


# Legal Issues and Ethics



## Chapter 24

## Objectives


- Explore ethical issues associated with information security.
- Explain the laws and rules concerning importing and exporting encryption software.
- Identify the laws that govern computer access and trespass.
- Identify the laws that govern encryption and digital rights management.
- Describe the laws that govern digital signatures



## Information

---

- Information is data endowed with relevance and purpose
  
- Properties:
  - Accurate
  - Timely
  - Complete
  - Verifiable
  - Consistent



## Information Security

---

- The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.
  
- It is the preservation of **confidentiality, integrity and availability** of information.

*BS7799/ISO17799*





## Information Assurance

---

- Practice of managing risks related to
  - the use, processing, storage, and transmission of information or data
  - and the systems and processes used for those purposes.
- Protecting information assets from **destruction, degradation, manipulation and exploitation** by an opponent
- Action taken that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non repudiation.


*US Department of Defense*

- 
- 
- Information Assurance And Security- a multi-disciplinary field
  - Involved disciplines
    - Computer science
    - Computer engineering
    - Mathematics
    - Information systems
    - Business
    - Political science
    - Psychology
    - Sociology
    - Law



---

Why are we here?  
What are we going to do?



---

**Recap- Job/Professional Level**

- The abilities that graduates need to be specific in professional practice. This includes, but is not limited to skills
  - recognized by professional organizations for certification
  - needed in research and development.



## Recap- Layer 1: Prerequisite Body of Knowledge

---

- For this course, we focus on students with a computer science and information systems background preparing to study information security, although we may use selected topics from other disciplines.
  
- For example, all computer science students might be expected to know operating system, networks, and so on.
  - This would be considered a part of the layer 1 computer science core body of knowledge



## Recap- Layer 2: Information Assurance Body of Knowledge

---

- The technical know how and expertise that extends beyond what a typical computer science/computer engineer/information technology professional would need/be expected to know.
  
- For example: The information assurance layer 2 skills that build on the computer science knowledge include
  - defining secure operating systems
  - securing an operating system,
  - and configuring and managing security tools.



### Recap- Layer 3: Higher Order Skills

---


- Skills and abilities that cut across the layer 1 and layer 2 topic areas.
- Regardless of the disciplinary foundation and the articulation of that foundation to advanced technical IA knowledge, all IA professionals need higher order information assurance skills in the areas of
  - Risk assessment
  - Modeling and mitigation
  - Evaluation of the efficacy of competing security mechanisms, methodologies, and models
  - Standards
  - Legal implications and laws.



### The Dilemma


---

- Teaching Information Assurance in Educational Institutions:
  - To counter the threat posed by antisocial and criminal elements, educational institutions are creating a cadre of professionals skilled in information assurance – **the art and science of protecting the integrity, availability and privacy of valuable information assets and systems.**



---


- *Endicott-Popovsky (2003)*
  - The cyber-criminal profile is not the stereotypical under-privileged person from an economically deprived household.
  - These cyber-criminals come from more affluent homes, with access to computers and Internet connectivity
  - Teens and adolescents are committing the majority of computer crimes.
    - **Can students indulge in questionable activities??**
    - **Might even be good students in school?**



## The Dilemma


---

- **Ryan & Ryan**
  - Are we as IA educators only adding to the problem by teaching computer security vulnerabilities in our classrooms?
  - Can we teach students to defend information infrastructures without teaching them how to attack such infrastructures either in theory or in practice??
  - We rely on the ready availability of useful tools ranging from scripting languages to programs and systems for cryptography, access control, firewall, malicious code detection, intrusion detection, trusted networking, forensic analysis and a host of other relevant and valuable functions.
  - Some student might abuse the information and techniques taught to them



---

- As the number of professionals trained and educated in the field of information assurance grows, so does the likelihood that some of those professionals will abuse the skills they have been taught and the tools they have been taught to use, and will attack rather than defend information infrastructures
  
- **We must understand the ethical and legal constraints that apply to the uses of the knowledge we impart or gain**




---

*Ethics in an IA curriculum*


- We will focus on
  - what constitutes ethical behavior.
  - Examining the consequences of actions
  - enhancing the ability to make the right decisions when faced with questions about how to use the information they learn in the classroom.
  - Legal issues
  
- Although IA and the subjects embraces—system vulnerabilities and controls and types of attacks—are **exciting and interesting topics**, there is a serious side to what we do, and **serious consequences for misguided behavior**.





---

- To minimize liabilities/reduce risks, we must
  - understand the gravity of what we are learning and follow ethical procedures and guidelines
  - understand the scope of an organization's legal and ethical responsibilities
  - understand the current legal environment
  - watch for new issues that emerge



### Law and Ethics in Information Security

---

- Laws:
  - Rules that mandate or prohibit certain societal behavior
  - Carry sanctions of a governing authority
- Ethics:
  - Define socially acceptable behavior
    - Provides the **ability** to distinguish right from wrong
  - Do not carry sanctions of a governing authority



## What is Ethics?

---

- A global term describing the system by which individuals distinguish right from wrong
  - Ethical systems describe the duties and behaviors commonly considered correct for a given circumstance
    - Documented by an ethical guideline that aids in behavior evaluation and as a framework to judge behavior
  - Ethics benefit information assurance because they are applied morality
    - They are logical assumptions about how moral principles should be applied in practice
    - They represent an understanding of what is morally correct
    - They become legal systems when the morality they capture is formalized into law



## Ethics

---

- Information practitioners need guidance in correct behavior
  - Especially essential because the commodity is abstract (intangible) and information assurance professionals have unprecedented access
  - Anonymity, intangibility, and evolution of the technology, increase ethical grey areas
  - Technological advances usually come without ethical instructions
  - Ethical violations of cyberspace occur regularly without widespread recognition or response
    - Nobody has thought through what a particular capability or activity represents in terms of right and wrong



## Ethics

---

- Globalization blurs ethical lines.
- Social norms vary among diverse principalities.
- Challenge for today's businesses:
- Code of ethics must be established.
- Employees need to understand what is expected.
- SANS published a set of IT ethical guidelines.



## Ethics and Technology

---

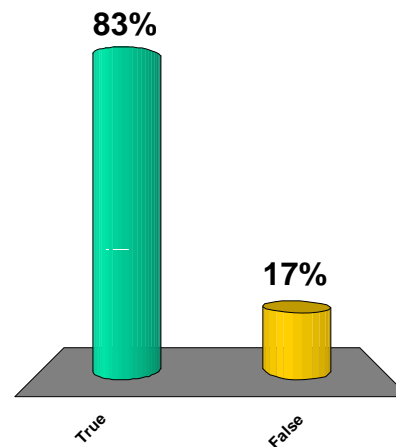
- Technology has advanced at a rate that exceeds society's ability to decide about its appropriateness
  - Data-mining industry is an example of organizations operating without an ethical compass
    - Privacy concerns and the question of the ethics
  - More grey areas are likely to develop
- It is essential for the information profession to consider, adopt, and use ethical guidelines
  - Without ethical guidance it is difficult to expect effective control of information workers' behavior

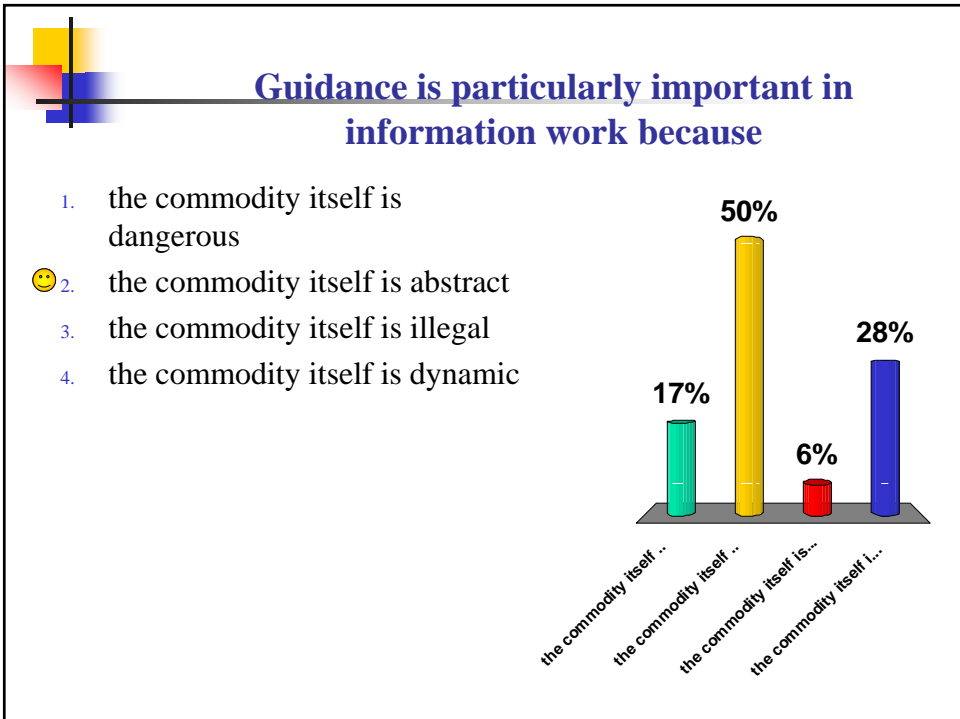
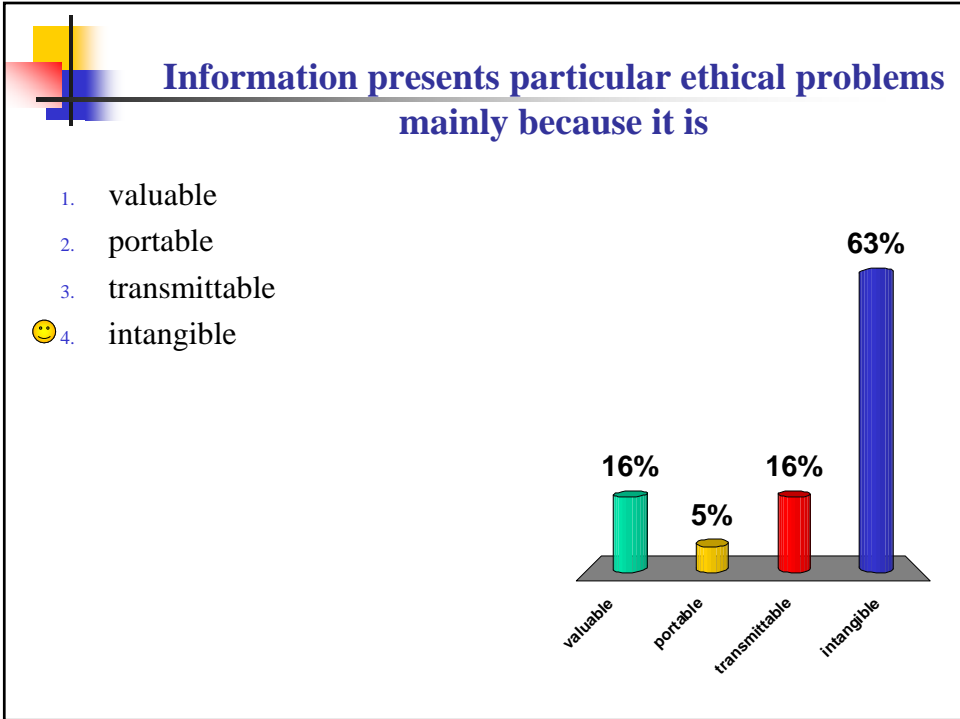
## Information Ethics

- Four areas where guidance about ethical behavior should be provided:
  - Unauthorized appropriation of information
    - use of a computer to obtain something under false pretenses
  - Breach of confidentiality
    - Disclosure of private information
  - Loss of integrity
    - Information has not been accidentally or maliciously altered or destroyed
  - Invasion of privacy
    - The unauthorized entry into a computer system via any means, including remote network connections

## Ethics provides the ability to distinguish right from wrong

- ✓ 1. True
2. False








## Professional Organizations

- **Association of Computing Machinery (ACM)**
  - Code of ethics contains references to protecting information confidentiality, causing no harm, protecting others' privacy, and respecting others' intellectual property
  
- **International Information Systems Security Certification Consortium, Inc. (ISC)<sup>2</sup>**
  - Non-profit organization focusing on development and implementation of information security certifications and credentials
  - Code primarily designed for information security professionals who have certification from (ISC)<sup>2</sup>
  - Code of ethics focuses on four mandatory canons
    - Protect society, the commonwealth, and the infrastructure;
    - Act honorably, honestly, justly, responsibly, and legally;
    - Provide diligent and competent service to principals; and
    - Advance and protect the profession.



## Professional Organizations


- **Information Systems Audit and Control Association (ISACA)**
  - Professional association with focus on auditing, control, and security
  - Concentrates on providing IT control practices and standards
  - ISACA has code of ethics for its professionals
  
- **Computer Security Institute (CSI)**
  - Provides information and training to support computer, networking, and information security professionals
  - Though without a code of ethics, has argued for adoption of ethical behavior among information security professionals



### Other Organizations

---

- **Internet Society (ISOC):** promotes development and implementation of education, standards, policy and education to promote the Internet
- **Computer Security Division (CSD):** division of National Institute for Standards and Technology (NIST); promotes industry best practices and is important reference for information security professionals
- **CERT Coordination Center (CERT/CC):** Center of Internet security expertise operated by Carnegie Mellon University
- **Computer Professionals for Social Responsibility (CPSR):** Public organization for anyone concerned with impact of computer technology on society



### CyberCrime & Law



## Cybercrime

- Characteristics
  - Technology is constantly changing
  - Sophistication of computer crimes has increased
  - Generally focus on financial gain
  - Often run by organized crime
  - Low risk of being caught
  - Difficult to prosecute



## Types of Cybercrime

- **Computer-involved crimes:**
  - **Computer-assisted**
    - The computer is a tool used by the criminal to accomplish his goal.
  - **Computer-targeted**
    - The computer is the victim of the criminal's actions.
  - **Computer-incidental**
    - The computer is merely related to the crime.
    - Crime could occur w/out the technology, however, technology helps the crime to occur faster, makes the crime more difficult to identify & trace
    - Money laundering, BBS supporting unlawful activity.



The \_\_\_\_\_ of being caught is one of the reasons that criminals are turning to computer crime.

😊 1. Low risk  
2. High risk  
3. No risk

Risk Level	Percentage
Low risk	94%
High risk	6%
No risk	0%

## Internet Crime

- Most computer crime revolves around money.
- **Internet Crime Complaint Center (IC3):**
  - Communicates issues associated with cybercrime.
  - Collaborative effort of
    - FBI
    - National White Collar Crime Center (NW3C)
    - Bureau of Justice Assistance (BJA)
  - Produces common Internet crimes list and descriptions
  - Provides advice on how to prevent becoming a victim of Internet crime

**IMPORTANT**

## Common Internet Crime Schemes

<http://www.ic3.gov/crimeschemes.aspx>

Current and ongoing Internet trends and schemes identified by the Internet Crime Complaint Center along with its description.

- ❑ Auction fraud
- ❑ Counterfeit cashier's check
- ❑ Credit card fraud
- ❑ Debt elimination
- ❑ Parcel courier e-mail scheme
- ❑ Employment/ Business opportunities
- ❑ Escrow services fraud
- ❑ Identity theft
- ❑ Internet extortion
- ❑ Investment fraud
- ❑ Lotteries
- ❑ Nigerian Letter or "419"
- ❑ Phishing/spoofing
- ❑ Ponzi/pyramid
- ❑ Reshipping
- ❑ Spam
- ❑ Third-party receiver of funds

<http://www.ic3.gov/preventiontips.aspx>

How to prevent these crimes through individual actions.

## Sources of Laws

- **Statutory law**
  - Statutory laws are the laws passed by local, state, and federal legislative bodies.
  - Specific statutory laws, such as the Computer Fraud and Abuse Act (CFAA), govern behavior.
- **Administrative law**
  - Power granted to government agencies through legislation.
  - This power of lies in the ability to enforce behaviors through administrative rule making.
  - Example: Federal Trade Commission (FTC), have made their presence felt in the Internet arena with respect to issues such as intellectual property theft and fraud.
- **Common law**
  - Laws derived from previous events or precedence and originates in the judicial branch of government.
  - As new cybercrime cases continue to unfold in the courts, precedents are being made on which future crimes involving computers can be judged.



## Computer Trespass

---

- Unauthorized access of a computer system
  - Independent of access method
  - Considered a crime in many countries
  - May warrant significant punishment
  - Treaties between countries regulate ways to deal with the cyber offenders



## Convention on Cybercrime (2004)

---

- First international treaty that addresses crimes committed through the Internet and other computer networks.
- Ratified by EU, U.S., Canada, Japan, and others
- Created common policies to handle cybercrime
- Focused on:
  - Copyright infringement
  - Computer-related fraud
  - Child pornography
  - Violations of network security



## Significant U.S. Laws

- **The United States**
  - A leader in the development and use of computer technology.
  - As such, it has a long history associated with computers, and with cybercrime.
  - Because legal systems tend to be reactive and move slowly, this leadership position has translated into a leadership position from a legal perspective as well.
- **Some significant US laws dealing with cybercrime**
  - Electronic Communications Privacy Act
  - Stored Communications Act
  - Computer Fraud and Abuse Act
  - Controlling the Assault of Non-Solicited Pornography and Marketing Act
  - USA Patriot Act
  - Gramm-Leach-Bliley Act
  - Sarbanes-Oxley Act




## Electronics Communications Privacy Act (ECPA)

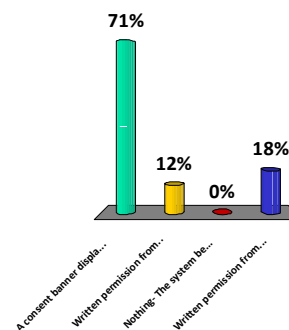
- Addresses legal privacy issues related to computer use and telecommunications
- A common practice with respect to computer access and privacy today is the use of a warning banner
- **Warning Banners are common practice in:**
  - Establishing the level of expected privacy
  - Serving notice of intent to conduct real-time monitoring
    - Real-time monitoring can be conducted for
      - Security reasons
      - Business reasons
      - Technical network performance reasons.
  - Obtaining user's consent to monitoring. Typically displayed upon login
  - Providing consent to law enforcement search

## Computer Fraud and Abuse Act (1986)

- Provides the foundation of U.S. law on unauthorized access
- Criminalizes activities such as:
  - to knowingly access a computer, either considered a government computer or a computer used in interstate commerce, without permission
  - Using a computer in interstate crime
  - Trafficking in passwords or access information
  - Transmitting code, commands, or programs that result in damage

### The VP of IS wants to monitor user actions on the company's intranet. What is the best method of obtaining the proper permission

1.  A consent banner displayed upon login
2. Written permission from a company officer
3. Nothing- The system belongs to the company
4. Written permission from the user






## Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)

- Established spam e-mail regulations
- **Provided rules of compliance**
  - Unsubscribe
    - Requires an obvious opt-out provision to allow users to unsubscribe, with these requests being honored within ten days.
  - Content
    - The content must be clear and not deceptive.
    - Adult content must be clearly labeled and subject lines must be clear and accurate.
  - Sending Behavior
    - Sending behavior rules include not using harvested e-mail addresses, not falsifying headers, and not using open relays.
    - CAN-SPAM criminalizes header manipulation
- Has had a poor track record of convictions




## USA Patriot Act

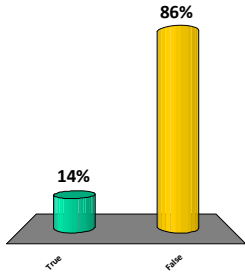
- Response to the 9/11 terrorist attacks
- Altered U.S. laws on Internet wiretaps and tracing
- Permits the Justice department to rollout Carnivore program, an eavesdropping program for the Internet
  - The name Carnivore has now been retired but the right of the government to eavesdrop remains a hot topic
- Requires ISPs to facilitate Internet monitoring
- Provides for federal law enforcement investigation and adjudication of computer intrusions




---

**Falsifying header information is not covered by the CAN-SPAM Act.**

1. True
2.  False




Response	Percentage
True	14%
False	86%



---


**Gramm-Leach-Bliley Act (GLBA)**

- Enacted in 1999
- Financial industry legislation to protect individual privacy.
- Key privacy tenet - Created an opt-out method providing individual control over the use of personal information
- Enforced by state, federal and securities laws
- Restricts information sharing with third-party firms, while still allowing for internal sharing in accordance with the Fair Credit Reporting Act.
  - For example: SSN, other facts kept by your bank



## **Payment Card Industry Data Security Standard (PCI DSS)**

- Contractual rules governing exchange of credit card data between banks and merchants
  - Voluntary standard
- Noncompliance may result in:
  - Higher transaction fees
  - Expensive fines
  - Inability to process credit cards



## **Import/Export Encryption Restrictions**

- Includes use to secure network communications
- U.S. export control laws handled by the Dept. of Commerce
- Administered by the Bureau of Industry and Security
- U.S. encryption export control policies rest on three principles:
  - Review of encryption products prior to sale
  - streamlined post-export reporting
  - License review of certain exports of strong encryption to foreign government end users.





## Non-U.S. Laws

- Wassenaar Arrangement
  - International agreement on export controls dealing with dual-use goods and technologies.
  - Removed key length restrictions on encryption products to allow for mass-market distribution of encryption products
  
- Cryptographic use restrictions
  - Many countries tightly restrict the use and possession of cryptographic technology.



## U.S. Digital Signature Laws

- **Signatures -**
  - A means of affixing a sign of one's approval for centuries
  - A ring and wax seal, a stamp, or a scrawl
- **Digital signatures-**
  - As communications have moved into the digital realm, there exists a need for signatures to move with the new medium
  - Means to show approval for electronic records
    - Cryptography provides integrity and non-repudiation.
    - Enables e-commerce transactions
  - Equivalent to notarized signatures for all transactions in the US for all transactions in which both parties agree to use digital signature
- **Electronic Signatures in Global and National Commerce Act (E-Sign Law)**
  - Electronic forms of signatures, contracts, and other records are just as valid and enforceable as those written on paper.



## Other Digital Signature Laws

---


- United Nations
  - UN Commission on International Trade Law Model Law on Electronic Commerce
- Canada
  - Uniform Electronic Commerce Act
- European Union
  - Electronic Commerce Directive



## Digital Millennium Copyright Act (DCMA)

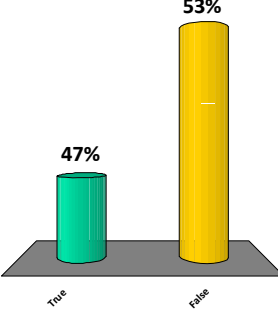
---

- **Digital Rights Management**
  - Generic term for [access control technologies](#) that can be used by [hardware manufacturers](#), [publishers](#), [copyright holders](#) and [individuals](#) to limit the usage of digital content and devices.
  - Used to describe any technology that inhibits uses of digital content not desired or intended by the content provider.
- **Digital Millennium Copyright Act (DCMA)**
  - Protects rights of recording artists.
  - Identifies how new computer technology relates to copyright laws.
  - Makes it illegal to develop, produce, and trade any device or mechanism designed to circumvent technological controls used in copy protection.




Digital signatures are equivalent to notarized signature **only for non-real property transactions** in the US in which both parties agree to use Digital signatures

1. True
2. False



Response	Percentage
True	47%
False	53%



## MSDN Alliance

- List of the available software  
<http://msdn2.microsoft.com/en-us/academic/bb676724.aspx>  
(look under “Developer AA”)
- The terms of use agreement:  
<http://msdn2.microsoft.com/en-us/academic/bb250608.aspx>
- Go to this web site:  
[http://msdn07.e-academy.com/stockton\\_cs/](http://msdn07.e-academy.com/stockton_cs/)
- click on the “Register” button, and self-register by entering their stk number, a valid email address, and select your passwords