ETHICS AND INFORMATION SECURITY: MIS BUSINESS CONCERNS

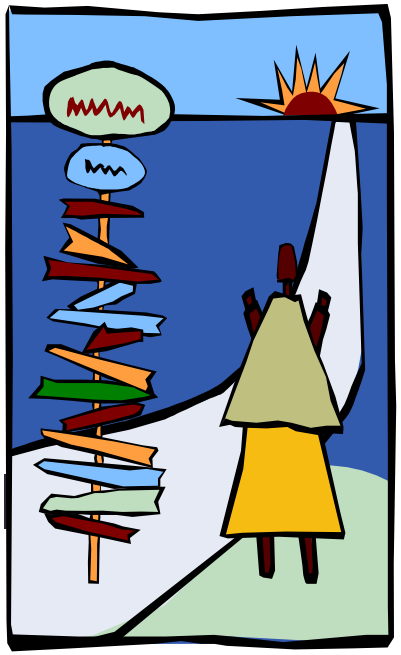
OVERVIEW

- **SECTION 4.1 – Ethics**
  - Information Ethics
  - Developing Information Management Policies
  - Ethics in the Workplace
- **SECTION 4.2 – Information Security**
  - Protecting Intellectual Assets
  - The First Line of Defense - People
  - The Second Line of Defense - Technology

PART 1
ETICS

1. Explain the ethical issues in the use of the information age
2. Identify the six epolicies an organization should implement to protect themselves

INFORMATION ETHICS



- **Ethics** – The principles and standards that guide our behavior toward other people
- **Information ethics** – Govern the ethical and moral issues arising from the development and use of information technologies, as well as the creation, collection, duplication, distribution, and processing of information itself

Clip MP3 copy rights: http ://video.google.com/videoplay?docid=1248542035906402031

INFORMATION ETHICS

Individuals copy, use, and distribute software.
Employees search organizational databases for sensitive corporate and personal information.
Organizations collect, buy, and use information without checking the validity or accuracy of the information.
Individuals create and spread viruses that cause trouble for those using and maintaining IT systems.
Individuals hack into computer systems to steal proprietary information.
Employees destroy or steal proprietary organization information such as schematics, sketches, customer lists, and reports.

FIGURE 4.1

Ethically Questionable or Unacceptable Information Technology Use

INFORMATION ETHICS

- Business issues related to information ethics
  - Intellectual property
  - Copyright
  - Fair use of doctrine
  - Pirated software
  - Counterfeit software



INFORMATION ETHICS

- Privacy is a major ethical issue
  - **Privacy** – The right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent
  - **Confidentiality** – the assurance that messages and information are available only to those who are authorized to view them



INFORMATION ETHICS

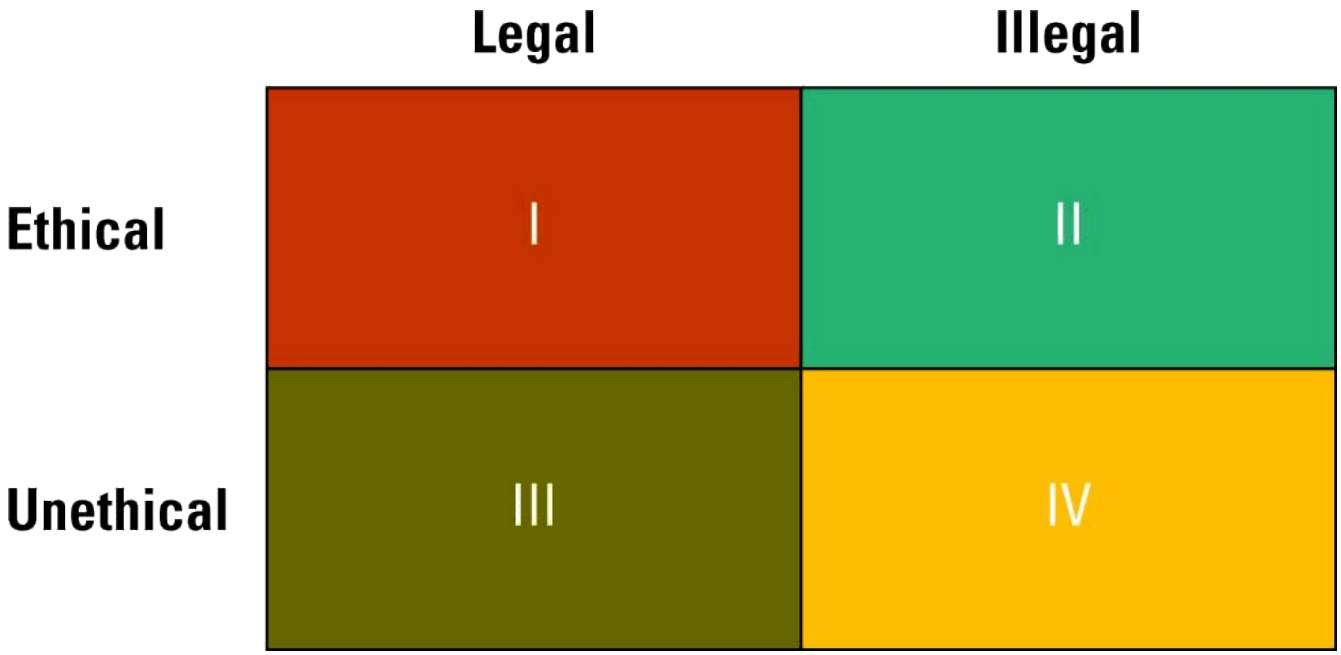
- Individuals form the only ethical component of MIS
  - Individuals ***copy***, use , and distribute software
  - Search organizational databases for sensitive and personal information
  - Individuals create and ***spread viruses***
  - Individuals ***hack*** into computer systems to steal information
  - Employees destroy and steal information



Article: The courtroom star witness pleaded guilty to faking his credentials, possibly putting several cases in question.

INFORMATION ETHICS

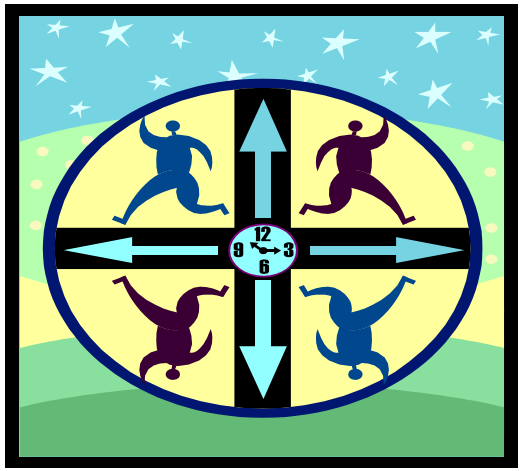
- Acting ethically and legally are not always the same



Article: schools banning iPods:
http://www.usatoday.com/tech/news/2007-04-27-ipod-cheating_N.htm

INFORMATION DOES NOT HAVE ETHICS, PEOPLE DO

- Information does not care how it is used, it will not stop itself from sending spam, viruses, or highly-sensitive information
- Tools to prevent information misuse
  - Information management IM
  - Information governance IG
  - Information compliance
  - Ediscovery



Established Information-Related Laws	
Privacy Act—1974	Restricts what information the federal government can collect; allows people to access and correct information on themselves; requires procedures to protect the security of personal information; and forbids the disclosure of name-linked information without permission.
Family Education Rights and Privacy Act—1974	Regulates access to personal education records by government agencies and other third parties and ensures the right of students to see their own records.
Cable Communications Act—1984	Requires written or electronic consent from viewers before cable TV providers can release viewing choices or other personally identifiable information.
Electronic Communications Privacy Act—1986	Allows the reading of communications by a firm and says that employees have no right to privacy when using their companies' computers.
Computer Fraud and Abuse Act—1986	Prohibits unauthorized access to computers used for financial institutions, the U.S. government, or interstate and international trade.
The Bork Bill (officially known as the Video Privacy Protection Act, 1988)	Prohibits the use of video rental information on customers for any purpose other than that of marketing goods and services directly to the customer.
Communications Assistance for Law Enforcement Act—1994	Requires that telecommunications equipment be designed so that authorized government agents are able to intercept all wired and wireless communications being sent or received by any subscriber. The act also requires that subscriber call-identifying information be transmitted to a government when and if required.
Freedom of Information Act—1967, 1975, 1994, and 1998	Allows any person to examine government records unless it would cause an invasion of privacy. It was amended in 1974 to apply to the FBI, and again in 1994 to allow citizens to monitor government activities and information gathering, and once again in 1998 to access government information on the Internet.
Health Insurance Portability and Accountability Act (HIPAA)—1996	Requires that the health care industry formulate and implement regulations to keep patient information confidential.
Identity Theft and Assumption Deterrence Act—1998	Strengthened the criminal laws governing identity theft making it a federal crime to use or transfer identification belonging to another. It also established a central federal service for victims.
USA Patriot Act—2001 and 2003	Allows law enforcement to get access to almost any information, including library records, video rentals, bookstore purchases, and business records when investigating any act of terrorist or clandestine intelligence activities. In 2003, Patriot II broadened the original law.
Homeland Security Act—2002	Provided new authority to government agencies to mine data on individuals and groups including emails and website visits; put limits on the information available under the Freedom of Information Act; and gave new powers to government agencies to declare national health emergencies.
Sarbanes-Oxley Act—2002	Sought to protect investors by improving the accuracy and reliability of corporate disclosures and requires companies to (1) implement extensive and detailed policies to prevent illegal activity within the company, and (2) to respond in a timely manner to investigate illegal activity.
Fair and Accurate Credit Transactions Act—2003	Included provisions for the prevention of identity theft including consumers' right to get a credit report free each year, requiring merchants to leave all but the last five digits of a credit card number off a receipt, and requiring lenders and credit agencies to take action even before a victim knows a crime has occurred when they notice any circumstances that might indicate identity theft.
CAN-Spam Act—2003	Sought to regulate interstate commerce by imposing limitations and penalties on businesses sending unsolicited email to consumers. The law forbids deceptive subject lines, headers, return addresses, etc., as well as the harvesting of email addresses from websites. It requires businesses that send spam to maintain a do-not-spam list and to include a postal mailing address in the message.

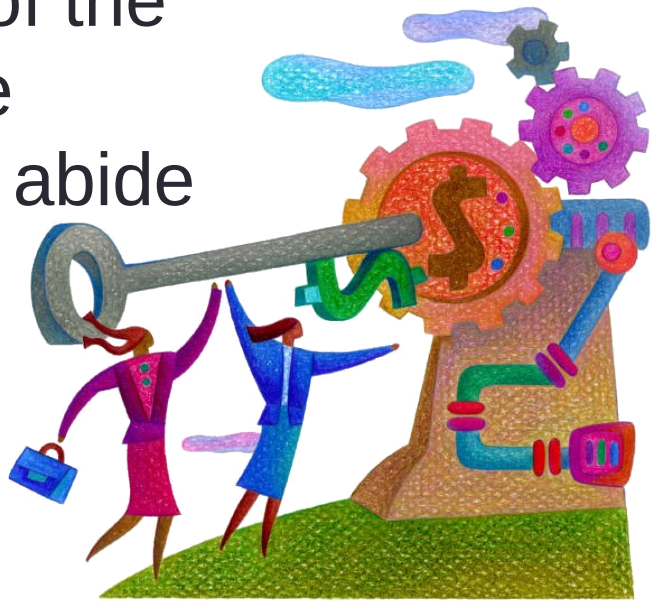
DEVELOPING INFORMATION MANAGEMENT POLICIES

- Organizations strive to build a corporate culture based on ethical principles that employees can understand and implement
- Epolicies typically include:
  - Ethical computer use policy
  - Information privacy policy
  - Acceptable use policy
  - Email privacy policy
  - Social media policy
  - Workplace monitoring policy



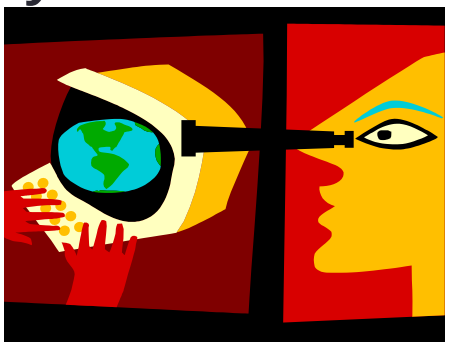
ETHICAL COMPUTER USE POLICY

- **Ethical computer use policy** – Contains general principles to guide computer user behavior
- The ethical computer user policy ensures all users are **informed** of the rules and, by agreeing to use the system on that basis, consent to abide by the rules



INFORMATION PRIVACY POLICY

- The unethical use of information typically occurs “unintentionally” when it is used for new purposes
- **Information privacy policy** - Contains general principles regarding information privacy



CEO steals IDs: example of information misuse

http://www.usatoday.com/tech/news/2006-11-02-ceo-id-theft_x.htm

ACCEPTABLE USE POLICY

- **Acceptable use policy (AUP)** – Requires a user to agree to follow it to be provided access to corporate email, information systems, and the Internet
- **Nonrepudiation** – A ***contractual stipulation*** to ensure that ebusiness participants do not deny their online actions
- **Internet use policy** – Contains general principles to guide the proper use of the Internet

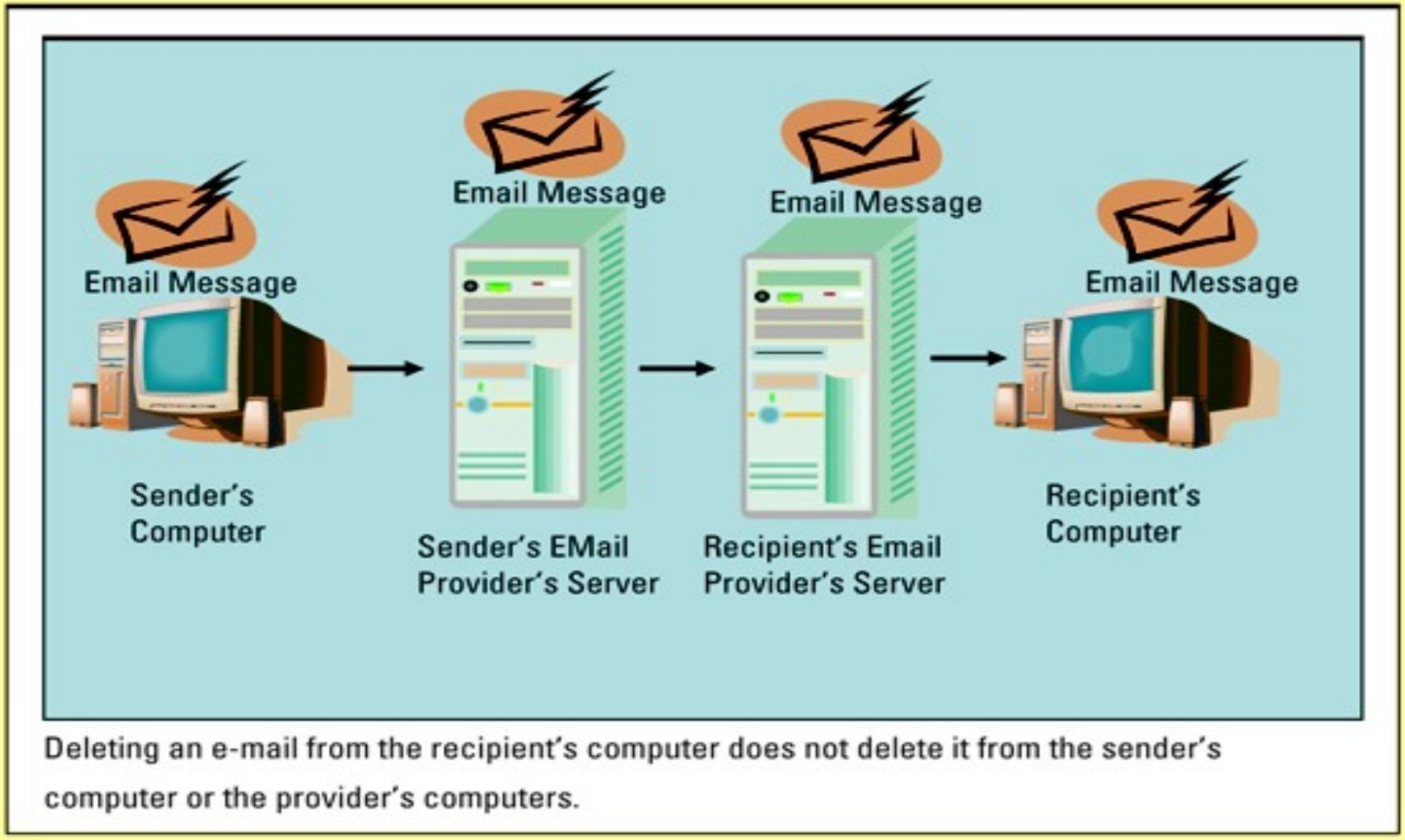
EMAIL PRIVACY POLICY

- Organizations can mitigate the risks of email and instant messaging communication tools by implementing and adhering to an email privacy policy
- **Email privacy policy** – Details the extent to which email messages may be read by others

http://www.eweek.com/c/a/IT-Management/Youre-Not-the-Only-One-Reading-Your-EMail/



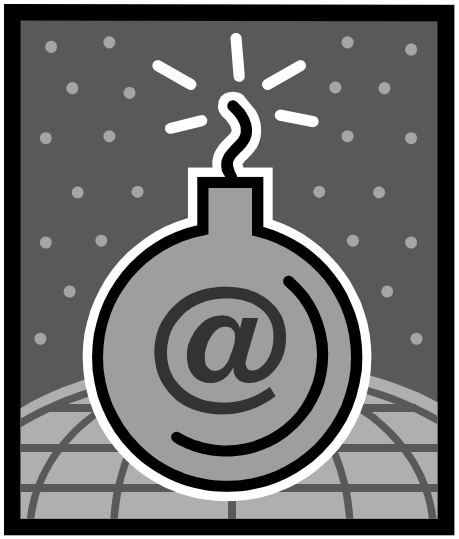
EMAIL PRIVACY POLICY



Deleting an e-mail from the recipient's computer does not delete it from the sender's computer or the provider's computers.

EMAIL PRIVACY POLICY

- **Spam** – Unsolicited email
- **Anti-spam policy** – Simply states that email users will not send unsolicited emails (or spam)



SOCIAL MEDIA POLICY

- **Social media policy** – Outlines the corporate guidelines or principles governing employee online communications ***(check blogs, message boards, USB drive policy)***



WORKPLACE MONITORING POLICY

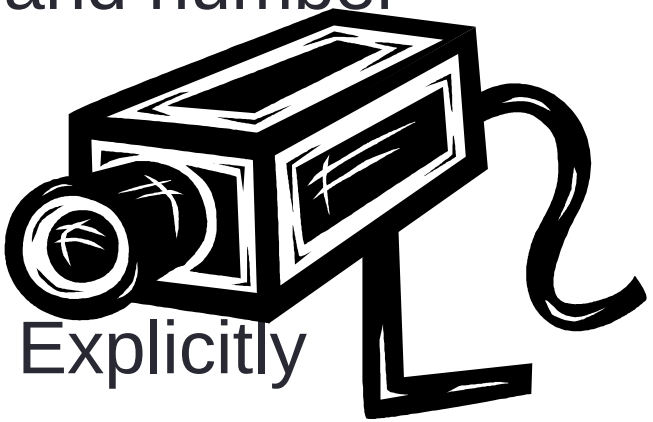
- Workplace monitoring is a concern for many employees
- Organizations can be held financially responsible for their employees' actions
- The dilemma surrounding employee monitoring in the workplace is that an organization is placing itself at risk if it fails to monitor its employees, however, some people feel that monitoring employees is unethical

Classroom Exercise

- ***debate?***
  - Workplace monitoring unethical? Or necessary?

WORKPLACE MONITORING POLICY

- **Information technology monitoring** – Tracks people's activities by such measures as number of keystrokes, error rate, and number of transactions processed



- **Employee monitoring policy** – Explicitly state how, when, and where the company monitors its employees
- article: http://www.law.duke.edu/journals/dltr/articles/2001dltr0026.html

WORKPLACE MONITORING POLICY

- Common monitoring technologies include:
  - Key logger or key trapper software/hardware
  - Cookie
  - Spyware
  - Clickstream



PART 2
INFORMATION SECURITY

3. Describe the relationships and differences between hackers and viruses
4. Describe the relationship between information security policies and an information security plan
5. Provide an example of each of the three primary security areas: (1) authentication and authorization, (2) prevention and resistance, and (3) detection and response

PROTECTING INTELLECTUAL ASSETS

Organizational information is intellectual capital - it must be protected

Information security – The protection of information from accidental or intentional misuse by persons inside or outside an organization



Clip: http://www.youtube.com/watch?v=-4LtYMNl4yw (an example of ebusiness creating security risks, and amount of information freely flowing over internet)

SECURITY THREATS CAUSED BY HACKERS AND VIRUSES

- **Hacker –** Experts in technology who use their knowledge to break into computers and computer networks, either for profit or just motivated by the challenge
  - Black-hat hacker
  - Cracker (criminal hacker)
  - Cyberterrorist
  - Hactivist
  - Script kiddies or script bunnies (spread viruses)
  - White-hat hacker



CLIP on hacking

http://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm

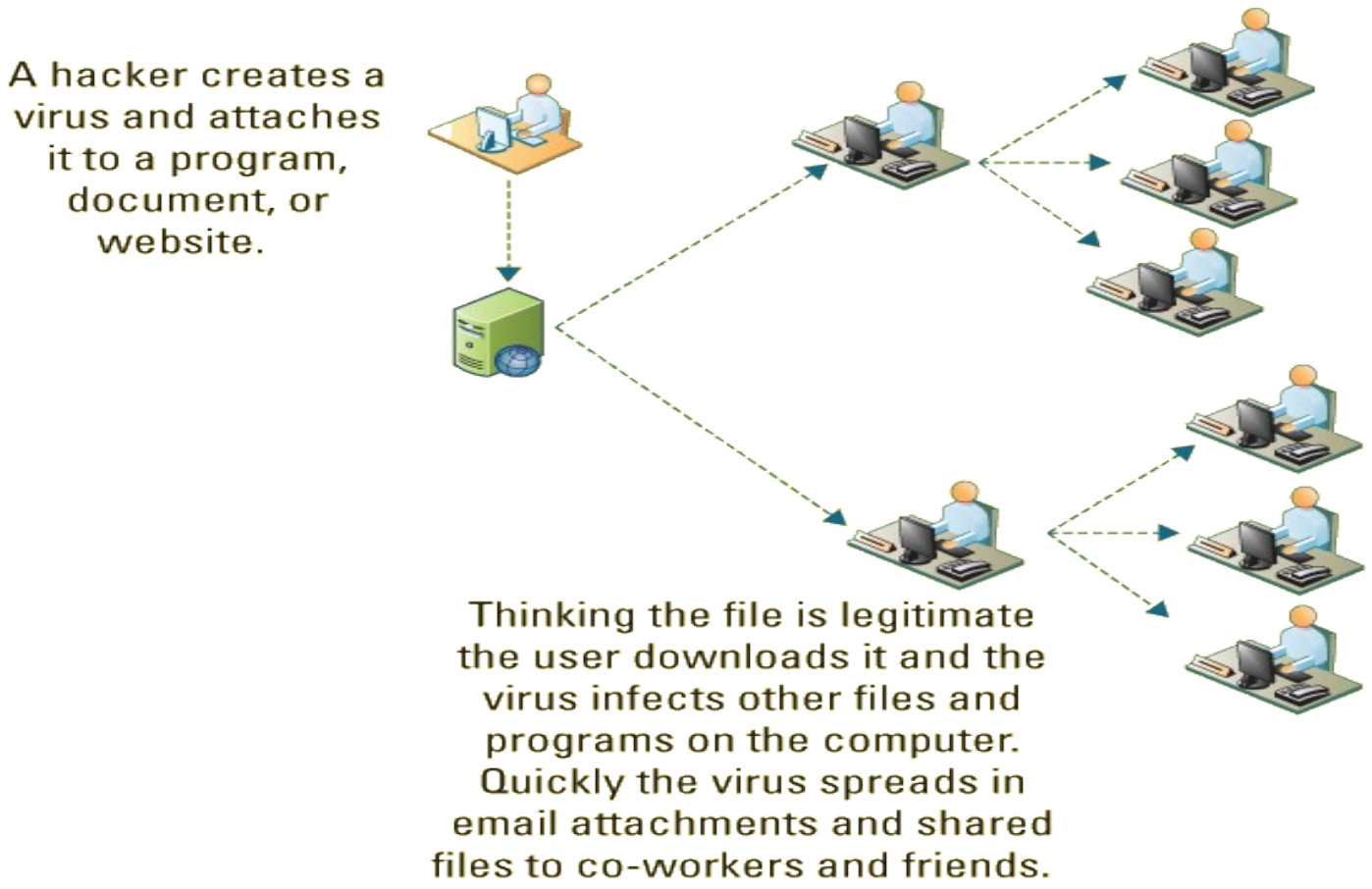
SECURITY THREATS CAUSED BY HACKERS AND VIRUSES

- **Virus** - Software written with malicious intent to cause annoyance or damage
  - Denial-of-service attack (DoS)
  - Distributed denial-of-service attack (DDoS)
  - Worm (email attachment)
  - Polymorphic virus (program that opens door for future attack)
  - Backdoor program (virus that opens door for future attack)
  - Trojan-horse virus (hides in software)



SECURITY THREATS CAUSED BY HACKERS AND VIRUSES

How Computer Viruses Spread



SECURITY THREATS CAUSED BY HACKERS AND VIRUSES

- Security threats to ebusiness include
  - Elevation of privilege
  - Hoaxes (transmit virus with virus attached)
  - Malicious code (virus, worms, Trojan horses)
  - Packet tampering
  - Sniffer (tx data monitoring software)
  - Spoofing (forging return address of email)
  - Splogs (fake blog to promote affiliate website)
  - Spyware (free bee software, tracks online movement, mines information stored etc.)



THE FIRST LINE OF DEFENSE - PEOPLE

- Organizations must enable employees, customers, and partners to access information electronically
- The biggest issue surrounding information security is not a technical issue, but a people issue
  - **Insiders**
  - **Social engineering**
  - **Dumpster diving**



THE FIRST LINE OF DEFENSE - PEOPLE

- The first line of defense an organization should follow to help combat insider issues is to develop information security policies and an information security plan
  - **Information security policies (rules)**
  - **Information security plan** (action plan)



THE SECOND LINE OF DEFENSE - TECHNOLOGY

- There are three primary information technology security areas
  1. People: Authentication and authorization
  2. Data: Prevention and resistance
  3. Attack: Detection and response



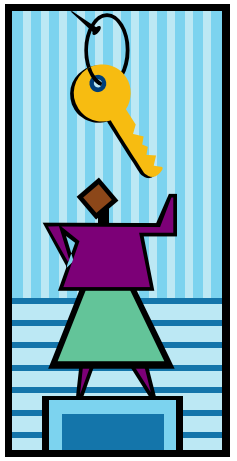
AUTHENTICATION AND AUTHORIZATION

- **Identity theft** – The forging of someone's identity for the purpose of fraud
- **Phishing** – A technique to gain personal information for the purpose of identity theft, usually by means of fraudulent email
- **Pharming** – Reroutes requests for legitimate websites to false websites



AUTHENTICATION AND AUTHORIZATION

- **Authentication** – A method for confirming users' identities
- **Authorization –** The process of giving someone permission to do or have something
- The most secure type of authentication involves
  1. Something the user knows
  2. Something the user has
  3. Something that is part of the user



SOMETHING THE USER KNOWS SUCH AS A USER ID AND PASSWORD

- This is the most common way to identify individual users and typically contains a user ID and a password
- This is also the most *ineffective* form of authentication
- Over 50 percent of help-desk calls are password related



SOMETHING THE USER KNOWS SUCH AS A USER ID AND PASSWORD

- Smart cards and tokens are more effective than a user ID and a password
  - **Tokens** – Small electronic devices t used to ease authentication
  - **Smart card** – A device in shape of a small card, containing embedded technologies that can store information and small amounts of software to perform some limited processing





SOMETHING THAT IS PART OF THE USER SUCH AS A FINGERPRINT OR VOICE SIGNATURE

- This is by far the best and most effective way to manage authentication
  - **Biometrics** – The identification of a user based on a physical characteristic, such as a fingerprint, iris, face, voice, or handwriting
- Unfortunately, this method can be costly and intrusive



PREVENTION AND RESISTANCE

- Downtime can cost an organization anywhere from $100 to $1 million per hour
- Technologies available to help prevent and build resistance to attacks include
  1. Content filtering
  2. Encryption
  3. Firewalls



System Downtime

- **Downtime** – Refers to a period of time when a system is unavailable

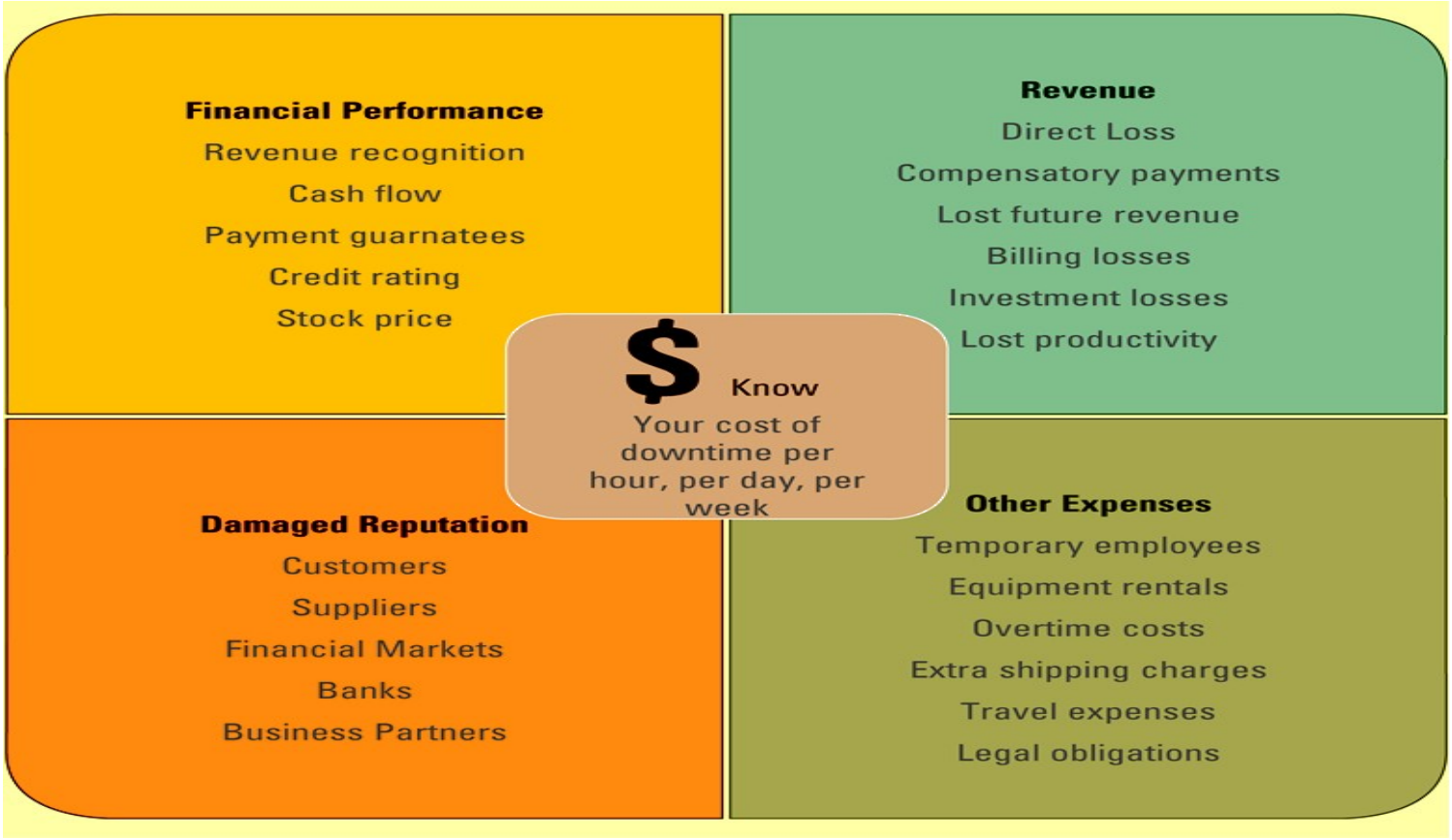
PROTECTING INTELLECTUAL ASSETS

Sources of Unplanned Downtime

Bomb threat	Hacker	Snowstorm
Burst pipe	Hail	Sprinkler malfunction
Chemical spill	Hurricane	Static electricity
Construction	Ice storm	Strike
Corrupted data	Insects	Terrorism
Earthquake	Lightning	Theft
Electrical short	Network failure	Tornado
Epidemic	Plane crash	Train derailment
Equipment failure	Frozen pipe	Smoke damage
Evacuation	Power outage	Vandalism
Explosion	Power surge	Vehicle crash
Fire	Rodents	Virus
Flood	Sabotage	Water damage (various)
Fraud	Shredded data	Wind

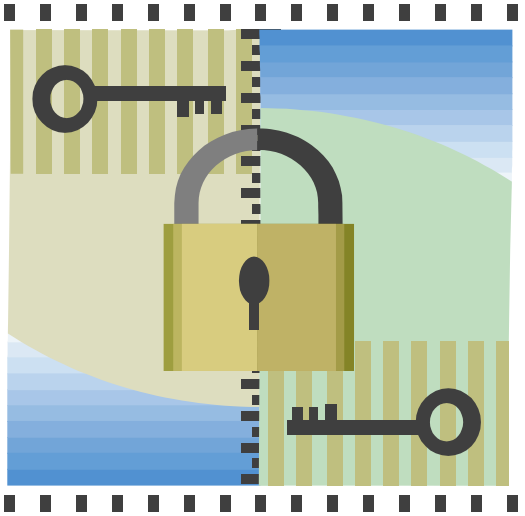
PROTECTING INTELLECTUAL ASSETS

How Much Will Downtime Cost Your Business?



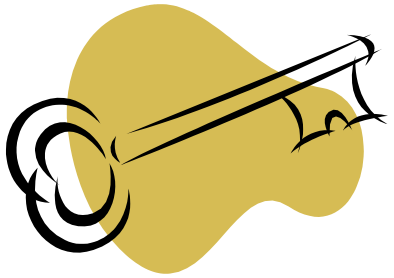
PREVENTION AND RESISTANCE

- **Content filtering** - Prevents emails containing sensitive information from transmitting and stops spam and viruses from spreading

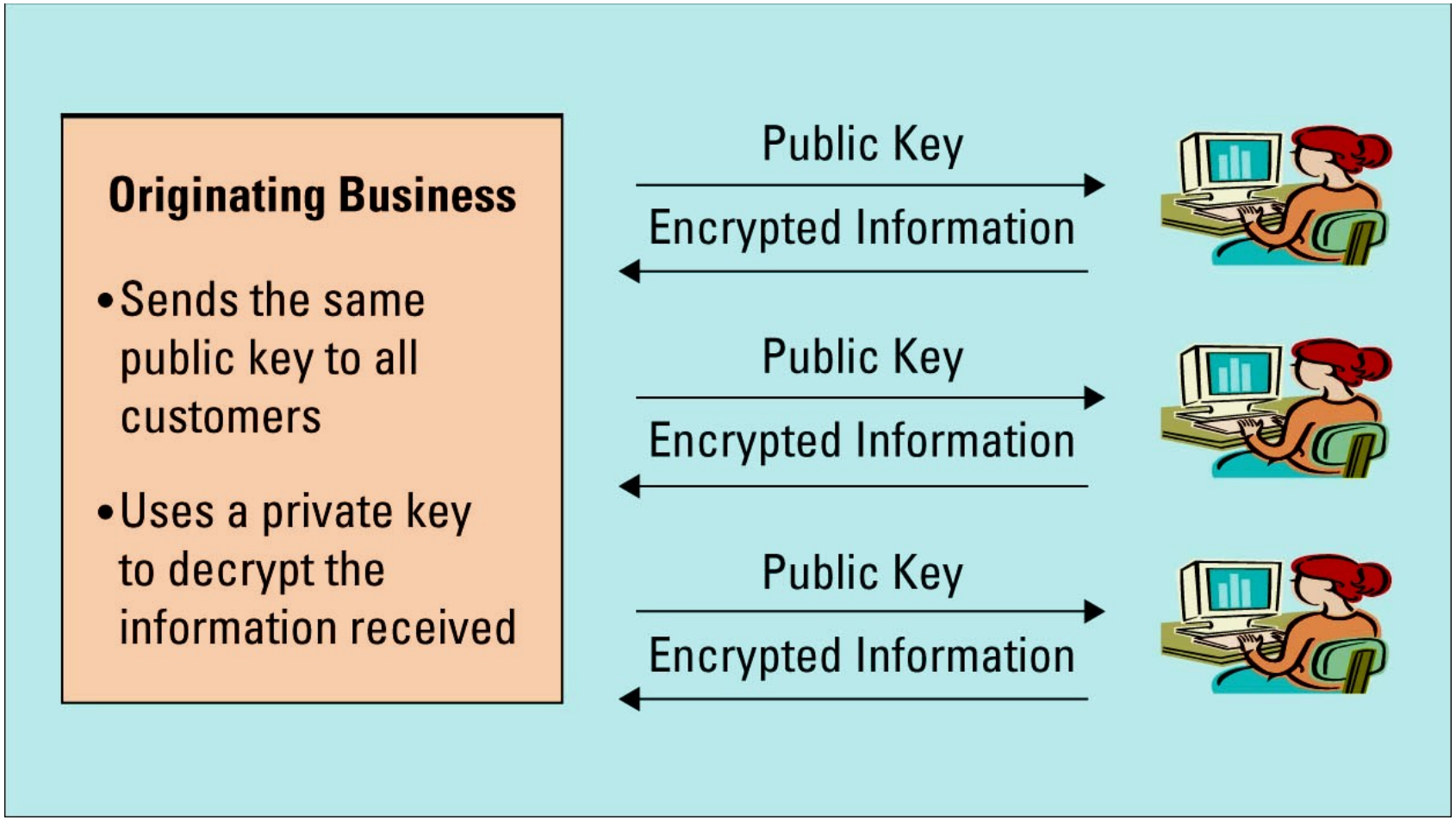


PREVENTION AND RESISTANCE

- If there is an information security breach and the information was encrypted, the person stealing the information would be unable to read it
  - **Encryption**
  - **Public key encryption (PKE)**
  - **Certificate authority**
  - **Digital certificate**



PREVENTION AND RESISTANCE



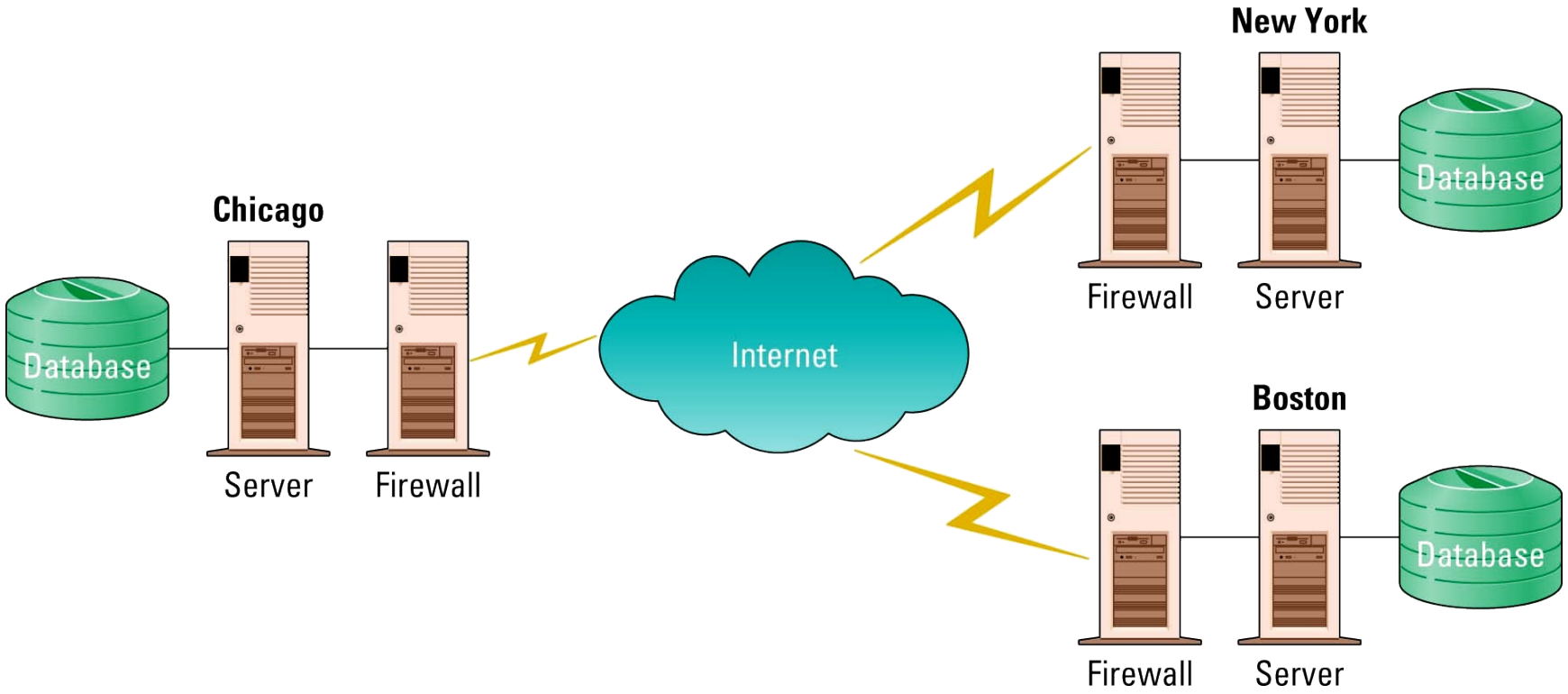
PREVENTION AND RESISTANCE

- One of the most common defenses for preventing a security breach is a firewall
- **Firewall** – Hardware and/or software that guards a private network by analyzing the information leaving and entering the network (examines all messages sent to network, only message with correct marking is allowed)



PREVENTION AND RESISTANCE

- Sample firewall architecture connecting systems located in Chicago, New York, and Boston



DETECTION AND RESPONSE

- If prevention and resistance strategies fail and there is a security breach, an organization can use detection and response technologies to mitigate the damage
- **Intrusion detection software** – Features full-time monitoring tools that search for patterns in network traffic to identify intruders

