finding fault for injuries caused by a product

8/24/2007

Class 10

4

## Tort Law and Computer Security

- Invasion of Privacy Tort (an injury to a "natural person")
  - Appropriation of a person's name or likeness
  - An intrusion upon a person's private affairs
  - The publication of information which places an individual in a "false light"
  - The disclosure of private facts about a plaintiff
- Product Liability
  - Software is usually treated as an information conveyance ("a book") rather than a machine, hence applicability of product liability to defective software has been limited
  - Warranty - promise made by manufacturer of a product about its capabilities

8/24/2007

Class 10

5

## Tort Law and Computer Security

- Downstream Liability
  - An attacker compromises one of your systems
  - Your compromised system is then used to attack others, causing damages
  - Are you liable for providing the attacker with an intermediary for attacking their target?
  - Motivation: The intermediary has "deep pockets", the attacker may not!
  - Consider 1999 Distributed Denial of Service attacks against Yahoo!, eBay, etc.
- TJ Hooper case
  - 1930's case, tug on Great Lakes sank
  - Onboard ship radio would have averted accident, though such radios were not the custom
  - Decision : Standard of care in liability may exceed accepted industry practice
  - Satisfaction of common custom may not preclude liability

Downstream Liability is still a "speculative" concept, and has not been supported by case law in the area of computer security

8/24/2007

Class 10

6

## Intellectual Property

- Copyright
  - Last for 75 years (renewable)
  - Easy to get
  - Protects a form of expression, rather than the idea expressed (not a strong protection against re-engineering)
  - "Fair Use" provided to protect academic research and First Amendment issues
  - Computer programs specifically covered under 17 U.S.C. 101 (1980)
  - Gives the author of a work the right to determine who may copy that work
- Trademark and Service Mark
  - Indefinite lifespan
  - Designed to help businesses establish their identities and prevent competitors from mis-leading the public

8/24/2007

Class 10

7

## Intellectual Property

- Patents
  - Last for 20 years (not renewable)
  - Designed to protect innovative industrial processes
  - Difficult to obtain - must prove innovation is new, useful, and non-obvious
  - Protects the idea itself, hence prevents re-engineering or claimed independent invention
  - Traditionally designed to protect machines, processes and substances
- Trade Secrets
  - Indefinite lifespan
  - Commercially valuable information that is kept secret
  - Owner must take "reasonable" steps to protect information
  - Recognizes right of business to control knowledge used in a new technology, and to prevent competitors from obtaining that knowledge improperly
  - Based on a long history of common law, but codified in the Uniform Trade Secrets Act of 1985
  - Traditionally was a civil tort
  - Laws vary from state to state
  - Federal law criminalized theft of trade secrets in 1996 ("Economic Espionage Act")

8/24/2007

Class 10

8

## “Classic” Federal Computer Crime Laws

- Computer Fraud and Abuse Act of 1986 (18 U.S.C. § 1030 )
  - Outlines certain acts relating to unauthorized access to a computer system for which a party can be criminally liable
  - Degree of crime is based on the subject of the access and the intent of the violator
  - Generally criminalizes Denial of Service attacks, including deliberate introduction of viruses into systems
  - Also criminalizes access without authorization, exceeding authorized access, and trafficking in passwords or other access information
  - 1994 amendments broadened the scope of coverage to any computer involved in interstate commerce or communications, not just the original “federal interest computer”

8/24/2007

Class 10

9

## “Classic” Federal Computer Crime Laws

- Computer Security Act of 1987
  - Outlines minimal acceptable practices for protecting sensitive information in federal government computer systems
  - Sensitive information is that whose misuse could affect national interest, conduct of federal programs, or individual privacy (per the Privacy Act) but NOT that covered by existing National Defense criteria
    - Effectively created the “sensitive but unclassified” category
  - Gives NIST responsibility for drafting specific standards and guidelines in this area.
  - Security plans are required of all operators of federal computer systems which contain sensitive information
  - Mandates periodic information security training for operators of federal computer systems which contain sensitive information

8/24/2007

Class 10

10

## “Classic” Federal Computer Crime Laws

- Electronic Communication Privacy Act of 1986
  - Generally prohibits eavesdropping or intercepting message contents
    - Protects against illicit interception of information in-transit
    - Prohibits access to stored communications
  - Exceptions
    - Corporate system/provider
    - Ordinary Course of Business, where employers can intercept communications
    - Consent, Permits interception of communication where one party has given prior consent
    - Stored communications not as stringently protected as are in-transit communications

8/24/2007

Class 10

11

## Current Major Federal Computer Crime Laws

- 1996 Kennedy-Kassebaum Health Insurance Portability Accountability Act (HIPAA)
  - Establishes standards for electronic interchange of health data and health insurance information
  - Requires specific standards for protecting personal health information privacy:
    - Training
    - Physical security
    - Logical access controls
  - Not just of concern for medical establishments – any entity processing health information (insurance claims, etc.) affected

8/24/2007

Class 10

12

## Current Major Federal Computer Crime Laws

- 1999 Gramm - Leach - Bliley Act (GLBA)
  - GLBA mandates that the Federal Trade Commission (FTC) create new regulations that address the privacy and security of customer information, “Standards for Safeguarding Customer Information”
  - Specifically requires:
    - ensure the security and confidentiality of customer records and information
    - protect against any anticipated threats or hazards to the security or integrity of such records
  - Not just of concern for financial institutions – other entities providing financial services may be affected.

8/24/2007

Class 10

13

## Current Major Federal Computer Crime Laws

- Federal Information Security Management Act (FISMA, passed December 2002)
  - Title II of the E-Government Act (Public Law 107-347)
  - Requires each federal agency to develop an information security program protecting operational systems and data
  - Requires reporting to Congress and the Office of Management and Budget on the effectiveness of these programs
  - Requires the Office of Inspector General to independently assess the effectiveness of these programs
- Sarbanes-Oxley Act of 2002
  - Intended to improve corporate governance and accountability, “post-Enron”
  - Section 404 centers around the internal controls of an organization their effectiveness
  - Controls evaluated with respect to common framework (COSO, or “Committee on Sponsoring Organizations” of the Treadway Commission)
  - Mandates internal controls evaluation must be included in annual report
  - Internal controls evaluation includes general controls, such as information security

8/24/2007

Class 10

14

## Investigation - Evidence

- Types of Evidence
  - Direct
  - Circumstantial
  - Judicial Notice
- Forms of Evidence
  - Oral Evidence (direct or hearsay)
  - Documentary Evidence
  - Real Evidence
  - Expert opinion

8/24/2007

Class 10

15

## Computer Records as “Business Record Exemption to Hearsay”

- Business records usually considered a form of hearsay. Not generally admissible, except under specific conditions.
- Federal Rule 803(6) requires that the record be created and maintained in the ordinary course of business:
  - Made at or near the time of the event recorded
  - Kept in the course of a regularly conducted business activity
  - The business made it a regular practice to keep this particular record
  - Kept for a business purpose
  - Process of collecting and recording data is trustworthy
- Federal Rule of Evidence 901 requires authentication of evidence
- You must present the “best evidence” - you can’t use a photocopy when the original exists
- Role of trusted witness (“custodian”) who can testify as to the reliability of the evidence

8/24/2007

Class 10

16

## Computer Records as Evidence

- Chain of Custody:
  - You must be able to demonstrate the record was accurate at the time it was made
  - You must also be able to document the handling of the record since it was made, to the time it was introduced as evidence
  - Must demonstrate chain of possession
- Discovery - prosecution must make evidence available to defense before going to trial
- Protective Order - limits use, disposition of evidence, to protect proprietary or trade secret documents used as evidence
- Forensics: The use of science and technology to investigate and establish facts in criminal or civil courts of law
  - See <http://www.cops.org> for the International Association of Computer Investigative Specialists (IACIS) for more information

8/24/2007

Class 10

17

## Conducting an Investigation

- Document everything you do
- DON'T document or communicate your activities using the same system or network you suspect has been compromised
- Be aware you may need to document damages for insurance purposes, and that results of an investigation may be used in civil as well as criminal trials
- Form a crises management team
- Be aware that prosecution is very time consuming, both the investigation as well as the subsequent trial.
- Once you call in law enforcement, they will be in charge.

8/24/2007

Class 10

18

## Morality and Ethics

- **Legal** - Conformity with the law. Meeting the minimal standards required to avoid going to jail, or otherwise being punished. *What you shouldn't do.*
- **Moral** - Conformity with standards of proper behavior, with respect to values. Basic inherent values internalized within the individual, as a result of their upbringing and training (and perhaps certain personal choices). *What you believe.*
- **Ethical** - Elaborated code of conduct on how to behave morally in certain contexts. Rules and standards which guide behavior. Modified by group standards, peer pressure, and laws. *What you should do.*
- **Is It Ethical?**
  - The Golden Rule. *Would I want someone else treating me this way?*
  - Conformance with core values. *Would my mother (father, spouse, etc.) approve of this?*
  - The Publicity Test. *How would I feel if this was printed in the newspaper? Would the community approve of this?*

8/24/2007

Class 10

19

## What This Means for Security Professionals

- Rule by consent not force
- Fairness is essential for compliance
- Documented standards ("The Law") are important
- Beware of corporate culture
  - Ethical issues at high levels are always reflected throughout
  - Some organizations are "ethically toxic"
  - A few are "downright crooked"
  - Your users are good at "watching their feet" and will ignore formal policies which conflict with management example
- Your own authority must be perceived as legitimate for you to succeed
- Your organization must support legitimate and ethical authority for you to succeed

8/24/2007

Class 10

20

## Components of Typical Ethical Codes

- Support "just" laws and directives
- Avoid even the appearance of conflict of interest
- Practice due diligence
  - Promise only what you can deliver
  - Truthfully state your expertise
  - Report all failings - don't conceal material security weaknesses
  - All conclusions must be based purely on the facts
  - Properly state all risks
- Assist the IS Security community
- Practice discretion