Legal and Ethical Issues in Computer Security

Prepared By: Rusul M. Kanona
Supervised By: Dr. Lo'a i A.Tawalbeh
Arab Academy for Banking & Financial Sciences
)AABFS(
Fall 2007

:Objectives for this session

- **To convince you that ethical and legal issues are integral to much of what we do as security professionals**
- **To get you thinking about how you feel about issues you are likely to encounter**
- **To introduce you to the alphabet soup of regulations that may affect how you do your job**

Ethical vs. Legal Issues

- **Q: What's the difference between a legal issue and an ethical issue?**
- **How do you determine which it is?**
- **Should you care which it is?**
- **What percentage of your time would you guess that you will spend dealing with ethical or legal issues?**

Ethical vs. Legal Issues

- **Legal issues:**
  - **Sometimes have a definitive answer**
  - **Determination is made by others (not you)**

- **Ethical issues:**
  - **Sometimes have a definitive answer**
  - **You determine your course of action**

- **The law doesn't make it "right"**
- **Being "right" doesn't make it legal**

Ethical Issues

- **Ethical**

  1. pertaining to or dealing with morals or the principles of morality; pertaining to right and wrong in conduct.

  2. in accordance with the rules or standards for right conduct or practice, esp., the standards of a profession.

- **Examples:**
  - **Should companies collect and/or sell customer data?**
  - **Should IT specialists monitor and report employee computer use?**

Consider Your Views on Ethical Behavior

- **In every job situation, we are all eventually faced with an ethical dilemma**
- **How will you react? How will you determine what the "right" course of action is? What are you willing to risk to do the "right thing"?**
- **How far are you willing to bend? And when?**

?Are Your Ethics Contextual

- **Are they unchanging or contextual?**
  - **Peoples know that downloading music or software they don't own is illegal, but do so anyway because they don't believe that it hurts the owners of the IP (intellectual property)**
  - **You have an expectation of privacy (lockers, email, etc.) except if there is suspicion of wrong doing**
  - **Never tell a lie….except if ……**
- **Somehow, legal doctrine must codify these complicated and contextual courses of action**

Framework for Ethics

- **What motivates us to view issues a certain way?**
- **Are we consistent in the way we approach ethical issues?**
- **How do we resolve conflicts in approach?**
- **Two basic camps:**
  - **consequence-based**
  - **rule-based**

From: “Case Studies in Information and Computer Ethics”, Richard Spinello, Prentice-Hall, 1997

Consequence-Based Ethics

- **Priority is given to choices that lead to a "good" outcome (consequence)**
- **The outcome outweighs the method**
- **Egoism: the "right choice" benefits self**
- **Utilitarianism: the "right choice" benefits the interests of others**

Rule-Based Ethics

- **Priority is given to following the rules without undue regard to the outcome**
- **Rules are often thought to codify principles like truth fulness, right to freedom, justice, etc.**
- **Stress fidelity to a sense of duty and principle (“never tell a lie”)**
- **Exist for the benefit of society and should be followed**

Example

- **Scenario:**
  - **Student copies answers on a final exam**
  - **As per policy, I confront student with evidence**
- **My perspective was:**
  - **The right thing to do is to tell the truth regardless of the consequences**
- **The student's perspective was:**
  - **"If I confess now, will the penalty be less than if I roll the dice with the University Judiciary Counsel and am found guilty?"**

Example

- **You are the security officer for a research network at the other large Florida University. You suspect that students are using P2P appliances to upload copyrighted music that they do not own. This violates federal law (DMCA) and is against the University computer use code.**

- **What are you going to do about it? Where is your comfort level?**

- **Options:**
  - **Do nothing until a suspicion is brought forward**
  - **Bandwidth limit P2P with a packet shaper**
  - **Filter P2P outright**
  - **Actively monitor the network looking for P2P**
  - **Read the local newsgroups and follow leads when P2P is discussed**

?Which camp were you in

- **Consequence-based**
  - **Egoism: the "right choice" benefits self**
  - **Utilitarianism: the "right choice" benefits the interests of others**

- **Rule-based:**
  - **Pluralism: stresses fidelity to a sense of duty and principle ("never tell a lie")**
  - **Rule-based: rules exist for the benefit of society and should be followed**

Privacy Issues

- **Many ethical issues (and legal issues, as we will see) in security seem to be in the domain of the individual's right to privacy verses the greater good of a larger entity (a company, society, etc.)**
- **Examples: tracking employee computer use, managing customer profiles, tracking travel with a national ID card, location tracking [to spam cell phone with text message advertisements], ….**
- **A key concept in sorting this out is a person's expectation of privacy**

Four Ethical Issues of the Information Age[1]

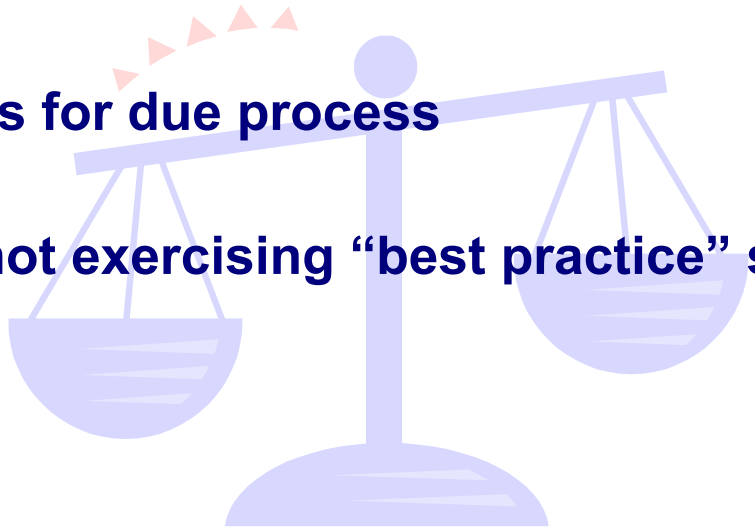
- **Privacy - right of individual to control personal information**
- **Accuracy – who is responsible for the authenticity, fidelity, and accuracy of information?**
- **Property – Who owns the information? Who controls access? (e.g. buying the IP verses access to the IP)**
- **Accessibility – what information does an organization have the right to collect? Under what safeguards?**

1: Richard O. Mason, Management Information Systems Quarterly, Volume 10, Number 1, March 1986

Legal Issues

Q: We need to know this because: ?

- **Emerging legal requirements for C.I.A. of data**
- **Requirements for due process**
- **Liability for not exercising "best practice" security?**



Hierarchy of Regulations

- International:
  - **International Cyber crime Treaty**
- Federal:
  - **FERPA, GLB, HIPAA, DMCA, Teach Act, Patriot Act, Sarbanes-Oxley Act, ….**
- State:
  - **UCITA, SB 1386, ….**
- Organization:
  - **Computer use policy**

Examples

- **Let's take a very quick look at a few of the)many regulations that could impact how you do your job**
  - **International cyber crime treaty**
  - **HIPAA** (Health Insurance Portability and Accountability Act)
  - **US Patriot Act**
  - **FERPA** (Family Educational Rights and Privacy Act)

What would we expect to see in ?“information protection” legislation

- **Components:**
  - **Statement of what we are trying to protect (what type of data)**
  - **Attributes that need protection (C.I.A.)**
  - **Changes to business practices**
  - **Assigning accountability for protection**
  - **Penalty for failure**
  - **Specific areas that technology should address (e.g., authentication, storage, transmission)**

International Cyber crime Treaty- 1

- **Goal: facilitate cross-border computer crime investigation**
- **Who: 38 nations, USA has not ratified it yet**
- **Provisions:**
  - **Obligates participants to outlaw computer intrusion, commercial copyright infringement, online fraud**
  - **Participants must pass laws to support search & seizure of email and computer records, perform internet surveillance, make ISPs preserve logs for investigation**
  - **Mutual assistance provision to share data**
- **Opposition: open to countries with poor human rights records; definition of a "crime"**

Health Data Security-2

- "All organizations that handle patient-identifiable health care information – regardless of size – should adopt the set of technical and organizational policies, practices, and procedures described below to protect such information."

1- Organizational Practices:

- Security and confidentiality policies
- Information security officers
- Education and training programs
- Sanctions

2- Technical Practices and procedures

- Individual authentication of users
- Access controls
- Audit trails
- Physical security and disaster recovery
- Protection of remote access points
- Protection of external electronic communications
- Software discipline
- System assessment

HIPAA

Health Insurance Portability and Accountability Act

- Focus: Addresses confidentiality of personal medical data through standards for administrative, physical, and technical security
- How does this apply to IT professionals?
  - If you have systems with patient data, and you either

    (a) transmit that data or

    (b) allows access to systems that store the data, then you need to be HIPAA compliant
  - If you transmit protected health information, you are accountable for: Integrity controls; message authentication; alarm; audit trail; entity authentication; and event reporting. If you communicate with others via a network: access controls; encryption.

HIPAA Security Examples

Data Integrity: not altered during transmission: e.g., TLS (transport level security), etc. Regardless of access method (web, shares, etc.)

Message Authentication: validate sender's identity e.g., signature, hash, public key, symmetric key

Alarms: notification of a potential security event, e.g., failed logins,

Audit trails: monitor all access to health information, must be kept around for 6 years or more,

Entity authentication: could be as simple as passwords & unique user ID

Error reporting: error and audit logs may need to be kept for a period of time

HIPAA Security Areas

1. **Administrative procedures to guard data CIA. Documented formal procedures to select and measure security mechanisms**
2. **Physical safeguards to protect computers, buildings, data.**
3. **Technical security services, including processes to protect information**
4. **Technical security mechanisms to prevent unauthorized access to stored or transmitted data**

1- Administrative Safeguards

- Security management processes: risk analysis, risk management, sanction policy, information systems activity review
- Assigned security responsibility: identified person accountable for security
- Workforce security: processes for clearance, authorization, and termination
- Incident procedures: response and reporting
- Contingency plan: backup, disaster recovery, testing

2- Physical Safeguards

- Facility Access controls: contingency operations, facility security plan
- Workstation use
- Workstation security
- Device and media controls: disposal, media re-use, backup

3- Technical safeguards:

- Access control: unique user ids, automatic logoff, encryption, emergency access
- Audit controls
- Integrity: mechanism to authenticate electronic protected health information
- Entity authentication
- Transmission security: integrity controls., encryption

3- US Patriot Act

- **This is a whole legal/ethical/moral debate that we could have some other time. Bottom line, it's the law, and you as an IT professional need to know:**
  - **simple search warrant will gain access to stored voice mail**
  - **Govt. can subpoena session times and duration; can request ISP payment information**
  - **cable companies can provide customer information without notifying customer**

FERPA- 4

Family Educational Rights and Privacy Act

- **Gives parents certain rights to their child's educational records**
- **Gives adult students right to:**
  - **See information the institution is keeping on the student**
  - **Seek amendment to the records in certain cases**
  - **Consent disclosure of his/her own records**
  - **File a complaint with FERPA**
- **Records include: personal information, enrollment records, grades, schedules; on any media**

?Questions