# Management Information Systems

Ethics, Privacy and Information Security

Dr. Shankar Sundaresan

## LEARNING OBJECTIVES

- Describe the major ethical issues related to information technology and identify situations in which they occur.
- Describe the many threats to information security.
- Understand the various defense mechanisms used to protect information systems.
- Explain IT auditing and planning for disaster recovery.

## Fundamental Tenets of Ethics

- Responsibility
  - Accepting the consequences of your decisions and actions.
- Accountability
  - determination of who is responsible for actions that were taken.
- Liability
  - legal concept meaning that individuals have the right to recover the damages done to them

## Ethical Scenario: File Sharing

- You have recently bought some graphic design software that is a far superior product, you believe, to its competitors on the market. The price is rather high, but the purchase was authorised by your boss for work related purposes. The software is delivered on a single CD ROM. You believe that many of your friends who work for other companies would benefit if they were able to use this software – and that the software developer would benefit as well through additional sales. From an ethical perspective, you believe that it would be unethical to keep this information to yourself, given its likely value for your friends, so you decide to share it with them. You make 10 copies on CD ROM and send it to them as a gift.
- Is this action legal?
- Is it ethical?
- What would you do?

## The Four Categories of Ethical Issues

- Privacy Issues
  - collecting, storing and disseminating information about individuals.
- Accuracy Issues
  - authenticity, fidelity and accuracy of information that is collected and processed.
- Property Issues
  - the ownership and value of information.
- Accessibility Issues
  - who should have access to information and whether they should have to pay for this access.

## Privacy

- Privacy. The right to be left alone and to be free of unreasonable personal intrusions.
- Court decisions have followed two rules:

  (1) The right of privacy is not absolute. Your privacy must be balanced against the needs of society.

  (2) The public's right to know is superior to the individual's right of privacy.

## Threats to Privacy

- Data aggregators
  - companies that collect *public data* (e.g., real estate records, telephone numbers) and *nonpublic data* (e.g., social security numbers, financial data, police records, motor vehicle records) and integrate them to produce digital dossiers.
- digital dossiers, and profiling
- Electronic Surveillance
- Personal Information in Databases
- Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites

## Personal Information in Databases

- Banks
- Utility companies
- Government agencies
- Credit reporting agencies

EQUIFAX

TransUnion

experian

## Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites

flickr

friendster

myspace.com

LinkedIn

twitter

facebook

## Protecting Privacy

- Privacy Codes and Policies
  - Opt-out Model
  - Opt-in Model

## Factors Increasing the Threats to Information Security

- Today's interconnected, interdependent, wirelessly-networked business environment
- Government legislation
- Smaller, faster, cheaper computers and storage devices
- Decreasing skills necessary to be a computer hacker
- International organized crime turning to cybercrime
- Downstream liability
- Increased employee use of unmanaged devices
- Lack of management support

## Key Information Security Terms

- Threat
  - is any danger to which a system may be exposed.
- Exposure
  - is the harm, loss or damage that can result if a threat compromises that resource.
- Vulnerability
  - the possibility that the system will suffer harm by a threat.
- Risk
  - the likelihood that a threat will occur.
- Information system controls
  - are the procedures, devices, or software aimed at preventing a compromise to the system.

## Categories of Threats to Information Systems

- Unintentional acts
- Natural disasters
- Technical failures
- Management failures
- Deliberate acts

(from Whitman and Mattord, 2003)

Example of a threat (video)

## Unintentional Acts

- Human errors
- Deviations in quality of service by service providers (e.g., utilities)
- Environmental hazards (e.g., dirt, dust, humidity)

## Human Errors

- Tailgating
- Shoulder surfing
- Carelessness with laptops and portable computing devices
- Opening questionable e-mails
- Careless Internet surfing
- Poor password selection and use
- And more

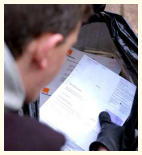
**Human Mistakes**

| Human Mistake | Description and Examples |
|---|---|
| Tailgating | A technique designed to allow the perpetrator to enter restricted areas that are controlled with locks or card entry. The perpetrator follows closely behind a legitimate employee and, when the employee gains entry, asks the legitimate employee to "hold the door." |
| Shoulder surfing | The perpetrator watches the employee's computer screen over that person's shoulder. This technique is particularly successful in public areas such as airports, commuter trains, and on airplanes. |
| Carelessness with laptops | Losing laptops, misplacing laptops, leaving them in taxis, and so on. |
| Carelessness with portable devices | Losing or misplacing these devices, or using them carelessly so that malware is introduced into an organization's network. |
| Opening questionable e-mails | Opening e-mails from someone unknown or clicking on links embedded in e-mails (see phishing attacks below). |
| Careless Internet surfing | Accessing questionable Web sites; can result in malware and/or alien software being introduced into the organization's network. |
| Poor password selection and use | Choosing and using weak passwords (see strong passwords below). |
| Carelessness with one's office | Unlocked desks and filing cabinets when employees go home at night; not logging off the company network when gone from the office for any extended period of time. |
| Carelessness using unmanaged devices | Unmanaged devices are those outside the control of an organization's IT department and company security procedures. These devices include computers belonging to customers and business partners, computers in the business centers of hotels, and computers in Starbucks, Paneras, and so on. |
| Carelessness with discarded equipment | Discarding old computer hardware and devices without completely wiping the memory; includes computers, cell phones, Blackberries, and digital copiers and printers. |

table_03_03

## Deliberate Acts

- Espionage or trespass
- Information extortion
- Sabotage or vandalism
- Theft of equipment or information
  - For example, dumpster diving



## Deliberate Acts (continued)

- Identity theft video
- Compromises to intellectual property
  - Intellectual property
  - Property created by individuals or corporations which is protected under *trade secret*, *patent,* and *copyright* laws.
  - Trade secret
  - Intellectual work, such as a business plan, that is a company secret and is not based on public information.
  - Patent
  - Document that grants the holder exclusive rights on an invention or process for 20 years.
  - Copyright
  - Statutory grant that provides creators of intellectual property with ownership rights for life of the creator plus 70 years.

## Deliberate Acts (continued)

- Software attacks
  - Virus
  - Worm
  - Trojan horse
  - Logic Bomb

## Deliberate Acts (continued)

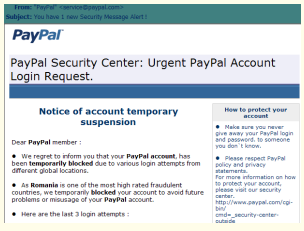
- Software attacks (continued)
  - Phishing attacks
    - use deception to acquire sensitive personal information by masquerading as official-looking e-mails or instant messages.
    - Phishing slideshow
    - Phishing quiz
    - Phishing example
    - Phishing example
  - Distributed denial-of-service attacks
    - See botnet demonstration

## Is the email really from eBay, or PayPal, or a bank?

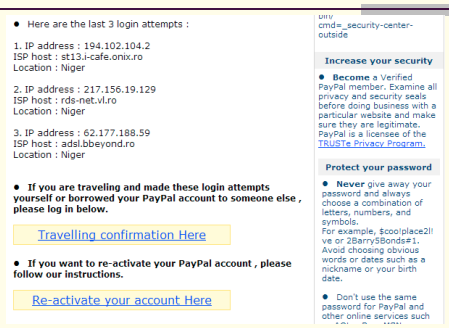
As an example, here is what the email said:

- Return-path: <service@paypal.com>
- From: "PayPal"<service@paypal.com>
- Subject: You have 1 new Security Message Alert !

Note that they even give advice in the right column about security



## Example Continued – bottom of the email



- Here are the last 3 login attempts :

1. IP address : 194.102.104.2
ISP host : st13.i-cafe.onix.ro
Location : Niger

2. IP address : 217.156.19.129
ISP host : rds-net.vl.ro
Location : Niger

3. IP address : 62.177.188.59
ISP host : adsl.bbeyond.ro
Location : Niger

- **If you are traveling and made these login attempts yourself or borrowed your PayPal account to someone else , please log in below.**

Travelling confirmation Here

- **If you want to re-activate your PayPal account , please follow our instructions.**

Re-activate your account Here

cmd=_security-center-outside

**Increase your security**

- **Become** a Verified PayPal member. Examine all privacy and security seals before doing business with a particular website and make sure they are legitimate. PayPal is a licensee of the TRUSTe Privacy Program.

**Protect your password**

- **Never** give away your password and always choose a combination of letters, numbers, and symbols. For example, $coolplace2l! ve or 2BarrySBonds#1. Avoid choosing obvious words or dates such as a nickname or your birth date.
- Don't use the same password for PayPal and other online services such

## How to see what is happening
### View Source

- In **Outlook**, right click on email, click 'view source'
- In **GroupWise**, open email and click on the Message Source tab
- In **Mozilla Thunderbird**, click on View, and Source.
- Below is the part of the text that makes the email look official – the images came from the PayPal website.

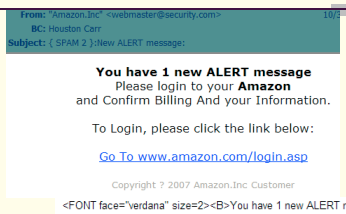
```
<table width=3D"100%" cellspacing=3D"0" cellpadding=3D"0" border=3D"0">
<tr>
        <td background=3D"http://images.paypal.com/images/bg_clk.gif"
width=3D100%><img src=3D"http://images.paypal.com/images/pixel.gif"=20
height=3D"29"
width=3D"1" border=3D"0"></td>
</tr>=09
=09
<tr>
        <td><img src=3D"http://images.paypal.com/images/pixel.gif"=20
height=3D"10"
width=3D"1" border=3D"0"></td>
</tr>
</table>
```

## View Source – The Real Link

```
class=3D"pp_sansserif" align=3D"center"><a
href=3D"ftp://futangiu:futangiu@209.202.224.140/index.htm">Travelling=20
confirmation Here</a></td>
```

- In the body it said, "If you are traveling, "Travelling Confirmation Here"
- Here is where you are really being sent
  - **href=3Dftp://futangiu:futangiu@209.202.224.140/index.htm**
- Notice that the link is not only not PayPal, it is an IP address, 2 giveaways of a fraudulent link.

## Another Example – Amazon




View Source

```
<FONT face="verdana" size=2><B>You have 1 new ALERT message
</B><BR>
Please login to your <B>Amazon</B><BR> and Confirm Billing And your
Information.<BR><BR>
To Login, please click the link below:<BR><BR>
<a href="http://68-116-36-144.static.mdfd.or.charter.com/Online.htm">Go To
www.amazon.com/login.asp </a></font></p>
<p><font size="2" face="Arial, Helvetica, sans-serif">
```

## Deliberate Acts (continued)

- Alien Software
  - Spyware (see video)
    - collects personal information about users without their consent.
    - keystroke loggers (keyloggers)
      - record your keystrokes and your Web browsing history
    - screen scrapers
      - record a continuous "movie" of what you do on a screen.
  - Spamware
    - alien software that is designed to use your computer as a launchpad for spammers
  - Cookies demo
    - small amounts of information that Web sites store on your

## Risk Management

- Risk
  - The probability that a threat will impact an information resource.
- Risk management
  - To identify, control and minimize the impact of threats.
- Risk analysis
  - To assess the value of each asset being protected, estimate the probability it might be compromised, and compare the probable costs of it being compromised with the cost of protecting it.
- Risk mitigation

## Risk Mitigation Strategies

when the organization takes concrete actions against risk. It has two functions:

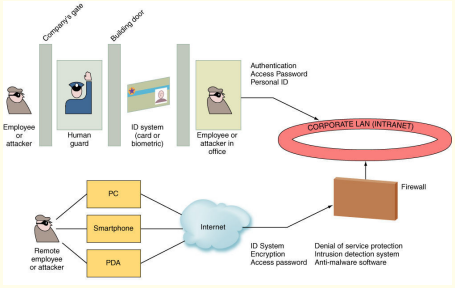
- (1) implement controls to prevent identified threats from occurring, and
- (2) developing a means of recovery should the threat become a reality.

- Risk Mitigation Strategies
  - Risk Acceptance
  - Risk limitation
  - Risk transference

## Controls

- Physical controls
  - Physical protection of computer facilities and resources.
- Access controls
  - Restriction of unauthorized user access to computer resources; use **biometrics** and **passwords** controls for user identification.
- Communications (network) controls
  - To protect the movement of data across networks and include border security controls, authentication and authorization
- Application controls

## Where Defense Mechanisms (Controls) Are Located



## Access Controls

- Authentication
  - Something the user is (biometrics)
    - Video on biometrics
    - The latest biometric: gait recognition
    - The Raytheon Personal Identification Device
  - Something the user has
  - Something the user does
  - Something the user knows

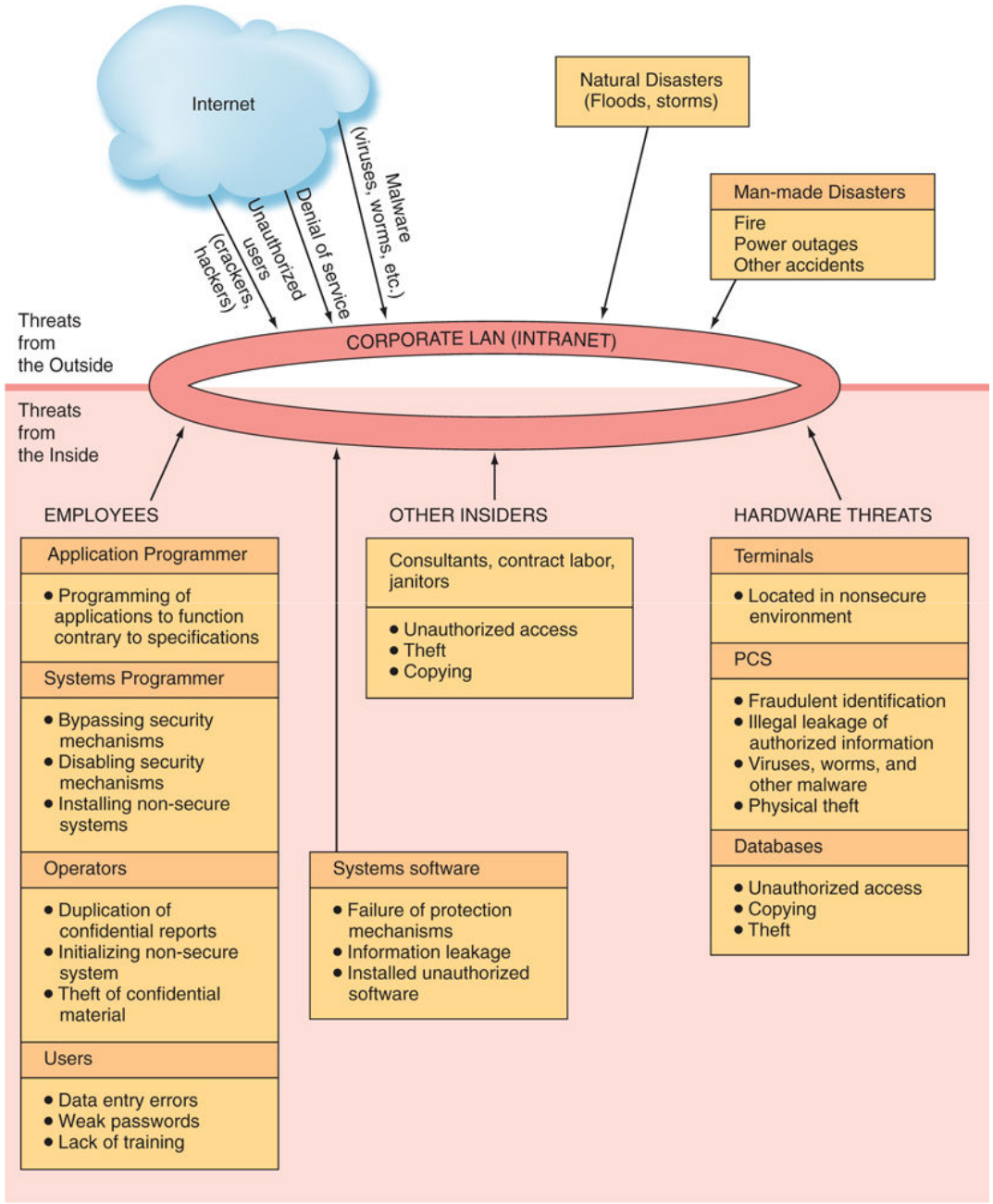

Internet
Natural Disasters
(Floods, storms)
Man-made Disasters
Fire
Power outages
Other accidents
Malware
(viruses, worms, etc.)
Denial of service
Unauthorized
users
(crackers,
hackers)
Threats
from
the Outside
CORPORATE LAN (INTRANET)
Threats
from
the Inside
EMPLOYEES
OTHER INSIDERS
HARDWARE THREATS
Application Programmer
• Programming of applications to function contrary to specifications
Systems Programmer
• Bypassing security mechanisms
• Disabling security mechanisms
• Installing non-secure systems
Operators
• Duplication of confidential reports
• Initializing non-secure system
• Theft of confidential material
Users
• Data entry errors
• Weak passwords
• Lack of training
Consultants, contract labor, janitors
• Unauthorized access
• Theft
• Copying
Systems software
• Failure of protection mechanisms
• Information leakage
• Installed unauthorized software
Terminals
• Located in nonsecure environment
PCS
• Fraudulent identification
• Illegal leakage of authorized information
• Viruses, worms, and other malware
• Physical theft
Databases
• Unauthorized access
• Copying
• Theft

fig_03_01

## A Framework for Ethical Issues

### Privacy Issues

- What information about oneself should an individual be required to reveal to others?
- What kind of surveillance can an employer use on its employees?
- What types of personal information can people keep to themselves and not be forced to reveal to others?
- What information about individuals should be kept in databases, and how secure is the information there?

### Accuracy Issues

- Who is responsible for the authenticity, fidelity, and accuracy of the information collected?
- How can we ensure that the information will be processed properly and presented accurately to users?
- How can we ensure that errors in databases, data transmissions, and data processing are accidental and not intentional?
- Who is to be held accountable for errors in information, and how should the injured parties be compensated?

### Property Issues

- Who owns the information?
- What are the just and fair prices for its exchange?
- How should one handle software piracy (copying copyrighted software)?
- Under what circumstances can one use proprietary databases?
- Can corporate computers be used for private purposes?
- How should experts who contribute their knowledge to create expert systems be compensated?
- How should access to information channels be allocated?

### Accessibility Issues

- Who is allowed to access information?
- How much should companies charge for permitting accessibility to information?
- How can accessibility to computers be provided for employees with disabilities?
- Who will be provided with equipment needed for accessing information?
- What information does a person or an organization have a right or a privilege to obtain, under what conditions and with what safeguards?

table_03_01

## Privacy Policy Guidelines: A Sampler

### Data Collection

- Data should be collected on individuals only for the purpose of accomplishing a legitimate business objective.
- Data should be adequate, relevant, and not excessive in relation to the business objective.
- Individuals must give their consent before data pertaining to them can be gathered. Such consent may be implied from the individual's actions (e.g., applications for credit, insurance, or employment).

### Data Accuracy

- Sensitive data gathered on individuals should be verified before they are entered into the database.
- Data should, where and when necessary, be kept current.
- The file should be made available so the individual can ensure that the data are correct.
- If there is disagreement about the accuracy of the data, the individual's version should be noted and included with any disclosure of the file.

### Data Confidentiality

- Computer security procedures should be implemented to ensure against unauthorized disclosure of data. These procedures should include physical, technical, and administrative security measures.
- Third parties should not be given access to data without the individual's knowledge or permission, except as required by law.
- Disclosures of data, other than the most routine, should be noted and maintained for as long as the data are maintained.
- Data should not be disclosed for reasons incompatible with the business objective for which they are collected.

## Human Mistakes

| Human Mistake | Description and Examples |
|---|---|
| Tailgating | A technique designed to allow the perpetrator to enter restricted areas that are controlled with locks or card entry. The perpetrator follows closely behind a legitimate employee and, when the employee gains entry, asks the legitimate employee to "hold the door." |
| Shoulder surfing | The perpetrator watches the employee's computer screen over that person's shoulder. This technique is particularly successful in public areas such as airports, commuter trains, and on airplanes. |
| Carelessness with laptops | Losing laptops, misplacing laptops, leaving them in taxis, and so on. |
| Carelessness with portable devices | Losing or misplacing these devices, or using them carelessly so that malware is introduced into an organization's network. |
| Opening questionable e-mails | Opening e-mails from someone unknown or clicking on links embedded in e-mails (see phishing attacks below). |
| Careless Internet surfing | Accessing questionable Web sites; can result in malware and/or alien software being introduced into the organization's network. |
| Poor password selection and use | Choosing and using weak passwords (see strong passwords below). |
| Carelessness with one's office | Unlocked desks and filing cabinets when employees go home at night; not logging off the company network when gone from the office for any extended period of time. |
| Carelessness using unmanaged devices | Unmanaged devices are those outside the control of an organization's IT department and company security procedures. These devices include computers belonging to customers and business partners, computers in the business centers of hotels, and computers in Starbucks, Paneras, and so on. |
| Carelessness with discarded equipment | Discarding old computer hardware and devices without completely wiping the memory; includes computers, cell phones, Blackberries, and digital copiers and printers. |

table_03_03

| Types of Software Attacks | Description |
|---|---|
| Virus | Segment of computer code that performs malicious actions by attaching to another computer program. |
| Worm | Segment of computer code that performs malicious actions and will replicate, or spread, by itself (without requiring another computer program). |
| Trojan Horse | Software programs that hide in other computer programs and reveal their designed behavior only when they are activated. |
| Back Door | Typically a password, known only to the attacker, that allows him or her to access a computer system at will, without having to go through any security procedures (also called trap door). |
| Logic Bomb | Segment of computer code that is embedded with an organization's existing computer programs and is designed to activate and perform a destructive action at a certain time or date. |
| Password Attack | |
| Dictionary Attack | Attacks that try combinations of letters and numbers that are most likely to succeed, such as all words from a dictionary. |
| Brute Force Attack | Attacks that use massive computing resources to try every possible combination of password options to uncover a password. |
| Denial-of-Service Attack | Attacker sends so many information requests to a target computer system that the target cannot handle them successfully and typically crashes (i.e., ceases to function). |
| Distributed Denial-of-Service Attack | An attacker first takes over many computers, typically by using malicious software. These computers are called *zombies*, or *bots*. The attacker uses these bots (which form a *botnet*) to deliver a coordinated stream of information requests to a target computer, causing it to crash. |
| Phishing Attack | Phishing attacks use deception to acquire sensitive personal information by masquerading as official-looking e-mails or instant messages. |
| Zero-day Attack | A zero-day attack takes advantage of a newly discovered, previously unknown vulnerability in a software product. Perpetrators attack the vulnerability before the software vendor can prepare a patch for the vulnerability. |

table_03_04

## The Difficulties in Protecting Information Resources

- Hundreds of potential threats exist.
- Computing resources may be situated in many locations.
- Many individuals control information assets.
- Computer networks can be located outside the organization and are difficult to protect.
- Rapid technological changes make some controls obsolete as soon as they are installed.
- Many computer crimes are undetected for a long period of time, so it is difficult to learn from experience.
- People tend to violate security procedures because the procedures are inconvenient.
- The amount of computer knowledge necessary to commit computer crimes is usually minimal. As a matter of fact, one can learn hacking, for free, on the Internet.
- The cost of preventing hazards can be very high. Therefore, most organizations simply cannot afford to protect against all possible hazards.
- It is difficult to conduct a cost-benefit justification for controls before an attack occurs because it is difficult to assess the value of a hypothetical attack.

table_03_05