Legal, Regulations, Compliance and Investigations

Domain 9

Overview

This domain addresses general computer crime legislation and regulations, the investigative measures and techniques which can be used to determine if an incident has occurred, and the gathering, analysis, and management of evidence if it exists.

Key Areas of Knowledge

- Understand legal issues that pertain to information security internationally
- Understand professional ethics
- Understand and support investigations
- Understand forensic procedures
- Understand compliance requirements and procedures
- Ensure security in contractual agreements and procurement processes

Agenda

- **Understand legal issues that pertain to information security internationally**
- Understand professional ethics
- Understand and support investigations
- Understand forensic procedures
- Understand compliance requirements and procedures
- Ensure security in contractual agreements and procurement processes

Types of Common Laws

- Civil Law
- Criminal Law
- Administrative (Regulatory) Law
- Intellectual Property Law

Civil (Tort) Law

- **Preponderance of evidence**
- **Damages**
  - Compensatory: Paid for the actual damage which was suffered by a victim, including attorney fees, loss of profits, medical costs, investigative costs, etc.
  - Punitive: Designed as a punishment for the offender
  - Statutory: an amount stipulated within the law rather than calculated based on the degree of harm to the plaintiff. Often, statutory damages are awarded for acts in which it is difficult to determine the value of the harm to the victim.
- **Liability, Due Care, Due Diligence, Prudent Person Rule are all pertinent to civil law , as well as administrative law**

Criminal Law

- **Beyond a reasonable doubt—can be difficult to meet this burden of proof in computer-related crimes**
- **Penalties: Financial, Jail-time, death**
  - Felonies: More serious of the two. Often penalty results in incarceration of at least a year.
  - Misdemeanors: Normally the less serious of the two with fines or jail-time of less than one year.
- **The Goal of criminal penalties is:**
  - Punishment
  - Deterrence

Administrative (Regulatory) Law

- **Defines standards of performance and regulates conduct for specific industries**
  - Banking (Basel II)
  - Energy (EPA Act) of 2005
  - Health Care (HIPAA)
- **Burden of Proof is "More likely than not"**
- **Penalties consist of financial or imprisonment**

Intellectual Property Law

- **Intellectual Property Law**
  - Protecting products of the mind
  - Company must take steps to protect resources covered by these laws or these laws may not protect them
- **Licensing is the most prevalent violation, followed by plagiarism, piracy and corporate espionage**

Intellectual Property Protection

- **Main international organization run by the UN is the World Intellectual Property Organization (WIPO)**
  - Handles complaints and enforcement
- **Trade Secret**
  - Resource must provide competitive value
  - Must be reasonably protected from unauthorized use or disclosure
  - Proprietary to a company and important for survival
  - Must be genuine and not obvious
- **Copyright**
  - Copyright protection lasts for the lifetime of the author plus 70 years or 75 years for corporations
  - Work does not need to be registered or published to be protected
  - Protects expression of ideas rather than the ideas themselves
  - Author to control how work is distributed, reproduced, used
  - Protects the expression of the resource instead of the resource itself
  - Limitations include “First Sale” and “Fair Use”

Intellectual Property

Trademark

- Protect word, name, symbol, sound, shape, color or combination used to identify product to distinguish from others
- Protect from someone stealing another company's "look and feel"
- Corporate Brands and Operating Systems "Logos"
- Internationally protected by the Trademark Law Treaty Implementation Act

Patent

- Protection for those who have legal ownership of an invention
- Invention must be novel and non-obvious
- Owner has exclusive control of invention for 20 years
  - Cryptographic algorithm
- The strongest form of protection
- Published to stimulate other inventions
- PCT (Patent Cooperation Treaty) has been adopted by over 130 countries to provide the international protection of patents
- No organization enforces patents. It is up to the owner to pursue the patent rights through the legal system.

Attacks on Intellectual Property

- Piracy
- Copyright infringement
- Counterfeiting
- Dilution (example: Kleenex, Xerox)
- Cybersquatting
- Typosquatting

Other legal terms

Business Associate

- A business associate performs an action on behalf of the covered entity

Downstream Liability

- It insurers that organizations working together under a contract are responsible for their information security management.

The Law Pertaining to Encryption

Export restriction

- WASSENAAR Agreement, successor to COCOM, makes it illegal to export munitions to terrorist sponsored nations
- Exporting of cryptographic software is allowed to non-government end-users of other countries
- No exporting of strong encryption software to terrorists states
  - Strong encryption is considered any algorithm capable of supporting key sizes of over 40 bits

Import restriction

- In many countries, the import of cryptographic tools with strong encryption requires a copy of the private keys be provided to law enforcement

International Issues

Transborder Issues

- Each country treats computer crimes differently
- Evidence rules differ between legal systems
- Governments may not assist each other in international cases
- Jurisdiction issues

Personal Data Passed Internationally

Transborder Information Flow

- Movement and storage of data by automatic means across national or federal boundaries
- Many European countries have strong restrictions on flow of personal and financial data
  - Bank statements, personal records, mailing lists, Safe Harbor, data haven
- Know laws before transmitting data through different areas
- Route data through other routes, if necessary

Agenda

- Understand legal issues that pertain to information security internationally
- **Understand professional ethics**
- Understand and support investigations
- Understand forensic procedures
- Understand compliance requirements and procedures
- Ensure security in contractual agreements and procurement processes

Different Sets of Ethics

- (ISC)^2 Code of Ethics Canons
- Internet Activities Board
- Generally Accepted System Security Principles (GASSP)
- Generally Accepted Information Security Principles (GAISP)

$(ISC)^2$ Code of Ethics Canons

1. **Protect society, the commonwealth, and the infrastructure**

2. **Act honorably, honestly, justly, responsibly, and legally**

3. **Provide diligent and competent service to principals**

4. **Advance and protect the profession**

   - Note: This is the order of importance and priority in situations of conflict.

Internet Activities Board – RFC 1087

- **Committee for Internet design, engineering, and management**
- **Internet use is seen as a privilege**
- **Deemed unethical:**
  - Purposely seeking to gain unauthorized access to Internet resources
  - Disrupting the intended use of the Internet
  - Wasting resources through purposeful actions
  - Destroying the integrity of computer-based information
  - Compromising the privacy of others
  - Furthermore, involving negligence in the conduct of Internet-wide experiments is “irresponsible and unacceptable.”

GASSP

- Based on Organization for Economic Cooperation and Development (OECD)
- NIST's guidelines on operational and management security issues
- Principles intended to guide organizations when creating new policies, practices and systems
- Committee that develops and maintains these principles for information security on an international level
- Now called GAISP

GAISP Principles

- Supports the mission of the organization
- Integral element of sound management and judgment
- Cost-effective
- Responsibilities and accountability is explicit
- Comprehensive and integrated
- Periodically reassessed
- Constrained by societal factors

Agenda

- Understand legal issues that pertain to information security internationally
- Understand professional ethics
- **Understand and support investigations**
- Understand forensic procedures
- Understand compliance requirements and procedures
- Ensure security in contractual agreements and procurement processes

Computer Crime

- **Tradition crime committed with computer technology**
  - Fraud, child exploitation, copyright infringement, etc.
- **Crime where computer technology is the target**
  - Hacking, DoS, malicious code, etc.
- **Computer Incidental crime**
  - Money laundering, unlawful banking transactions, distribution of pornographic information

- **Who commits crime?**
- **Why is it committed?**
- **How is it committed?**

Why Crimes are Committed – M.O.M.

Motivations

- Who commits these crimes and why
- What do they get out of these acts

Opportunities

- Where do opportunities exist for computer crimes
- When would someone take advantage of these opportunities

Means

- Who has the capabilities to commit these types of crimes

Computer Crime Characteristics

A Process of:

- Identifying suspects
  - Criminal Profiling: Hackers and crackers, Business competitors, disgruntled parties, Political opponents, etc.
  - Modus Operandi (MO) & signature behaviors
- Identify witnesses
- Identify systems
- Identify investigative team
- Identify and collect evidence

Lack of Basic Protection

- Lack of awareness & incident response capability
- Inadequate safeguards
- Insufficient security staff, skill, resources
- Companies do not press charges

Computer Crime Issues

Problems Prosecuting Computer Crimes:

- Complex legal definitions and technical definitions
- Cross-jurisdiction problems
- Lack of understanding and skill
- New types of crimes
- Private sector lack of reporting
- Setting appropriate punishments
- Intangible evidence
- Not viewed as “serious” crimes

Attack Motivations

Grudge

- "Get back" at a company
- Disgruntled employees
- Political reasons

Terrorist

- Using technology to assist in attacks
- Causing harm against another country
  - Patriot Act

International Warfare

Attack Motivations

Financial

- E-commerce and banking on-line may experience
- Loss of funds or financial information

Business

- Competitive intelligence through computer related attacks

"Fun"

- Joy riding attacks

Attacks

Salami

- Skimming a small amount of money with the hopes of not being noticed
- Series of minor computer crimes that are part of a larger crime

Data Diddling

- Altering data before it is input into a program or after it is output

Password Sniffing

- Capture passwords as they travel over a network

Attacks

IP Spoofing

- Use a bogus IP address to hide identity

Dumpster Diving

- Go through trash in hopes of finding useful information

Masquerading

- Hiding one's identity or origin of attack

Attacks

Wiretapping

- Eavesdropping on a conversation – passive attack

Social Engineering

- Pretending to be someone else to uncover information

Information Warfare

- Attacking the information infrastructure of a nation

Agenda

- Understand legal issues that pertain to information security internationally
- Understand professional ethics
- Understand and support investigations
- **Understand forensic procedures**
- Understand compliance requirements and procedures
- Ensure security in contractual agreements and procurement processes

Crime or Mistake?

Violation Analysis

- Process of capturing system activities, repetitive violations, and recurring problems in the hope of uncovering a solution to the visible problem

- Used to uncover if a computer crime is being committed, if there is user error or problem within a program design

Incident Handling

Incident Management

- Detect, Triage, Respond

Incident Response

- Plans and procedures for responding to particular situations

Dealing with Technical Disturbances

- Containing and repairing damage from an incident
- Preventing further damage
- Data used in next risk analysis
- Necessary reporting structure to a centralized entity
- Should be integrated into disaster recovery and contingency planning
- Should be integrated into security awareness

Responding to a Computer Incident

- **Incident Response**
  - Company should plan how to react to a computer crime before it happens
  - If handling in-house, an incident response team must be in place
    - Items the Computer Incident Response Team must have at its disposal
      - List of outside agencies and resources to contact or report to
        - » Computer Emergency Response Team (CERT)
      - List of computer or forensics experts to contact
      - Steps on how to secure and preserve evidence
      - Steps on how to search for evidence
      - List of items that should be included on the report
      - A list that indicates how the different systems should be treated in this type of situation

Computer Crime Investigation

Challenges

- Intangible evidence
  - In form of electronic pulses and magnetic charge
- Unclear definitions of authorized and unauthorized activities
- Complexity of technology
- Computer evidence gathering
- Cooperation of organizations
- Time intensive
- Jurisdiction

Who Should Do The Investigation?

Internal Employees

- Time and resources of individuals
- Limited knowledge of law and forensics
- Information dissemination is controlled

Consultants

- Expensive
- Privacy issues
- Information dissemination is controlled

Who Should Do The Investigation?

Law Enforcement

- Available skilled resources for this investigation?
- Fourth amendment, jurisdiction, Miranda, privacy issues
  - More restrictions than private citizen
- Information dissemination is not controlled

Investigating a Computer Crime

- **Search and seizure has to have probable cause**
  - Fourth Amendment right
  - Warrant is required
- **Exceptions to previous statement**
  - Private citizen not subject to Fourth Amendment rules unless acting as a police agent
  - Citizen may be subject to restrictions of Electronic Communications Privacy Act
- **Computer evidence can be obtained by law enforcement only through:**
  - Subpoena
  - Search warrant
  - Voluntary consent

Collecting Evidence

- Photograph area, record what is on the screen
- Dump contents from memory
- Power down system
- Photograph inside of system
- Label each piece of evidence
- Record who collected what and how
- Have legal department and possibly human resources involved
- Items go to forensics

Forensics

- **Computer Forensics: The discipline of using proven methods toward the collection, preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence.**
- **IOCE and SWGDE are two entities that provide forensics guidelines and principles as follows**
  - All forensic principles must be applied to digital evidence
  - Evidence should not be altered as a result of collection
  - If a person is to access original digital evidence, that person must be trained for such a purpose
  - All activity relating to the seizure, access, storage, and transfer of digital evidence must be fully documented and available for review
  - An individual is responsible for actions affecting digital evidence while that evidence is in their possession
  - Any entity responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles

Five Rules of Digital Evidence

Digital Evidence Must:

- Be authentic
- Be accurate
- Be complete
- Be convincing
- Be admissible

The Forensics Investigation Process

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Decision

Report or Not Report?

Incident Reporting to Law Enforcement

- The team should consult with management before contacting law enforcement and reporting a crime
- Many companies choose not to report computer crime for many reasons
  - Reputation
  - Cost of litigation
- The FBI and Secret Service are responsible for investigating computer crimes

What is Evidence?

- Material offered to the court and jury to prove the truth or falsity of a fact
- Tends to prove directly or indirectly that an individual may be responsible for committing a crime

Chain of Custody

Chain of Custody of Evidence

- Who obtained the evidence and secured it?
- Where and when it was obtained?
- Who had control or possession of the evidence?

Evidence Life Cycle

- Collection and identification
- Analysis
- Storage, Preservation, Transportation
- Present in court
- Return to victim (owner)

Usable Evidence – Proper Collection

- **The most common reasons for improper evidence collection**
  - No established incident response team
  - No established incident response procedures
  - Poorly written policy
  - Broken chain of custody
- **The chain of custody dictates**
  - Document, document, document, etc.
  - All evidence is labeled with information indicating who secured and controlled it
  - Who, What, When, Where, and How

Evidence Requirements

Material

- Must be relevant to case

Competent

- Proper process of collecting and producing evidence

Relevant

- Sensible relationship to findings
- Evidence should prove or disprove a fact

These values are to be determined by a judge

Evidence Types

Best Evidence

- Primary evidence – most reliable
- Original documents – not copies
- Not oral evidence

Secondary Evidence

- Not as reliable as best evidence
- Copies of documents, oral evidence, witness testimony

Conclusive Evidence

- Irrefutable and cannot be contradicted

Evidence Types

Real Evidence

- Also known as associative or physical evidence
- Tangible objects

Direct Evidence

- Can prove fact by itself
- Does not need backup information
- Information from a witness's five senses – usually oral testimony

Corroborative Evidence

- Supporting evidence to prove a fact or point
- Supplementary tool

Evidence Types

Opinion Evidence

- Witness testifies and gives opinion
- Expert witness giving educated opinion

Documentary Evidence

- Business records, manuals, printouts
- Most evidence submitted is documentary

Circumstantial Evidence

- Used to assume the existence of another fact
- Used so jury will assume the existence of a primary fact
- Cannot be used alone to directly prove a fact

Evidence Types

Demonstrative Evidence

- Aids jury in their understanding of a concept
- Experiments, charts, steps of a crime, computer animation

Hearsay Evidence

- Oral or written evidence
- No firsthand proof of its reliability or accuracy
- Computer-generated evidence
- Electronic bit is original and printed version is copy
- He said she said

Exception to Hearsay Rule

- **Business Record Exemption to Hearsay Rule**
  - Business documents can be admitted if they were created in the course of regular business activity
  - Audit trails can ONLY be used if produced during normal course of business
  - What is the “normal course of business”?
    - Documented Standards, Policies, and/or Procedures

- **Accepting Business Records as Evidence**
  - It meets the Business Record Exemption to Hearsay Rule
  - The Chain of Custody was maintained
  - It is found to be material, competent, and relevant by a judge

Challenges of Going to Trial

- Judge and jury must be made to understand high-tech crimes
- Must find prosecutor that deals with these cases
- Since jury does not always understand, there is “doubt” and not guilty verdicts
- Less stringent punishments, same as white collar crimes

Suspect's Actions and Intent

Enticement

- Tempting a potential criminal
- Legal and ethical
- Honeypot

Entrapment

- Tricking a person into committing a crime
- Illegal and unethical
- Pointing user to a site and then saying they trespassed

Agenda

- Understand legal issues that pertain to information security internationally
- Understand professional ethics
- Understand and support investigations
- Understand forensic procedures
- **Understand compliance requirements and procedures**
- Ensure security in contractual agreements and procurement processes

Liabilities – who is at fault?

- **Failure of management to execute Due Care and/or Due Diligence can be termed negligence**
  - Culpable negligence is often used to prove liability
- **Prudent Man Rule**
  - Perform duties that prudent people would exercise in similar circumstances
  - Example: Due Care: setting a policy; Due Diligence: enforcing that policy
- **Downstream Liabilities**
- **Integrated technology with other companies can extend one's responsibility outside the normal bounds**

Legal Liability

- **Legally Recognized Obligation**
  - A standard exists that outlines the conduct expected of a company to protect others from unreasonable risks
- **Proximate Causation**
  - Fault can actually be proven
- **Violation of Law**
  - Regulatory, criminal, or intellectual property
- **Violation of Due Care**
  - Stockholders suits
- **Violation of Privacy**
  - Employee suits

Risk Assessment – Legal Methodology

- **Balance probability and gravity of possible injury and the cost of the necessary countermeasures to avoid injury**
- **Assess potential loss**
  - Financial
  - Customers
  - Legal exposure
- **If cost of countermeasure is less than the loss potential, you can be legally liable for failure to implement**

Compliance

- **Management is responsible for following industry laws and regulations**
- **Regulatory examples:**
  - Sarbanes-Oaxley (SOX) – pertains to corporate accountability
  - Gramm-Leach-Bliley (GLB) – pertains to banking consumer privacy
  - Basel II – pertains to international banking
- **Audits are used to measure compliance levels**
  - Formal written examination of controls
  - Independent evaluator is essential
  - Continuous evaluation through automated tools
  - Key Performance Indicators (KPI) are metrics that can be used to reflect compliance level

Privacy and Personal Data

PII – Personally Identifiable Information

- Information that can identify, lead to contact, or allow someone to locate the owner of the information

Privacy and identity theft laws vary among jurisdictions

Examples of Privacy Laws

- US – Health Insurance Portability and Accountability Act (HIPAA)
- Canada – Personal Information Protection and Electronic Documents Act (PIPEDA)
- EU – European Union Data Protection Directive
- International (30 member countries) – Organization for Economic Co-operation and Development (OECD)

Privacy Issues – Employee Monitoring

- **Local labor laws related to privacy cannot be violated**
- **Be mindful of the reasonable expectation of privacy (REP)**
  - Gain an employee waiver by signature on policies, etc.
- **Notify of monitoring that may be used, or do not monitor the employees at all**
  - Banner and security awareness
  - Ensure that monitoring is lawful
  - Do not target individuals in monitoring
- **Monitor work-related events:**
  - Keystroke, Cameras, Badges, Telephone, E-mail
- **EU's Seven Principles of Workplace Privacy**

Laws, Directives, and Regulations

- The Sarbanes-Oxley Act (SOX)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Gramm-Leach-Bliley Act of 1999 (GLBA)
- The Computer Fraud and Abuse Act
- The Federal Privacy Act of 1974
- Basel II
- Payment Card Industry Data Security Standards (PCI DSS)
- The Computer Security Act of 1987
- The Economic Espionage Act of 1996
- 1991 US Federal Sentencing Guidelines
- Electronic Communications Privacy Act of 1986

Agenda

- Understand legal issues that pertain to information security internationally
- Understand professional ethics
- Understand and support investigations
- Understand forensic procedures
- Understand compliance requirements and procedures
- **Ensure security in contractual agreements and procurement processes**

Security in Contracts and procurement

- **Ensure security in contractual agreements and procurement processes**
  - All third-party contracts, including any outsourcing agreements should be reviewing for the appropriate security clauses. Software escrow being a key area where SDLC is considered.
  - The procurement process, whether it be for third-party services or for hardware/software should include provisions to maintain the confidentiality, integrity, and availability of the organization's data and systems.

Bringing Things Together

- There are different entities that have developed ethics dealing with the use of computers
- It is important to understand the motives of a crime
- Due care and due diligence have direct relationships with liability
- If a company will handle incidents in-house, they need to develop a team and procedures
- There are different types of evidence for different reasons
- Evidence must always be protected to be presented in court
- Fighting computer crime can be a complex and overwhelming task