

Ethics

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: ethics.pdf*
- ❖ *GNU Free Documentation License*
- ❖ *Version 1.00, 2005-05-27*
- ❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*
- ❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Introduction

➤ Objectives

- Understand what laws apply to computers crimes
- Understand how to determine if a crime has occurred
- Understand how to preserve evidence
- Understand liabilities under the Law

➤ Computer Crime Categories

- Crimes Committed against the computer
- Crimes committed using the computer
- Military and Intelligence Attacks
- Business Attacks
- Financial Attacks
- Terrorist attacks
- "Fun" Attacks

➤ Computer Crimes

- **Salami**
 - Involving subtracting a small amount of funds from an account with the hope that such an insignificant amount would be unnoticed
- **Data Diddling**
 - Alteration of existing data and many times this modification happens before it is entered into an application or as soon as it completes processing and is outputted from an application
- **Excessive Privileges**
 - Occurs when a user has more computer rights, permissions and privileges than what is required for the tasks she needs to fulfill
- **Password Sniffing**
 - Sniffing network traffic in the hopes of capturing passwords being sent between computers
- **IP Spoofing**
 - Manually change the IP address within a packet to point to another address
- **Denial of Services DoS**
 - Denying others the service that the victim system usually provides
- **Dumpster Diving**
 - Refers to someone rummaging through another person's garbage for discarded document
 - Information and other precious items that could then be used against that person or company
 - It is Illegal
- **Emanations Capturing**

- Eavesdropping of the electrical waves emitted by every electrical device
- **Wiretapping**
 - Eavesdropping of communication signals
- **Social Engineering**
 - The art of tricking people and using the information they know unknowingly supply in a malicious way
- **Masquerading**
 - A method that an attacker can use to fool others of her real identity
- **International Economic Espionage**
 - Called also Information Warfare
 - Country perform espionage on another country
- **Grudge Attacks**
 - A disgruntled employee who plants a logic bomb
 - These are attacks to get back at someone or something because they hold a grudge against them.
- **Network Intrusion**
- **Illegal Content of Material**
- **Fraud**
- **Software Piracy**
- **Malicious Code**
- **Destruction or the Alteration of Information**
- **Embezzlement**
- **Terrorism**
- **Well-Know Computer Crimes**
 - **Cuckoo's Egg**
 - Book describing how Cliff Stoll (a student) tracked down 75 cent accounting error in 1980
 - He is the first one who set up a Honeytrap
 - **Kevin Mitnick**
 - **Chaos Computer Club**
 - Freedom of Information across borders
 - Formed in 1981
 - **Phone Phreakers**
 - 2600
 - ♦ Stands for the tone that phreakers used to make free long distance calls
 - ♦ Invented by a Blind man Captain Crunch
 - ♦ He found a whistle that generate 2600 HZ that allowed him to make free calls
 - 414 Gang
 - Blue boxing
 - ♦ A device that simulates a tone 2600 HZ
 - Red boxes
 - ♦ Simulates the sound of coins being dropped into a payphone
 - Black boxes
 - ♦ Manipulates the line voltage to receive a toll-free call
 - **Cult of the Dead Cow**
 - Back orifice Creator
 - Remotely take over Windows 95 , 98
 - **Equity Funding**
 - **Internet Worm**

❖ Investigation Computer Investigation Issues

- **Order for Incident handling steps?**
 - Preparation
 - Identification
 - Containment
 - Eradication
 - Recovery
 - Lessons learned
 - Perphase I Can Erase Red Lines (Adonis)
- **Incident response team**
 - Team should have the following Items
 - - List of outside agencies and resources to contact or report to.
 - - List of computer of 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.
- **Forensics investigation**
 - **1st step**
 - Make a sound image of the attacked system and perform forensic analysis on this copy
 - This will ensure that the evidence stays unharmed on the original system in case some steps in the investigation actually corrupt or destroy data
 - Also the memory of the system should be dumped to a file before doing any work on the system or powering it down
 - Forensics system Should have the ability to:
 - ♦ A.) Validate software and procedures
 - ♦ B.) Authenticate the file system
 - ♦ C.) Conduct a disk image backup
 - ♦ D.) Conduct forensic analysis in a controlled environment
 - **2nd step**
 - Chain of custody
 - ♦ Must follow a very strict and organized procedure when collecting and tagging evidence
 - ♦ All evidence be labeled with information indication who secured and validated it
 - ♦ The chain of custody is a history that shows
 - How evidence was collected
 - How evidence analyzed
 - How evidence was transported
 - How evidence was preserved
 - Chain of custody Include
 - ♦ Location of evidence when obtained
 - ♦ Time evidence was obtained
 - ♦ Identification of individual(s) who discovered evidence
 - ♦ Identification of individual(s) who secured evidence
 - ♦ Identification of individual(s) who controlled evidence
 - **Evidence**
 - Evidence Life cycle Covers
 - ♦ Collection and identification
 - All relevant storage Media
 - Make image of hard disk before removing power

- Print out screen
- Avoid degaussing equipment
- ◆ Storage, preservation and transportation
 - Protect magnetic media
 - Store in proper environment
- ◆ Presentation in court
- ◆ Being returned to victim or owner
- Handling of evidence guidelines
 - ◆ Discovery
 - Discovering the Pyramid
 - ◆ Recognition
 - Recognize what the pyramid to look for
 - ◆ Protection
 - Protect my self while looking for the pyramid
 - ◆ Recording
 - Tape a tape recorder and record any noise
 - ◆ Collection
 - Collect any Egyptian writing or anything with value
 - ◆ Identification
 - Identify the collected Items
 - ◆ Preservation
 - Put the identified items in a Metal Box
 - ◆ Transportation
 - Transport them back home using safe plane
- Type of Evidence
 - ◆ The most common forms of evidence are
 - A.) direct
 - Can prove fact all by itself instead of needing backup information to refer to
 - Direct evidence is oral testimony,
 - The knowledge is obtained from any of the witness's five senses
 - B.) real
 - Also known as associative or physical evidence,
 - Made up of tangible objects that prove or disprove guilt.
 - The purpose of the physical evidence is to link the suspect to the scene of the crime.
 - C.) documentary
 - Evidence is evidence presented to the court in the form of business records, manuals, and printouts, for example.
 - Much of the evidence submitted in a computer crime case is documentary evidence.
 - D.) demonstrative
 - Evidence used to aid the jury.
 - It may be in the form of a model, experiment, chart, or an illustration offered as proof.
 - ◆ Direct
 - Can prove fact all by itself instead of needing backup information to refer to
 - Direct evidence is oral testimony,
 - The knowledge is obtained from any of the witness's five senses
 - ◆ Best Evidence
 - Is the primary evidence used in a trial because it provides the most reliability
 - Is used for documentary evidence such as contracts.
 - ◆ Secondary Evidence
 - Is not viewed as reliable and strong in proving innocence or guilt when compared to best evidence
 - ◆ Conclusive Evidence (The BEST)
 - Is irrefutable and cannot be contradicted

- ♦ Circumstantial Evidence
 - Can prove an intermediate fact that can then be used to deduce or assume the existence of another fact.
 - Is used as a supplementary tool to help prove a primary piece of evidence
 - It cannot stand on its own
- ♦ Corroborative evidence
 - Is supporting evidence used to help prove an idea or point.
- ♦ Opinion evidence
 - When a witness testifies, the opinion rule dictates that she must testify to only the facts of the issue and not her opinion of the facts.
 - Expert
 - Nonexpert
- ♦ Hearsay Evidence
 - Pertains to oral or written evidence that is presented in court
 - Secondhand and has no firsthand proof of accuracy or reliability
- Evidence Admissibility
 - ♦ Evidence must be Sufficient
 - It must be persuasive enough to convince a reasonable person of the validity of the findings
 - Means also that it cannot be easily doubted.
 - ♦ Evidence must be reliable
 - It must be consistent with fact, must be factual and not circumstantial
 - ♦ Evidence must be Relevant
 - It must have a reasonable and sensible relationship to the findings
 - ♦ Evidence must be Legally permissible
 - It was obtained in a legal way
 - ♦ Evidence must be properly identified
 - ♦ Evidence must be properly preserved

➤ **Surveillance / Search**

- **Often done quickly due to the nature of the evidence**
- **Electronic Monitoring**
 - Use log-on Banner to tell user
 - Inform users
 - Enticement
 - ♦ Legal and Ethical
 - Entrapment
 - ♦ Illegal and Un-ethical
- **2 Types of surveillance**
 - Physical
 - ♦ Security Camera (e.g. CCTV)
 - Via the computer
 - ♦ Auditing events passively or actively
 - ♦ Active monitoring
 - Require search warrant
 - ♦ Passive Monitoring
 - ♦ There are exceptions to requiring a search warrant
 - ♦ If the suspect tries to destroy evidence called Exigent Circumstances
- **Obtain ?**
 - · Voluntary or consent
 - · Subpoena
 - ♦ A court issues the subpoena to an individual with the instructions to bring the evidence to court
 - · Search warrant

- ♦ A search warrant is issued to a law enforcement officer allowing them to take the equipment

➤ **Issues to be addressed**

• **Investigations**

- **Preliminary**
 - ♦ Planning for and conducting investigations
 - ♦ A Preliminary Investigation should be conducted
 - ♦ To determine if a crime has been committed by examining the audit records and system logs
 - ♦ Interviewing witnesses, and assessing the damage incurred
- **Timing**
 - ♦ The timing of requesting outside assistance from law enforcement is a major issue
 - ♦ This may bring negative publicity resulting in a lack of confidence in the business of the organization
- **Good sources of evidence include**
 - ♦ Telephone records
 - ♦ Video Cameras
 - ♦ Audit Trails
 - ♦ System Logs
 - ♦ System Backups
 - ♦ Registry (Added by me)
 - ♦ Witnesses
 - ♦ Emails
- **If the investigation is undertaken internally**
 - ♦ The suspect should be interviewed to acquire information
 - ♦ This interrogation should be planned in advance
 - ♦ Common mistake is providing the suspect with too much information
- **Evaluate (MOM)**
 - ♦ Motivations, Opportunities and Means
 - ♦ Motivations
 - Who and why of a crime
 - These motivations can be induced by internal or external conditions
 - ♦ Opportunity
 - Where and when of a crime
 - Opportunities arise when certain vulnerabilities are weaknesses are present
 - ♦ Means
 - The capabilities a criminal would need to be successful

• **Liaison**

- Establish a prior liaison with law enforcement

• **Decide**

- Decide when and if to bring the law enforcement

• **Reporting**

- Setting up means for reporting computer crimes
- Established procedures for handling and processing reports of computer crime.

• **Senior Management**

• **Collection**

• **Alert**

❖ **Liability and Its Ramifications**

➤ **Management Obligation**

• **Protect**

- Natural disasters
- Malicious code

- Proprietary compromise
 - Damage to reputation
 - Violation of the law
 - Employee Privacy suits
 - Stockholder suits
 - **Due care**
 - Steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and have taken the necessary steps to help protect the company, its resources and employees
 - The officers must exercise due care or reasonable care to carry out their responsibilities to the organization
 - Continual activities that make sure the protection mechanisms are continually maintained and operational
 - Means to prevent the organization's computer resources from being used as a source of attacks.
 - Example of Due care
 - ♦ Backups
 - ♦ Scans for Malicious code
 - ♦ Business continuity and business disaster plans
 - ♦ Elimination of unauthorized and unsecured modems
 - ♦ Ensuring the C.I.A of organization databases
 - ♦ Establishing an organizational incident handling capability
 - **Prudent man rule**
 - Perform duties that prudent people would exercise in similar circumstances
 - **Downstream liabilities**
 - When companies come together to work in an integrated manner, special care must be taken to ensure that each party promises to provide the necessary level of protection, liability and responsibility needed which should be clearly defined in the contracts that each party signs.
 - **Legally recognized obligation**
 - There is a stand of conduct expected of the company to protect others from unreasonable risks
 - The company must fail to conform to this standard, which results in injury or damage to another
 - **Proximate Causation**
 - An action that was taken or not taken was part of a chain that resulted in negative consequences
 - Someone can prove that the damage that was caused was the company's fault
- **Incident Handling should address**
- **Is it an Incident ?**
 - What is considered an incident
 - **Reporting ?**
 - How ? an incident should be reported
 - Whom ? To whom should the incident be reported
 - **What Action ?**
 - What action should be taken if an incident is detected
 - **Who handle ?**
 - Who should handle the response to the incident
 - **Damage ?**
 - How much damage was caused by the incident

- **Info damage ?**
 - What information was damaged or compromised by the incident
- **Recovery**
 - Are recovery procedures required to remediate damages caused by the incident
- **Follow-up**
 - What type of follow-up and review should be conducted after the incident is handled
- **Additional Safeguards**
 - Should additional safeguards be instituted as a result of the incident
- **Part of Contingency Plan**
 - Incident handling can be considered as the portion of contingency planning
 - Contingency planning is when we responds to malicious technical threats and can be addressed by establishing a computer Incident Response Team CIRT.

❖ Ethics

➤ (ISC)2 Code of Ethics

- **Code of Ethics Canons**
 - Protect society, the commonwealth, and the infrastructure.
 - Act honorably, honestly, justly, responsibly, and legally.
 - Provide diligent and competent service to principals.
 - Advance and protect the profession.
- **Protect society, the commonwealth, and the infrastructure**
 - Promote and preserve public trust and confidence in information and systems.
 - Promote the understanding and acceptance of prudent information security measures.
 - Preserve and strengthen the integrity of the public infrastructure.
 - Discourage unsafe practice.
- **Act honorably, honestly, justly, responsibly, and legally**
 - Tell the truth; make all stakeholders aware of your actions on a timely basis.
 - Observe all contracts and agreements, express or implied.
 - Treat all constituents fairly
 - Consider public safety and duties to principals, individuals, and the profession in that order.
 - Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort.
 - Take care to be truthful, objective, cautious, and within your competence.
 - Give preference to the laws of the jurisdiction in which you render your service.
- **Provide diligent and competent service to principals**
 - Preserve the value of their systems, applications, and information.
 - Respect their trust and the privileges that they grant you.
 - Avoid conflicts of interest or the appearance thereof.
 - Render only those services for which you are fully competent and qualified.
- **Advance and protect the profession**
 - Sponsor for professional advancement those best qualified.
 - Take care not to injure the reputation of other professionals through malice or indifference.
 - Maintain your competence; keep your skills and knowledge current.
 - Give generously of your time and knowledge in training others.
 - Avoid professional association with those whose practices might diminish the profession.
- **Behaviors**
 - Discourage certain common but egregious behavior.
 - Crying wolf

- Consenting to bad practice
- Attaching weak systems to the public net
- Consorting with hackers
- Reading and keeping up on hacker practices is NOT mentioned,

➤ **The Computer Ethics Institute's Ten Commandments**

- Thou shalt not use a computer to harm other people
- Thou shalt not interfere with other people's computer work
- Thou shalt not snoop around in other people's computer files
- Thou shalt not use a computer to steal
- Thou shalt not use a computer to bear false witness
- Thou shalt not copy or use proprietary software for which you have not paid
- Thou shalt not use other people's computer resources without authorization
- Thou shalt not appropriate other people's intellectual output
- Thou shalt think about the social consequences of the program you are writing
- Thou shalt use a computer in a ways that ensure consideration and respect for your fellow humans

➤ **The Internet Activities Board IAB (unacceptable activities)**

- Seeks to gain unauthorized access to the resources of the Internet
- Destroys the integrity of computer based information
- Disrupts the intended use of the Internet
- Wastes resources such as peoples, computers through such actions
- Compromises the privacy of users
- Involves negligence in the conduct of Internet wide experiments

➤ **The U.S. Department of Health, Education**

- The U.S. Department of Health, Education, Welfare Code of Fair Information Practices
- There must not be personal data record keeping systems whose very existence is secret
- There must be a way for a person to find out what information about them is in a record and how it is used
- There must be a way for a person to prevent information about them, which was obtained for one purpose, from being used for another purposes without their consent

➤ **GASSP**

- Generally Accepted System Security Principles
- Seeks to develop and maintain GASSP with guidance from security professionals
- 1- Computer security supports the mission of the organization
- 2- Compute security is an integral element of sound management
- 3- Compute security should be cost-effective
- 4- Systems owners have security responsibilities outside their organizations
- 5- Compute security and accountability should be made explicit
- 6- Compute security requires a comprehensive & integrated approach
- 7- Compute security should be periodically reassessed
- 8- Compute security is constrained by social factors