

LAWS AND ETHICS

NOTE*Because the development of new technology usually outpaces the law, cops use embezzlement, fraud, and wiretapping to prosecute computer criminals

Types of Computer Crimes:

Emanation Eavesdropping-Receipt and display of info, which is resident on computers or terminals, through the interception of RF signals. The US Government established a program called **TEMPEST**. Required implementation of shielding.

Social Engineering-Using social skills to obtain info, such as passwords or PIN numbers

Dumpster Diving-Obtaining sensitive data, such as manuals from dumpsters

Information Warfare-Attacking the info infrastructure of a nation

Data-Diddling-modification of data

LAW

There are many types of legal system in the world that differ in how they treat evidence, the rights of the accused, and the role of the judiciary.

Example: The United States

Under the common law system of the US, there are 3 branches. The **legislative** does statutory. The administrative create admin laws. The **judicial** makes common laws.

Statutory Law-Collected as session laws, arranged in order of enactment or as codes, that arrange the laws according to subject matter.

Administrative Law-Arranged either chronologically in admin registers, or by subject matter.

Common Law-Compiled as case reporters in chronological fashion and case digests arranged by subject matter

Criminal Law-Individual Conduct that violates laws enacted for the protection of the public. Punishment can be financial or prison.

Civil Law-Laws about a wrong inflicted upon an individual or organization that results in damage or loss. Punishment CANT include prison.

Admin/Reg Law-Standards of performance and conduct expected by government agencies from industries, organizations, officials, and officers. Violation can result in financial and/or prison.

Intellectual Property Law

Patent-provides owner of the patent with a legally enforceable right to exclude others from practicing the invention

Copyright-Protects original works of authorship

Trade Secret-Maintains confidentiality of business related info. Valuable to business of the owner.

Trademark-Used to distinguish goods from others.

Information Privacy Laws

The EU has defined privacy principles that are more protected than the laws of the US

US Kennedy Assenbaum (HIPPA) Health Insurance Portability and Accountability act-addresses the issues of health care privacy and plan portability in the US. Act states, “no later than the date that is 12 months after the date of the enactment of this act, the secretary of health and human services shall submit detailed recommendations on standards with respect to the privacy of individually identifiable health information.

Electronic Monitoring

Additional personal security issues involve keystroke monitoring, email, surveillance cameras, badges.

- Inform them email is being monitored
- Explain what is considered acceptable use of email system
- Explain who can read the email and how long it is backed up

Enticement-occurs after an individual has gained unauthorized access to a system.

Entrapment-Encourages the commission of a crime that the individual initially had no intention of committing.

Investigation

- Investigators and prosecutors have compressed time frame
- Information is intangible
- Investigation may interfere with the normal conduct of the business of an organization
- Data needed may reside on a computer needed for normal business operations.

Evidence

Specifically, there is a chain of evidence. The following are major components of this chain of evidence:

- Location of evidence
- The time it was obtained
- Identification of person who discovered evidence
- identification of person who secured evidence

EVIDENCE LIFE CYCLE-covers the evidence gathering and application process.

- Discovery and recognition
- protection
- recording
- collection

DON'T REFORMAT HARD DRIVE

Evidence Admissibility

To be admissible in a court of law, evidence must meet certain requirements. The evidence must be relevant, legally permissible, reliable, properly identified, and preserved.

- label with permanent marker
- record serial numbers
- identify OS used
- don't prematurely remove power
- back up hard disk image
- write protect media
- Authenticate the file system by creating a digital signature. SHA

Types of Evidence

Best evidence-Original or primary evidence, rather than a copy

Secondary-a copy

Direct evidence-Proves/disproves a specific act through oral testimony

Conclusive evidence-Incontrovertible; overrides all other evidence.

Opinions: *Expert*-May offer an opinion based on personal expertise/facts

Nonexpert-May testify only as to facts

Circumstantial evidence-Inference of info from other relevant facts

Hearsay(3rd party)Evidence based on personal, first hand knowledge of the witness. Generally not admissible in court. (EXCEPTIONS TO THIS RULE)

Searching and Seizing Computers

FBI and Secret service can seize.

The topics covered include the application of the 4th amendment (Electronic communications and privacy act)

Conducting Investigation

In a corporate environment, an investigation should involve management, corporate security, human resources, the legal department etc.. Important to prepare a plan beforehand on how to handle reports of suspected computer crimes.

If a crime is suspected, it is important not to alert the suspect. A preliminary investigation should be done to determine if a crime has been committed by examining audit record, system logs, interviewing witnesses etc..

It is critical to determine if disclosure to legal authorities is required by law or regulation. US Federal sentencing guidelines require organizations to report criminal acts.

Remember, there are a number of things to consider before issuing outside disclosure. Negative publicity could result in lack of confidence in your company.

In the US, law enforcement personnel are bound by the 4th amendment to obtain a warrant to search for evidence. Private citizens are not held to this, and in some cases, a private individual can conduct a search without a warrant. However, if a private individual were asked by a law enforcement officer to search, a warrant would be required. An exception to the search warrant requirement for law enforcement officers is the Exigent Circumstances Doctrine. Under this, if probable cause is present and destruction of evidence is deemed imminent, the search can go on without a warrant.

Good sources of evidence to keep are telephone records, video cameras, audit trails, system logs, backups, emails, witnesses, and results of surveillance.

..Continued

A standard discriminator used to determine whether a subject may be the perp, is to evaluate whether the person had a MOTIVE, OPPORTUNITY, and MEANS to commit the crime. (MOM)

If the investigation is to be done internally, the suspect should be interviewed to acquire the information and to determine who committed the offense. The interrogation should be planned in advance, and expert help should be obtained in order to conduct interview. Do not give the suspect too much knowledge. Original documents should not be used to conduct the interview to avoid possible destruction of the documents.

Liability

In '97, the Federal Sentencing Guidelines were extended to apply computer crime. Under these guidelines, senior corporate officers can be personally subject up to \$290million in fines if their organizations do not comply with the law.

Management has the obligation to protect the organization from losses due to natural disasters, code, violation of law. Management must follow the prudent man rule that requires officers to perform duties with diligence and care that ordinary, prudent people would exercise under similar circumstances. The officers must exercise due care or reasonable care to carry out their responsibilities.

The computer ethics Ten Commandments

In '92, the Coalition for Computer ethics made this

1. Don't harm other people with computers
2. Don't interfere with other peoples computer work
3. Don't snoop
4. Don't use a computer to steal
5. Don't use a computer to bear false witness
6. Don't copy software
7. Don't use other peoples computer without consent
8. Thou shalt not appropriate other peoples intellectual output
9. Think about consequences of the program you are writing
10. Use the computers in respect for humans

The Internet Activities Board

Access to and use of the internet is a privilege and should be treated as such
Any activity is defined as unacceptable and unethical that:

1. Seeks to gain unauthorized access
2. destroys integrity of computer based info
3. Disrupts use of internet
4. wastes resources
5. Compromises privacy of users
6. involves negligence in the conduct of internet wide experiments

The US department of Health code of fair info practices

1. There must not be personal data record keeping systems whose very existence is secret
2. there must be a way for a person to find out the info that is kept on record about them and how it is used
3. There must be a way for a person to prevent info about them, which was obtained for one purpose, from being used or made available for another purpose without their consent.
4. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use and must take precautions to prevent misuses of that data.