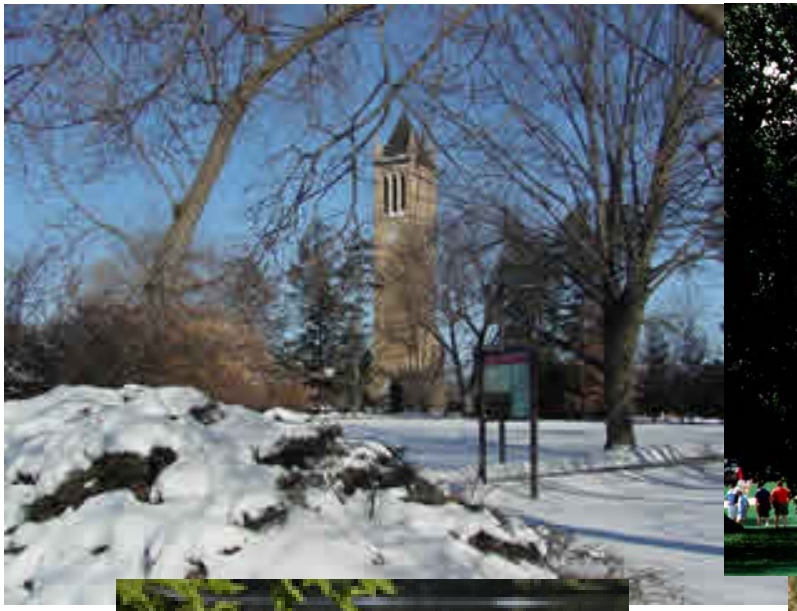
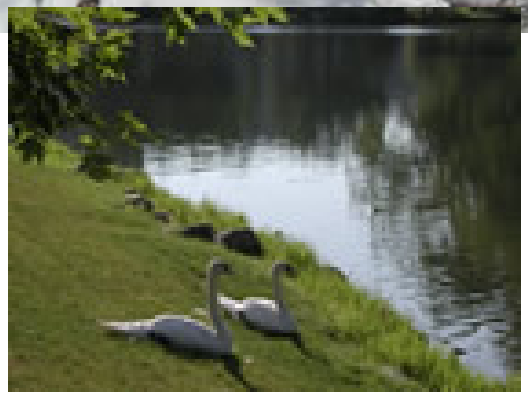
A Few Legal and Ethical Issues in Computer Security

Jim Davis
Chief Information Officer
Iowa State University

Iowa State University





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**

Warm-Up:

- **You are the security officer for a research network at the other large University. You suspect that students are using P2P appliances to share 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 you receive a DMCA complaint**
  - **Bandwidth limit P2P with a packet shaper**
  - **Filter all P2P outright**
  - **Actively monitor the network looking for P2P**
  - **Read the campus newsgroups and rat out students whose identity can be determined**

Post-Processing

- **Did your group develop a consensus?**
- **What did you feel were the legal issues?**
- **What were the ethical issues?**
- **Was there anything you needed to know that might have influenced your response?**

Privacy stories in the news

- SANS NewsBits (www.sans.org)
- I have about 10 of these that help to show the breadth of issues – we will breeze through stopping only if you'd like to discuss them [post note – full stories can be found on the SANS web site or the links provided]

1. SANS PrivacyBits January 18, 2004 Vol. 3, Num. 3
USA: Judge Rules Police Can Use GPS to Track Suspect Without Warrant (12 January 2005)
http://news.com.com/Snooping+by+satellite/2100-1028_3-533560.html

2. SANS PrivacyBits January 11, 2004 Vol. 3, Num. 2
USA: NJ Legislature to Consider Two Privacy-Related Bills (07 January 2005) http://www.newsday.com/news/local/state/ny-bc-nj--privacyissues0107jan07,0,2515930.story?coll=ny-region-apnewjersey

3. SANS PrivacyBits December 14, 2004 Vol. 2, Num. 50
USA: State Supreme Court Rules Parents' Eavesdropping Violates Privacy Act (10 December 2004)
http://seattlepi.nwsource.com/local/aplocal_story.asp?category=6420&slug=WA%20SCOW%20Parental%20Snooping&dpfrom=th

4. SANS PrivacyBits December 7, 2004 Vol. 2, Num. 49
USA: Call for a Database of All University and College Students (30 November 2004)
http://seattlepi.nwsource.com/national/201622_ecollegedata30.html

5. SANS PrivacyBits November 23, 2004 Vol. 2, Num. 47
USA: Keylogger Devices Do Not Violate Federal Wiretap Law Says Judge (19 November 2004)
http://www.securityfocus.com/news/99

6. SANS PrivacyBits November 2, 2004 Vol. 2, Num. 44
USA: California's Expanded DNA Database Proposal Goes to Voters (29 October 2004)
http://www.napanews.com/templates/index.cfm?template=story_full&id=04B91738-7DB6-4CD4-A117-4F51AFD7FBFE

7. SANS PrivacyBits November 30, 2004 Vol. 2, Num. 48

USA: Secret Tracking Number in Every Document Printed on Laser Printer (22 November 2004)

http://story.news.yahoo.com/news?tmpl=story&cid=1093&e=4&u=/pcworld/20041122/tc_pcworld/118664

Your Turn

- **Question: should schools offer a course that teaches students how to break security mechanisms (hack systems)?**
- **Process:**
  - **You can have 3-5 minutes to discuss this in your group**
  - **All group members must contribute**
  - **Any group member should be prepared to report out**

Post-Processing

- **Did your group have a consensus?**
- **What was your top argument supporting your position?**
- **Is it illegal for me to teach this topic?**
- **Is it unethical for me to teach this topic?**
- **Is it negligent? i.e., should I be liable if a student uses this knowledge to do something illegal?**

Ethical vs. Legal Issues

- **Q: What are the differences 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 adj. 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?**
  - **Should you act on information you inadvertently see due to having administrator privileges?**

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?**
- **Recommendation: As you read about these issues during your studies, take time to reflect on what you would do**

Are Your Ethics Contextual?

- **Are they unchanging or contextual?**
  - **Folks know that sharing 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 and**
  - **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 truthfulness, right to freedom, justice, etc.**
- **Stress fidelity to a sense of duty and principle (“never tell a lie”)**
- **Rules exist for the benefit of society and should be followed**

A Personal Example

- **Scenario:**
  - **Student copies answers on a final exam**
  - **As per policy, I confront student with evidence**
- **My perspective was:**
  - **The “right thing” for the student 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?”**

Your turn – Examples?

- **Consequence-based**
  - Priority is given to choices that lead to a “good” outcome
  - Egoism: the “right choice” benefits self
  - Utilitarianism: the “right choice” benefits the interests of others
- **Rule-based**
  - Priority is given to following the rules without undue regard to the outcome
  - Stress fidelity to duty and principle (“never tell a lie”)
  - Rules exist for the benefit of society and should be followed

Your Turn:

1. **Bill is the network manager for a research group in a company. He downloads a traffic sniffer on his own, and notices that a colleague (Sam) is downloading stolen software.**
2. **Bill decides to take a closer look by inspecting Sam's computer in the evening when Sam is not at work. Bill's worst suspicions are confirmed.**
3. **Bill reports this to his supervisor (Sara) who in a fit of rage demands that Bill install a keystroke logger to capture passwords for all of Sam's private web accounts. Sara further demands that Bill turn over the passwords to Sara so she can "take care of this herself". Bill has a payment due on his Lexus and complies.**

Consider each step. What would you have done?

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, crowd surveillance, 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

Your Turn …

- What are your thoughts about Ethical issues in security?

  Examples?

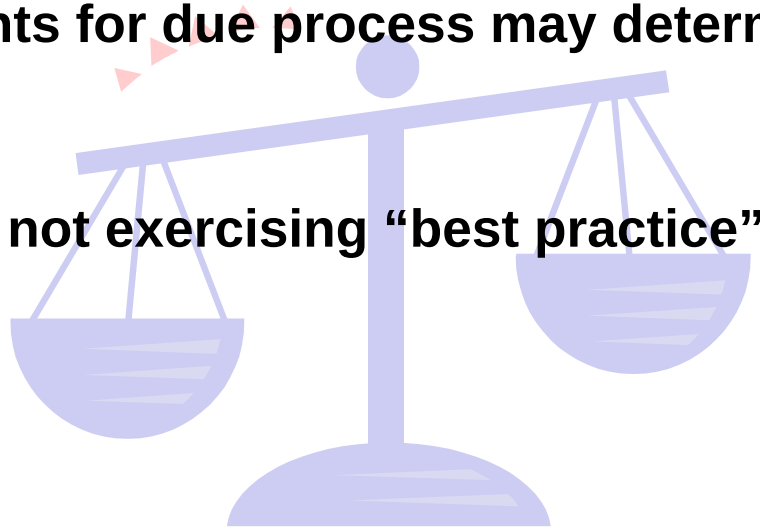
  Concerns?

  Emerging issues?

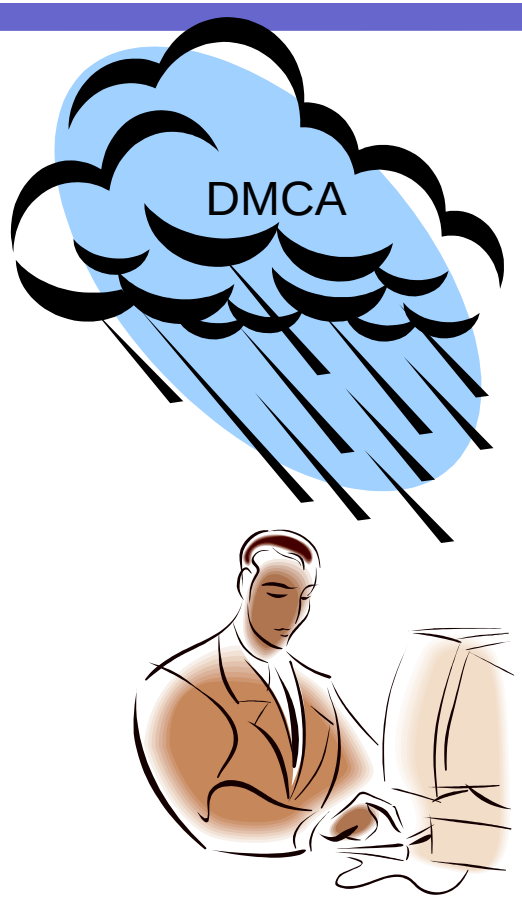
Legal Issues

Q: I need to know this because: ?

- **Emerging legal requirements for C.I.A. of data**
- **Requirements for due process may determine your course of action**
- **Liability for not exercising “best practice” security?**



Are You Ready?



Hierarchy of Regulations

- **International:**
  - **International Cybercrime 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 cybercrime treaty**
  - **Sarbanes-Oxley**
  - **FERPA**
  - **HIPAA**
  - **GLB**
  - **US Patriot 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)**
- **Hopefully, not prescriptive in technology**

1. International Cybercrime Treaty

- **Goal: facilitate cross-border computer crime investigation**
- **Who: 38 nations, USA has not ratified it yet**
- **Provisions:**
  - **Obligates participants to outlaw computer intrusion, child pornography, 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"**

2. Sarbanes-Oxley Act of 2002

- **Holds executives personally liable for many operational aspects of a company, including computer security, by making them pledge that the company internal controls are adequate**

- **Let me repeat, this holds executives personally liable for computer security by making them pledge that companies security mechanisms are adequate**

3. Health Data Security Requirements
(National Research Council 1997 report)

- Recommendation: "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."
  - Organizational Practices:
    - Security and confidentiality policies
    - Information security officers
    - Education and training programs
    - Sanctions
  - 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
- Recommendation: "the federal Government should work with industry to promote and encourage an informed public debate to determine an appropriate balance between the primary concerns of patients and the information needs of various users of health care information"

HIPAA

Health Insurance Portability and Accountability Act

- **Focus: Addresses confidentiality of personal medical data through standards for administrative, physical, and technical security**
- **Became law in 1996; cost for compliance estimated to exceed Y2K costs**
- **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., SSL, TLS (transport level security), etc. Regardless of access method (web, shares, ftp, 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**

Appendix A – Security STDs Matrix

- **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
- **Physical Safeguards**
  - Facility Access controls: contingency operations, facility security plan
  - Workstation use:
  - Workstation security:
  - Device and media controls: disposal, media re-use, backup
- **Technical safeguards**:
  - Access control: unique user ids, automatic logoff, encryption, emergency access
  - Audit controls: required
  - Integrity: mechanism to authenticate electronic protected health information
  - Entity authentication: required
  - Transmission security: integrity controls., encryption

HIPAA

- **It's the law – if you are accountable for systems with patient data, then you need to ensure that protection mechanisms are in place and are <u>working</u>**

4. Financial Modernization Act of 1999 (GLB, Gramm-Leach-Bliley Act)

- **Requires financial institutions under FTC jurisdiction to secure customer records and information**
- **All "significantly-engaged" financial organizations must comply: check cashing businesses, mortgage, data processors, non-bank lenders, real estate appraisers, ATM, credit reporting agencies, …**
- **Provides for: mandatory privacy notices and an opt-out for sharing data with some third parties**

GLB Components

Three basic parts to GLB:

- **Financial Privacy Rule – governs collection and disclosure of customer personal data**
- **Safeguard Rule – requires you to design, implement, and maintain security safeguards**
- **Pretext rule – protects consumers from individuals and companies who obtain personal information under false pretext**

Safeguard Rule

- **Each company implements its own specific security program. FTC recommends focus on:**
- **Employee Management and Training**
  - Background checks
  - Security best practices (e.g., passwords)
- **Information Systems**
  - Record storage, secure backup
  - Secure data transmission
  - Disposal of customer information
- **Managing system failures**
  - Patch management, AV software, change control
  - Continuity of operations

5. US Patriot Act

- **This is a whole legal/ethical debate that we could have some other time. Bottom line, it's the law, and you as an IT professional need to know:**
  - **(sunsets 12/05): simple search warrant will gain access to stored voice mail (Title III wiretap not needed)**
  - **Govt. can subpoena session times and duration; can request ISP payment information ("pen register and trap")**
  - **cable companies can provide customer information without notifying customer**
  - **(sunsets): devices can record any information relevant to an investigation, not just info on terrorist activities**
  - **the ISP cannot reveal the purpose of the gathering of "tangible things"**

Patriot Act

- **…and more**
- **Best advice: If you see this headed your way, contact your company legal staff so you understand <u>what is being asked</u> for so you can <u>comply in a timely manner</u>**

6. FERPA

- **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**

FERPA implications for IT

- **Organization must have policies and mechanisms in place to protect this information – technology and practices (e.g., posting grades, class email lists, etc.)**
- **Audit use, to demonstrate compliance with policies**
- **Provide opt-out for public part of the information (directory)**

E.g., University of Maryland

- **It is the policy of UM to permit students to inspect their education records, regardless of the media (only valid students, only their records, read-only, log access)**
- **It is the policy of UM to limit disclosure of personally identifiable information from educational records unless it has the student's prior written consent, subject to the following exclusions..**
- **It is the policy of UM to provide students the opportunity to seek correction of their educational records.**
- **Right to file a complaint**
- **Other resources: www.educause.edu**

  See http://www.terpparent.umd.edu/informing/policies.html

Summary - Emerging Issues

- **Interesting discussions about privacy:**
  - **RFID**
  - **National ID card**
  - **Face recognition systems**
  - **State web sites that list….tax evaders, sex offenders, etc.**
  - **Privacy vs anonymity vs accountability**
  - **Anything dealing with the PATRIOT Act**
- **Liability for security breeches**
  - **Liability for not exercising due diligence**
  - **Downstream liability for attack replay?**
- **Suit against Microsoft for dominance in market**

Objectives for This Session:

- **To convince you that ethical and legal issues are pervasive in 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**

Questions?

Thank You!