

Motivation and Study Techniques to help you learn, remember, and pass your technical exams!

Cisco
CISSP
CEM
More coming soon...

www.mindcert.com @ Visit us

Subscribe via RSS



Certified Professionals are morally and legally held to a higher standard
Should be included in Organizational computing policy

Conduct themselves with highest standards of ethical, moral, and legal behavior

- Not commit any unlawful or unethical act
- Appropriately Report unlawful behavior

Support effort to promote prudent information security measures

- provide competent services to their employees and clients
- Execute responsibilities with highest standards

Not misuse information in which they come into contact with during their duties

- Internet Activity should be treated as a privilege

Seeks to gain unauthorized access to resources

- Disrupts intended use of the Internet
- Wastes resources
- Unacceptable actions
- Compromises privacy of others
- Involves negligence in conduct of Internet Experiments

The ethical requirements of those working in computer security

IS2 Code of Ethics

Information is intangible

- An investigation will interfere with normal business operations
- May find difficulty gathering evidence
- Experts are required
- Geographic Jurisdictions
- Gathering, control, and preservation
- Computer evidence can be easily modified

Must be followed in order to protect evidence

- Location
- Time obtained
- Identification of individual who discovered
- Components
- Chain of evidence
- Identification of individual who secured the evidence
- Identification of individual who controlled/maintained possession of evidence

Life Cycle

- Discovery and recognition
- Protection
- Recording
- Collect all relevant storage media
- Make image of HDD
- Collection
- Print out screen
- Avoid Degaussing equipment
- Tagging and marking
- Identification
- Store in a proper environment
- Preservation
- Transportation
- Presentation in court
- Return to evidence owner

Evidence must meet stringent requirements

- Related to the crime
- relevant

Obtained in a lawful manner

- Legally Permissible

Not been tampered or modified

- reliable

Identified without changing or damaging evidence

- Properly Identified

Not subject to damage

- Preservation

The investigation of Computer Crime

Original - Best Evidence

Copy - Secondary Evidence

Proves or disproves an act based upon the five senses

- Witness
- Direct Evidence

Inconvertible

- Conclusive Evidence

Overrides all evidence

- Expert
- Opinions
- Non Experts

Inference on other information

- Circumstantial
- Not based on first hand knowledge
- Hearsay
- Exceptions
- Made at or near the time of occurrence of act being investigated

Types of Evidence

- Telephone Records
- Video Camera
- Audit Trails
- System Logs
- System backups
- Good sources of evidence
- Witnesses
- Surveillance
- Emails

Establish liaison with Law Enforcement

Decide when and if to bring in Law Enforcement

Setting up means of reporting computer crimes

procedures

Investigations committee

- Start Internal
- Conducting Investigations

Senior Management

HR

Proper Collection of Evidence



Law as it applies to Information Systems Security

Covers computer crimes, preserving evidence and conducting basic investigations

Many go unnoticed

Two Categories

Crimes against a computer

Crimes using a computer

Denial of Service

Theft of passwords

Network Intrusions

Emanation Eavesdrop pig

Social Engineering

Illegal Content of Material

Porn

Fraud

Software Piracy

Virus

Malicious Code

Trojan

Worm

Spoofing

Information Warfare

Data-Diddling

Modification of data

Terrorism

DDoS of Yahoo, Amazon, ZDNet

Feb 2000

Love Letter Worm

May 2000

Microsoft - Source Code

Oct 2000

Mitnick

1985-1995

Blaster Worm

2003

Well known examples

- 1 Legislative - Makes the Statutory laws
- 2 Administrative - makes the Administrative Laws
- 3 Judicial - Common laws found in court decisions

Three Branches of Government

Made by legislative branch

Held in the United States Code (U.S.C)

Title 18 of the 1992 edition of the U.S.C

Crimes and Criminal Procedures

many computer crimes under this

Title comes first!!!

18 U.S.C § 1030 (1986)

US Computer Fraud and Abuse Act 1986

Addresses Fraud using government computers

Administrative Law

Code of the Federal Register (C.F.R)

Violates government laws for the protection of the people

Criminal Law

Wrong inflicted upon a person or organization

Civil Law

Standards of performance and conduct

Admin/Regulatory Law

Company Law

Intert varies country to country

EU has more protective laws for individual privacy

Personnel Security

Keystroke monitoring

e-mail monitoring

Badges

Magnetic card keys

Electronic Monitoring

Must inform users

Use banners

Apply uniformly

Must be done in a lawful manner

Explain who can read e-mail and how long it is backed up for

No guarantees of privacy

Access Controls may not provide granularity

Access to Internet causes potential problems

Criminal and Civil penalties can be imposed

Effective 21 August 1996

Health Care Issues

HPAA

Addresses

The rights of the individual for people who have information over them

Procedures for the execution of such rights

The uses and disclosures that should be authorized

Occurs after individual has gained unlawful access to a system, then lured into an attractive area "honey pot" in order to provide time to identify the individual

Enticement vs Entrapment

Enticement

Encourages the commitment of a crime that the individual had no intention of committing

Entrapment

Non-Ethical

Generally Accepted Systems Security Principles (GASSP)

Accepted Principles

Not Law

Computer Security Act 1987

US

United Kingdom Misuse Act 1990

Electronic Communications Privacy Act 1986

Protect against eavesdropping

Patent

Exclude Others

17 Years

Trademark

Protects words sounds that present an good or service

Copyright

Protects original works of authorship

Can be used for software

Trade Secret

Propriety technical or business information