Law, Investigations and Ethics

Andrés Velázquez, CISSP, GCFA, BS7799, CSIRT

avelazquez@dodomex.com
Introduction - Law

This domain addresses:
Computer crime laws and regulations that affect organizations personnel.

The CISSP should be able to:
Describe the laws and legal issues that are applicable to computer crime.
Introduction - Investigation

The domain addresses:

The investigate measures and techniques that can be used to determine if a crime has been committed.

Investigation of crime incidents, collection of evidence, and contacting of law enforcement.
Introduction - Ethics

This domain addresses:
Information security ethics as applied to society, (ISC)$^2$ members, and, employees.

The CISSP should understand:
The ethical issues and the code of conduct applicable for the security professional.
Information Protection Requirements - Law

Need to be aware of legal issues, new legislation and regulatory requirements.

Need to provide management with:

- Assurance of compliance with legal requirements
- Awareness of legal liabilities or areas of possible non-compliance
Information Protection Environment

Law

The environment for law includes all aspects of an organization that pertain to personnel, policy, safety, secure infrastructure, and governing regulations.
Information Protection Environment

Laws

Information Security Related Legal Issues
Major Legal Systems
Intellectual Property Laws
Privacy Laws
Liability of Corporate Officers
Information Security Related Legal Issues

Three types of harm usually addressed in computer crime laws:

- Unauthorized access
- Unauthorized alteration, destruction, or disclosure of information
- Insertion of malicious programming code
Information Security Related Legal Issues

Computer Crime Categories include:

Financial attacks
  • Fraud, credit card theft

Business attacks
  • Competitive intelligence

Military and intelligence attacks

Terrorist attacks
  • “Hactivism”
Information Security Related Legal Issues

Computer Crime Categories include:

Grudge attacks
- Insiders, ex-employees
- Dissatisfied customers

Fun attacks
- “Script Kiddies”
Information Security Related Legal Issues

Computer Crimes and Related Laws
Computer-related crimes and abuses (denial of service)
Viruses and malicious code
Software piracy
Illegal content issues (child pornography)
Wire fraud and mail fraud
Various economic or financial crime laws
Issues involved in developing computer crime laws include:
The definition of property expanded to include electronic information
Unlawful destruction or denial of use is criminalized
Using a computer use to commit, aid, or abet crime is prohibited
Theft of intellectual property is defined
Known authorized use is criminalized
Legislative Approaches to Computer Crime

Issues involved in developing computer crime laws include:
- Complex legal definitions of technical issues
- Legislation without consideration of prosecution requirements
- Private sector lack reporting
- Setting appropriate punishments
International Differences in Computer Crime Laws

Nations differ in view of seriousness of computer crime.
  – Not all countries recognize computer crimes as a threat.
  – Nations differ in how they interpret crime and technology issues.
  – Evidence rules differ by legal systems.

Law enforcement technical capabilities vary.
Governments may not wish to assist each other in international cases.
International Differences in Computer Crime Laws

Jurisdictional Legal Disputes

– Computer criminals are not hampered by borders or physical limitations.
– Must be settled under laws of one of the concerned countries.
– Jurisdictional clauses must be included in contracts, such as where the contract is entered into and where the provisions of the contract are performed.
International Differences in Computer Crime Laws

It is very important to gain commonality of legal understandings (harmonization) and an understanding to work together (cooperation) regarding the preventing, detecting, prosecuting, and reporting of computer crimes.
Information Security Related Legal Issues

Legislation is being developed to include:

- Electronic contracts and non-repudiation
- Encrypting import, export, and usage
- Internet violations
- Identify theft
- Network attacks
Information Security Related Legal Issues

Extent of Computer Crime:
“Guesstimates” are that losses are in the $ Billions
- Consulting groups
- Government agencies
- Security associations
- Few computer criminals are caught or punished.
- Both high tech and low tech attacks occur.

Various “watchdog” organizations

- Computer Emergency Response Team – CERT®
- CERIAS
- COAST
- BugTraq
- CIAC
Major Legal Systems

Common Law Systems
The law developed in historical England
It is based on tradition, past practices, and legal precedents set by courts through interpretation of statues, legal legislation, and past rulings.
Legal Systems – Categories of Common Law

Common Law System

- Major important categories include:
  - Criminal Law
  - Civil Law
  - Administrative or Regulatory Law
Legal Systems – Categories of Common Law

Criminal Law

– Individual conduct that violates government laws that are enacted for the protection of the public.

– Violations of criminal law regarding computer crimes can lead to a variety of punishments, including imprisonment, financial penalty, loss of right to work with computers, etc.
Legal Systems – Categories of Common Law

Civil or Tort Law

- Wrong against individual or business that results in damage or loss.
- Violations of civil law regarding computer crimes can lead to financial restitution or compensatory damages. There is no prison time.
Legal Systems – Categories of Common Law

Administrative or Regulatory Law

- Standards of performance and conduct expected by government agencies from organizations, industries, and certain officials or officers.
  - Banks
  - Insurance companies
  - Stock markets
  - Food and drug companies
Major Legal Systems in the World

Civil Law or Code Law Systems

Originally civil law was a common legal system to much of Europe; however with the development of nationalism around the time of the French Revolution it became fractured into separate national systems.

It is based on a comprehensive system of written rules of law and divided into commercial, civil, and criminal codes.
Major Legal Systems in the World

Socialist Legal Systems

It is the legal system that is used in Socialist or Communist countries.

It is based on concepts of economic, political, and social policies of the state.
Religious Legal Systems
It is the law of the clergy, of belief systems, religions, and secret societies.
Special rights are afforded to the clergy over the common people and often the clergy has legal powers that exceed that of the government.
Intellectual Property Laws Subtopics

Intellectual Property typically involves at least four types of laws:

- Patent
- Trademark
- Copyright
- Trade Secrets

One application in information security is determining the legal protections for sensitive information.
Intellectual Property Laws

Patent

• Grants owner a legally enforceable right to exclude others from practicing the invention covered.
• Protects novel, useful, and non-obvious inventions.
Intellectual Property Laws

Trademark

• Any word, name, symbol, color, sound, product, product shape, device, or combination of there that are used to identify goods and distinguish them from those made or sold by others.
Copyright ©

- Covers the expression of ideas rather than the ideas themselves – “origin works of authorship”

Trade Secret

- Proprietary business or technical information that is confidential and protected as long as the owner takes certain security actions.
Privacy Laws could include:
Information privacy – collection and handling of personal data
Medical Records
Communications privacy – protection of mail, phones, email, etc.
Privacy Laws

Importance of privacy protections include:

Globalization – distribution of information beyond a single nation’s borders – world markets.

Tranborder Data Flow – how different nations provide privacy protection of an individual’s information.

Convergent Technologies – technical means of gathering, analyzing, and distributing information.

Data Retrieval Advances – methods of creating vast repositories of personal information.
Privacy Laws

Privacy recognized as fundamental right in many nations.
Privacy Act of 1974 (United States)
United Nations Declaration of Human Rights
The International Covenant on Civil & Political Rights
Existing or newly written constitutions
Organization for Economic Cooperation and Development

European Union Principles
Privacy Laws
European Union Principles

European Union Principles include items such as:

- Data collected fairly and lawfully.
- Data only used for the purposes for which collected and only for reasonable time.
- Persons are entitled to receive a report, on request, on data about them.
Accurate and, where necessary, kept up to date.
One’s personal data cannot be disclosed to third parties unless authorized by statute or consent of individual.
Persons have a right to make corrections to their personal data.
Transmission to locations where “equivalent” personal data protection cannot be assured is prohibited.
Privacy Laws

Models of privacy protection include:

Regulatory Model
Industrial Regulations
Self-regulation
  – Companies/industries –Codes Of Practice
Individual User (Self Protection)
  – PGP and other self-protections
Privacy Laws

Privacy issues include items such as:
Employee electronic monitoring
Email monitoring
Document monitoring
Internet activity monitoring
Personally identifiable information (PII)
Privacy Laws
Employee Monitoring Issues

Legal actions that must be taken to perform employee electronic monitoring include:

– Establish policy for use of system and distribute policy to users of the system.
– Notify your employees that you are monitoring.
– Ensure that monitoring is used in a lawful manner such as:
  • Consistent usage applied to all rather than targeting some.
  • Monitor activities that are work-related.
Privacy Laws
Email Policy Contents

For example an email policy might include:
An explanation of the system
A definition of what is acceptable personal use
Who can/cannot read messages (monitoring)
Describe circumstances where managers or security officers might need access
How mail is stored and sent – how long messages are stored and kept in backup log
Allowance or non-allowance of encryption
Liability of Corporate Officers

U.S. Federal Sentencing Guidelines state that senior executives have the responsibility to ensure that their organizations are in compliance with the law.

– Prevent, detect, and report crimes
– Punishments can reach $290 million
– In 1997, computer-related crime was added

Due Care
It is the concept that corporate officers and other with fiduciary responsibilities must meet certain requirements to ensure corporate security.
Liability of Corporate Officers

International applications are:
Applicable to foreign companies currently operating in the U.S.
Changing business environments of nations around the world.
Liability of Corporate Officers

Examples of liability may include:

Computer security breach causing harm
  – Senior managers/officers/directors held responsible

Catastrophic loss – IT disaster
  – VP or IS manager personally liable

Disgruntled stockholders
  – Suing officers/directors for wrongdoing
Liability of Corporate Officers
Negligence

- Failure to implement recommended precautions
- No contingency/disaster recovery plan
- Failure to use anti-virus software

Hiring
  - Failure to conduct background investigation
Liability of Corporation, Officers, Directors, and Employees

Liability and the failure to institute appropriate information security measures

– Expose organization and Board of Directors (individually and personally)
  • Board of Directors fiduciary responsibility to stockholders to protect assets of corporation

– Corporation may also be liable to others
  • Contractually
  • Under doctrines of civil law
Liability of Corporation, Officers, Directors, and Employees

Liability and the failure to follow policy or local laws and regulations

- Expose employees to personal liability.
- Expose corporation to liability for failure to enforce policy.
  - This could result in either criminal or civil charges under common law.
Computer Forensics

Computer forensics: The study of computer technology as it relates to the law.

Forensic Analysis: Examination of material and/or data to determine its essential features and their relationship in an effort to discover evidence in a manner that is admissible in a court of law; post-mortem examination.
Computer Forensics

**Electronic Evidence:** Evidence relating to the issue that consists of computer files, or data, in their electronic state.

**Electronic Media Discovery:** The discoverability of electronic data or files.
Computer Forensics

**Chain of Custody:** A means of accountability, that shows who obtained the evidence, where and when the evidence was obtained, who secured the evidence, who had control or possession of the evidence.

**Rules of Evidence:** Evidence must be competent, relevant, and material to the issue.
Computer Forensics
Guidelines for Electronic Search and Seizure

Keep in mind:
Electronic evidence is fragile
Integrity of the “scene”
Admissibility in court
Only one chance to do it correctly
Electronic evidence and “hearsay”
Source of Evidence
Guidelines for Electronic Search and Seizure

Sources of evidence

- Oral (witnesses
  • Avoid threats
  • Written statement
- Written (original documents)
- Computer generated
- Visual/audio
  • During event
  • After event
Hearsay Rule
Guidelines for Electronic Search and Seizure

Hearsay is second-hand evidence; normally not admissible.

– Value depends on veracity and competence of source.
– Depending on the circumstance, business records may be considered hearsay.
  • No first-hand proof of accuracy, reliability, trustworthiness.
Computer Forensics
Guidelines for Electronic Search and Seizure
Subtopics

Admissibility of computer evidence – it must be:
Relevant
Foundation of admissibility
Legally permissible
Evidence identification and preservation
Computer Forensics
Guidelines for Electronic Search and Seizure

Admissibility of computer evidence – Relevant
Proof that crime occurred
Documentation of events/time frame
Identification of acts/methods
Proof linking suspects – acts/methods
Proof of suspect’s motives
Computer Forensics
Guidelines for Electronic Search and Seizure

Admissibility of computer evidence – *Foundation*

Witnesses that evidence is trustworthy

– Custodian identity and custodian familiarity with IT record procedures
– Description of procedures
– Precautions against errors and error correction
– Reasons why portions of the media was erased
– Collected through normal business methods
– Reason for bypassing some procedures
Computer Forensics
Guidelines for Electronic Search and Seizure

Admissibility of computer evidence – Legally permissible
Avoid illegal acts
– Unlawful obtaining of evidence
– Unlawful search and seizure
– Secret recording (except authorized by court)
– Privacy violations (access to personal data)
– Forced confessions/statements
Computer Forensics
Guidelines for Electronic Search and Seizure

Laws governing the rights of people and ability to obtain computer records
  – Consent or voluntary
  – Legal requirements

Computer evidence can be quickly changed, leaving no traces of information or evidence
Computer Forensics
Guidelines for Electronic Search and Seizure
Subtopics

Admissibility of computer evidence: Evidence
Identification and Preservation

Key Aspects to processing and examining evidence:
– Planning
– Recognition
– Preservation, collection, and documentation
– Classification, comparison, and individualization
– Reconstruction
Planning
Determine what computer equipment to expect.
  – Is it a stand alone or networked system?
  – What cables, packing will be needed?
Determine what assistance may be required from a system administrator or other skilled individuals.
Appoint one person who will be responsible and take charge of all evidence.
Planning – Establish Chain of Custody of Evidence

Appoint one person who will be responsible and take charge of all evidence.

Maintain chain of custody of evidence throughout the evidence life cycle

– Who protected, read, accessed the evidence.
Computer Forensics
Guidelines for Electronic Search and Seizure

Recognize what to seize:
Hardware including peripherals external drives, PDAs, electronic cameras, printers, scanners.
Software
Removable media: DVD’s, floppies, CD’s.
Documentation that is related to the hardware, software, or removable media.
Computer Forensics
Guidelines for Electronic Search and Seizure

Also seize:
Passwords and phone numbers on or near the computer.
Look through trash for printouts or other pieces of relevant evidence.
Log files and electronic trails.
Computer Forensics
Guidelines for Electronic Search and Seizure

Preservation, Collection, and Documentation

Videotape and photograph the scene prior to touching anything.
Photograph, videotape or make detailed notes of the content of the computer screen.
Printout as much as feasible. Sign and date any hard copies immediately.
Take detailed notes and draw diagrams.
Seizing electronic evidence only:

Use a boot disk that starts the system and ensures that the disk has been virus checked.
Lock the suspicious hard drive(s) to prevent inadvertently writing data to the drive.
Note the current date and time.
Make two bit stream images of all the electronic evidence onto new media.
Label, Date, and initial all evidence.
Inventory the contents of all imaged drives. Include the file creation, modification, and changed dates.
Calculate the message digest for all files and disks. Dump contents of RAM or swap files.
Analysis of Evidence

Examine all evidence for common attributes.
Do thorough and systematic analysis of evidence. Take care not to miss or contaminate anything.
Look for characteristics that may indicate known inappropriate activity or unique non-traditional behavior.
Reconstruct damaged or deleted data including free or slack space, binary files, etc.
Computer Forensics
Guidelines for Electronic Search and Seizure

Reconstruction of damaged or deleted data

Make detailed notes.
Recover as much deleted or damaged data as possible.
Search slack, residue, free space, and binary files.
  Determine where the electronic evidence was located in relation to other evidence.
Computer Forensics
Guidelines for Electronic Search and Seizure

Determine the purpose of each piece of electronic evidence (i.e., how it works and how it was used).

Determine when events occurred. Construct a chronology of events including the modified, accessed, or changed time information.
Case Load Reviews

Do regular reviews of outstanding and closed cases:

- Review documentation and policies
  - Are changes needed to policy?
  - Are incidents being documented and pursued in accordance with policy?
Case Load Reviews

Do regular reviews of outstanding and closed cases:

- Identify skills training needed
- Was the analysis effective and accurate
- Should other individuals or agencies be involved
- Keep senior management informed
Training

Conduct training programs for staff affected by new laws and regulations

– Familiarize management and users with risks to corporation, and personal liability for breaches of legislative or regulatory rulings
Information Protection Requirements - Investigations

Need to conduct reliable investigations that will stand up to scrutiny and cross-examination up to and including in an arbitration or court setting.

Need to ensure that all investigations conducted are thorough and equitable.
Information Protection Environment Investigations

The environment for investigation includes the infrastructure, policies, personnel, techniques, culture, and tools that assist an organization in conducting an investigation.
Investigations
What is an Incident?

**Incident:** An adverse event or series of events that impacts the security or ability of an organization to conduct normal business.

**Event:** An observable occurrence; an aspect of an investigation that can be documented, verified, and analyzed.
Investigations

What is an Incident?

An incident includes, but is certainly not limited to:

Viruses and other malicious code
Hacker attack
Terrorist attack
Insider attack
Competitive intelligence gathering
Unauthorized acts by employees
Employee error
Hardware software malfunction
Motives for Committing Computer and Internet Offenses

The motives for committing computer related offences are the same as for the motives for general crimes. These include but are not limited to:

– Revenge
– Profit or financial need
– Attention
Modus Operandi

Modus Operandi (Method of Operation)

- Three purposes:
  - To protect individual’s identity
  - Ensure success of the crime
  - Assist in the individual’s escape
Modus Operandi

Examining the Modus Operandi of the suspect can provide key information about the party(s) responsible:

– Amount of prior planning that would have been necessary
– Materials used by the suspect
– Any indication of pre-surveillance or intelligence gathering
– Offense location selection
Modus Operandi

Method used to conduct the “attack” (e.g., DDoS, Trojans attached to e-mail)
Any precautionary acts (e.g., using zombied systems as base).
Investigations
Incident Response

Goals of Incident Response:
Provide an effective and efficient means of dealing with the situation in a manner that reduces the potential impact to the organization.
Provide management with sufficient information in order to decide on an appropriate course of action.
Maintain or restore business continuity.
Defend against future attacks.
Deter attacks through investigation and prosecution.
Investigations
Incident Response
Subtopics

Skill sets required to meet the goals:

– Recognition Skills
– Technical Skills
– Response Skills
Investigations

Incident Response – Recognition Skills

Must be able to recognize that an incident has occurred.

- Abnormal activities
- Suspicious activities
- Malicious code activates
- Pattern recognition
- Alarms
Investigations
Incident Response – Technical Skills

Need to possess the sufficient skills to be proficient when dealing with the technology.

– Incident analysis
– Audit trails, event logs
– Incident logs
– Forensic evidence collection and protection
– Counter and/or corrective measures
Investigations
Incident Response – Response Skills

Investigators need:

Sufficient knowledge and training in order to proficiently execute the phases of the response escalation process.
Ability to document and record all information related to the incident
Ability to develop team leadership skills
Incident Response Guidelines for Incident Response

Policies Procedures and Guidelines
- Formally in place prior to an incident Sanctioned by upper management
- Well known to all potential team members
- Need to be enforced
Incident Response
Guidelines for Incident Response

Incident response team members should include representation from various departments, such as:

Information Security
Legal
Human Resources
Public Relations
Communications
Physical Security
Network Security
Network and System Administrators
Internal Audit
Incident Response
Guidelines for Incident Response
Subtopics

Three major sections of the escalation process:

Triage
  – Notification and Identification

Action/Reaction
  – Containment, Analysis, Tracking

Follow up
  – Repair and Recovery, Prevention
Incident Response Guidelines for Incident Response

- Notification
- Identification
- Triage
- Containment
- Action/Reaction
- Analysis
- Tracking
- Repair
- Recovery
- Follow Up
- Prevention
- Feed Back
Incident Response
Guidelines for Incident Response

Triage

– The process of receiving, initial sorting, and prioritizing information to facilitate its appropriate handling.

– Detection
  • Notification of an event.
  • Identifying that an event has become an incident.
  • Determine if incident has violated any policies or laws.
Incident Response Guidelines for Incident Response

Triage – Notification and Identification

Notification and Identification
Alerted to the fact that something has happened.

Monitoring systems
– Intrusion Detection
– Event logs

Alert Function
– Preferably automated

Human decision
– False positives
Incident Response
Guidelines for Incident Response

Action/Reaction

Once an event becomes an incident it has to be dealt with in a legally appropriate manner in order to mitigate or reduce the impact.

– Containment
– Analysis
– Tracking
Incident Response
Guidelines for Incident Response
Action/Reaction - Containment

Containing the incident is vital. This may involve unplugging systems from the network, or from the Internet.

Some incidents are contained over protracted time periods for analysis purposes.

Isolating affected or infected systems
Goal is to minimize the spread and thus the damage.
Incident Response
Guidelines for Incident Response
Action/Reaction - Analysis

Logs
Audit Trails
Information gathering to understand:
  - Who, what, when, where, why, and how
Report to management
Incident Response Guidelines for Incident Response

Action/Reaction - Tracking

Source of the incident
  – Internal
  – External

Point of entry or exit
Must be done in a forensic friendly manner
  – Admissibility

May involve outside organizations
Incident Response
Guidelines for Incident Response
Follow-Up

Follow-Up

– Once the incident has been dealt with it is necessary to conduct a debriefing in order to determine what went well and what did not.

– The findings must be “fed” back into the Incident Response process.
Incident Response
Guidelines for Incident Response
Follow-Up – Repair and Recovery

Reduce the damage
  – Reputation
  – Contractual obligations
  – Financial

Protect environment while recovering
  – Limit services & functions

Repair systems and environment
Incident Response
Guidelines for Incident Response
Follow-Up - Prevention

Prevent similar incidents from occurring
  – Additional security controls
  – Procedures

Active Monitoring of environment
Learning and Education
Incident Response
Guidelines for Incident Response
Sanctions

Management decision based on information provided by the escalation phases

Criminal
Civil

Job Sanctions
– Termination
– Suspension
– Permanent file
Behavioral Evidence: Determining Suspects

Determine suspects

– Who and level in company
– Suspect Check list
  • MOM
    – Means
    – Opportunity
    – Motives
  • Vacation history
  • Prior employment
  • Recent consultants/temps
Behavioral Evidence: Determining Suspects

Victimology (target of the attack)
  – Intended target
  – Collateral target

Target Risk Assessment
  – Why was target chosen
  – What was the risk to the attacker
  – Recent history of target
Behavioral Evidence: Determining Suspects

Crime Scene Characteristics
- Attempts at concealing activities.
- Point of ingress.
- Method of initiation.

Attacker Skill level
- Script kiddie or professional criminal.

Apparent Intent
- Jump off point, Cover up, Exploration, Theft, Vandalism, Damage
Interviewing and Interrogation

**Interviewing**
Purpose
  – Discover information
  – Obtain confession

**Interrogation**
Purpose
  – Obtain evidence for trial
Interviewing and Interrogation

Problem areas

- Disclosing investigation.
- Witness or suspect obtains useful information.
- Witness or suspect might flee before charges or bail.
- Investigator deceived by witness or suspect.
Interviewing and Interrogation

Process
- 1 lead plus 1-2 other team members.
- Prepare topics or questions.
- Put witness or suspect at ease.
- Summarize information.
Interrogation Tips

Interrogator employee senior to employee suspect.

Prepare for interrogation, such as:

- Facts to obtain
- Suspect’s background
- Detailed questions
- Interrogation plan
- Copies of exhibits
Interrogation Tips

Private interrogation place
Allow suspect basic physical comforts
Video tape interrogation
Don’t interrogate alone
Appear calm when interrogating
Supervisor brings suspect without warning
Keep exhibits in folder – present individually
Only law enforcement officers in certain nations required to give rights warning
Enticement

- Intruder lured to selected files
  - Cuckoo's Egg
  - Presence of downloaded files evidence

Entrapment

- Law enforcement induces a crime by a person who was not previously contemplating the crime.
Incident Response
Guidelines for Incident Response

Need pre-approved policy and procedures for dealing with:

– External reporting agencies
– Law Enforcement
Incident Response
External Reporting

Include incident reference numbers
Contact information
Disclosure information
Summary of hosts involved
Description of activity
Log extracts showing the activity
Timezone and accuracy of your clock
Clarify what you would like from the recipient
Incident Response
External Reporting to Agencies

What to report?

Any violations of security policy

– Attempts Denial of Service
– Unauthorized use of a system
– Unauthorized changes to hardware, software, or firmware
Incident Response
Reporting to Law Enforcement

Obtain management permission
Use a single point of contact (e.g., legal dept.)
Provide detailed chronology
Provide all documentation, logs, data, video tapes, etc.
Develop a formal procedure with the assistance of local agency
Investigation Success

Follow-up on investigations:

- Audit investigations
  - Timely resolution of situation
  - Comprehensive and thorough investigation
  - Examine impact on morale of department Effectiveness of interaction with other departments or outside agencies
Training and Awareness

Investigations can be used as a training tool to create awareness of policy, risks and threats to the corporation:

– Use lessons learned
– Explain risk
– Do not harm people’s reputations
– Keep information accurate and meaningful
Information Protection Requirements - Ethics

Need to encourage adoption of ethical guidelines and standards.

Need to inform users through security awareness training about ethical responsibilities.
Information Protection Environment

Ethics

The environment for ethics includes all aspects of an organization – the culture, market, government interface, policies, and procedures that govern employees behavior and interactions with outside vendors, customers, regulatory agencies an law enforcement.
Ethics

Relevant Professional Codes of Ethics include:

– (ISC)² and other professional codes of ethics.
– Professional codes may have legal importance.
Ethics

Basis of and Origin of Computer Ethics

Common good/interest
National interest
Religion
Individual rights
Enlightened self interest
Law Professional ethics/practices
Standards of good practice
Tradition/culture
Ethics
Common Ethical Fallacies

Computer game
Law-abiding citizen
Shatterproof
Candy-from-a-baby
Hackers
Free information
Ethics

Information Security Ethical Responsibilities

Data collectors to data subjects – accuracy and privacy
Data custodians to data owner – availability, integrity, and confidentiality
Data users to owners/subjects – confidentiality, integrity
Data users to system owner – availability, software integrity
System managers to users – availability, integrity
Users to other users - availability
Ethics
Internet Architecture Board (IAB)

Ethics and the Internet (RFC No. 1087)

– Access to and use of Internet is a privilege and should be treated as such by all users.
Ethics
Internet Architecture Board (IAB)

Any Activity unethical and unacceptable that purposely:
Seeks to gain unauthorized access to Internet resources
Disrupts the intended use of the Internet
Wastes resources (people, capacity, computer) through such actions
Destroys the integrity of computer-based information
Compromises the privacy of users
Involves negligence in the conduct of Internet-wide experiments
Ethics
An Ethics Action Plan

Corporate guide to computer ethics
Business and computer ethics policy
Ethics on employee handbook
Computer ethics training campaign
E-mail and other privacy-related policy development
Assurance, Trust, and Confidence Mechanisms

Security Reviews

– Monitoring Employees
– Review of Corporate Culture
  • Fraud detection and awareness
  • Sales Practices
  • Purchasing Procedures
  • Competitive Intelligence Gathering
Assurance, Trust, and Confidence
Mechanisms

Violation Reports

– Complaints from Customers, Vendors, employees investigated thoroughly
– How many complaints received
– Employee turnover in a department higher than average
Information Protection and Management Services

Awareness and Training

– Have regular training programs and management statements to raise ethics consciousness
– Reward ethical practices
1. What type of law has been broken when a person does something that prevents others from using their property (with a resulting loss to the property owner)?

a. Fraud  
b. Malicious mischief  
c. Denial of use  
d. Vandalism  

Respuesta: C
2. Some privacy laws are partly based on the principle that information obtained about a user for some purpose

a. cannot be used for another purpose.
b. must be copied and provided to the user.
c. may only be used with the user's permission.
d. may be reviewed by the user's manager.

Respuesta: A. Esto es aunque el principio no se haya seguido completamente
3. Under the principle of negligence, executives can be held liable for losses that result from computer system breaches if

a. the company is not a multi-national company.
b. they have not exercised due care protecting computing resources.
c. they have failed to properly insure computer resources against loss.
d. the company does not prosecute the hacker that caused the breach.

Respuesta: B.
Due Care = Debido Cuidado
4. If a company has no written policy notifying employees of its right to monitor network activity, what must it do to be in compliance with certain current privacy laws or principles?

a. Monitor only during off hours.
b. Obtain a search warrant prior to monitoring.
c. Not capture any network traffic.
d. Apply for a waiver from Interpol before monitoring.

*Respuesta: C.*
5. To deal more effectively with computer crime, legislative bodies have adopted which of the following strategies?

a. Expanding the control requirements for data privacy.
b. Redefining covert acts to include data privacy.
c. Broadening the definition of property to include data.
d. Increasing the liability of insurance providers over IT resources.

Respuesta: C
6. What is the primary goal of incident handling?

a. Successfully retrieve all evidence that can be used to prosecute
b. Improve the company's ability to be prepared for threats and disasters

c. Improve the company's disaster recovery plan
d. Contain and repair any damage caused by an event.
7. 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 the exploitation of the corresponding vulnerability. Therefore, a legal liability exists when:

a. $C < L$

b. $C < L - \text{(residual risk)}$

c. $C > L$

d. $C > L - \text{(residual risk)}$
8. In the US, HIPAA addresses which of the following?

a. Availability and Accountability
b. Accuracy and Privacy
c. Security and Availability
d. Security and Privacy
9. Which of the following is NOT a Generally Accepted System Security Principle (GASSP)?

a. Computer security supports the mission of the organization
b. Computer security should be cost-effective
c. The conception of computer viruses and worms is unethical.
d. Systems owners have security responsibilities outside their organization.
10. One difficulty with the prosecution of computer crimes is that
a. they do not always fall into traditional criminal activity.
b. they require wiretapping to gather evidence.
c. there is no reliable method of capturing digital data.
d. computer based evidence cannot follow the rules of best evidence.
11. Since disks and other media are only copies of the actual or original evidence, what type of evidence are they often considered to represent?

a. Hearsay
b. Irrelevant
c. Incomplete
d. Secondary
12. Computer-generated evidence is not considered reliable because it is
a. stored on volatile media.
b. too complex for jurors to understand.
c. seldom comprehensive enough to validate.
d. too difficult to detect electronic tampering.
13. The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit is called

a. alteration.
b. investigation.
c. re-direction.
d. enticement.
14. Under what circumstances may the investigator's notebook be admissible in court?

a. When the investigator is unable to be present.
b. When other forms of physical evidence are not available.
c. To refresh the investigator's memory while testifying.
d. When requested by a judge to acquire knowledge of the elements of the offense.
15. With which department MUST the collection of physical evidence be coordinated if an employee is suspected of wrongdoing?

a. Physical Security  
b. Human Resources  
c. Computer Security  
d. Audit
16. Which element must computer evidence have to be admissible in court?

a. It must be relevant.
b. It must be annotated.
c. It must be printed.
d. It must contain source code.
17. Why can computer crime be difficult to investigate?

a. Telecommunications network providers refuse to cooperate.

b. Criminals often hop from network to network.

c. Special equipment is required to detect criminals.

d. Privacy laws forbid wiretapping.
18. A chain of custody of evidence shows who obtained the evidence, who secured it, and
   a. who duplicated it.
   b. who validated it.
   c. who controlled it.
   d. who transcribed it.
19. Which type of communication should an investigator use so that a hacker is not aware of an ongoing investigation?

a. PGP authenticated mail
b. Digitally signed e-mail
c. Shared directory documents
d. Out-of-band messaging
20. Before powering off a computer system, the computer crime investigator should record the contents of the monitor and
a. save the contents of the spooler queue.
b. dump the memory contents to disk.
c. backup the hard drive.
d. remove the hard drive.
21. Why does the collection and submission of computer-related evidence present a significant challenge to the information technology security professional?

a. Magnetic media data retention is poor.
b. Strong encryption limits discovery.
c. System complexity often causes evidence loss.
d. The evidence is mostly intangible.
22. The means of providing accountability and protection for evidence once it has been gathered is called

a. evidence continuity.
b. the chain of custody of evidence.
c. the rule of best evidence.
d. evidence safeguarding.
23. The study of computer technology as it relates to crime is called
a. computer criminology.
b. information systems science.
c. information investigation criteria.
d. computer forensics.
24. After seizing a computer system, the next step in the crime investigation process is
   a. off-load all the data files to tape.
   b. dust the system for fingerprints.
   c. lock the system in the company safe.
   d. make an image copy of the storage media.
25. The Internet Activities Board characterizes which of the following as unethical behavior for Internet users?

a. Writing computer viruses.
b. Monitoring data traffic.
c. Wasting computer resources.
d. Concealing unauthorized accesses.
26. A CISSP candidate signs a non-disclosure statement prior to taking the CISSP examination. Which of the following actions would place the candidate in jeopardy of losing their certification because of a violation of the (ISC)² Code of Ethics?

a. Directing comments to the Board of Directors regarding the content of the training classes.

b. E-mailing comments to CISSP candidates regarding the content of the training class or the exam.

c. Submitting comments on questions at the time of the training and/or the exam.

d. Conduct a presentation about the importance of CISSP certification.
27. According to the Internet Activities Board, which one of the following activities is a violation of RFC 1087 “Ethics and the Internet”?

a. Performing penetration testing against an Internet host
b. Entering information into an active web page
c. Creating a network based computer virus
d. Disrupting Internet communications
28. Which of the following proves or disapproves a specific act through oral testimony based on information gathered through the witness’s five senses?

a. Direct evidence
b. Circumstantial evidence
c. Conclusive evidence
d. Corroborative evidence
29. Something that is proprietary to that company and important for its survival and profitability is what type of intellectual property law?

a. Trade Property
b. Trade Asset
c. Patent
d. Trade Secret
30. Which of the following categories of hackers poses the greatest threat?

a. Disgruntled employees
b. Student hackers
c. Criminal Hackers
d. Corporate spies
31. Computer crime is generally made possible by which of the following?

a. The perpetrator obtaining advanced training & special knowledge
b. Victim carelessness
c. Collusion with others in information processing
d. System design flaws
32. Evidence life cycle does not include which of the following?

a. Protection
b. Identification
c. Recording
d. Destruction
33. Which of the following European Union (EU) principles pertaining to the protection of information on private individuals is incorrect?

a. Individuals have the right to correct errors contained in their personal data
b. Data should be used only for the purposes for which it was collected, and only for a reasonable period of time
c. Transmission of personal information to other organizations or individuals is prohibited
d. Individuals are entitled to receive a report on the information that is held about them
34. Which of the following best defines a Computer Security Incident Response Team (CSIRT)?

a. An organization that provides a secure channel for receiving reports about suspected security incidents

b. An organization that ensures that security incidents are reported to the authorities

c. An organization that coordinates and supports the response to security incidents

d. An organization that disseminates incident-related information to its constituency and other involved parties
35. Which of the following exceptions is less likely to make hearsay evidence admissible in court?

a. Records are collected during the regular conduct of business
b. Records are collected by senior or executive management
c. Records are collected at or near the time of occurrence of the act being investigated
d. Records are in the custody of the witness on a regular basis
36. Which of the following would best describe secondary evidence?

a. Oral testimony by a non-expert witness
b. Oral testimony by an expert witness
c. A copy of a piece of evidence
d. Evidence that proves a specific act
37. Which kind of evidence would printed business records, manuals, and printouts classify as?

a. Direct evidence
b. Real evidence
c. Documentary evidence
d. Demonstrative evidence
38. To understand the “whys” in crime, many it is necessary to understand MOM. Which of the following is not a component of MOM?

a. Opportunities
b. Methods
c. Motivation
d. Means
39. Which of the following statements is not from the (ISC)2 Code of Ethics?

a. All information systems security professionals who are certified by (ISC)2 shall observe all contracts and agreements, express or implied

b. All information systems security professionals who are certified by (ISC)2 shall render only those services for which they are fully competent and qualified

c. All information systems security professionals who are certified by (ISC)2 shall promote and preserve public trust and confidence in information and systems

d. All information systems security professionals who are certified by (ISC)2 shall think about the social consequences of the program they write
40. Under the principle of culpable negligence, executives can be held liable for losses that result from computer system breaches if:

a. The company is not a multi-national company
b. They have not exercised due care protecting computing resources
c. They have failed to properly insure computer resources against loss
d. The company does not prosecute the hacker that caused the breach
41. After an intrusion has been contained and the compromised systems been reinstalled, which of the following need not be reviewed before bringing the system back to service?

a. Access control lists
b. System services and their configuration
c. Audit trails
d. User accounts
42. Why would a memory dump be admissible as evidence in court?

a. Because it is used to demonstrate the truth of the contents
b. Because it is used to identify the state of the system
c. Because the state of the memory cannot be used as evidence
d. Because of the exclusionary rule
43. The Internet Activities Board characterizes which of the following as unethical behavior for Internet users?

a. Writing computer viruses
b. Monitoring data traffic
c. Wasting computer resources
d. Concealing unauthorized accesses
44. Which type of attack would a competitive intelligence attack best classify as?

a. Business attack
b. Intelligence attack
c. Financial attack
d. Grudge attack
45. Which of the following statements regarding trade secrets is false?

a. For a company to have a resource qualify as a trade secret, it must provide the company with some type of competitive value or advantage.

b. The Trade Secret Law normally protects the expression of the idea of the resource.

c. Many companies require their employees to sign nondisclosure agreements regarding the protection of their trade secrets.

d. A resource can be protected by law if it is not generally known and if it requires special skill, ingenuity, and/or expenditure of money and effort to develop it.
46. Which of the following stands for HIPAA?
   a. Hospital Investigation Privacy Agreement Act
   b. Health Insurance Portability and Accountability Act
   c. Health Integrity Patient and Actives Act
   d. Hospital Insurance Private and Accountability Act
47. Which Agency can collect and distribute information about cross-border crimes?

a. US Secret Service  
b. KGB  
c. FBI  
d. Interpol
48. Which agency does not provide international cooperation?
   a. G8
   b. Interpol
   c. European Comission
   d. FBI
49. Which law establishes the standards of performance and conduct from government agencies to organizations?

a. Punitive Law
b. Administrative Law
c. Civil Law
d. Criminal Law
50. In the US, HIPAA addresses which of the following?

a. Availability and Accountability
b. Accuracy and Privacy
c. Security and Availability
d. Security and Privacy
51. Data diddling refers to
a. delete in small pieces existing data
b. alteration of existing data
c. add new data to existing data
d. alteration of deleted data
52. Which of the following threats is not addressed by digital signature and token technologies?

a. spoofing  
b. replay attacks  
c. password compromise  
d. denial-of-service
53. What is called an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim’s system, in order to flood it with REPLY packets?

a. SYN Flood attack  
b. Smurf attack  
c. Ping of Death attack  
d. Denial of Service (DOS) attack
54. Monitoring electromagnetic pulse emanations from PCs and CRTs provides a hacker with what significant advantage?

a. Defeat the TEMPEST safeguards
b. Bypass the system security application
c. Gain system information without trespassing
d. Undetectable active monitoring
55. Which of the following would best define the “Wap Gap” security issue?

a. The processing capability gap between wireless devices and PCs
b. The fact that WTLS transmissions have to be decrypted at the carrier’s WAP gateway to be re-encrypted with SSL for use over wired networks
c. The fact that Wireless communications are far easier to intercept than wired communications
d. The inability of wireless devices to implement strong encryption algorithms