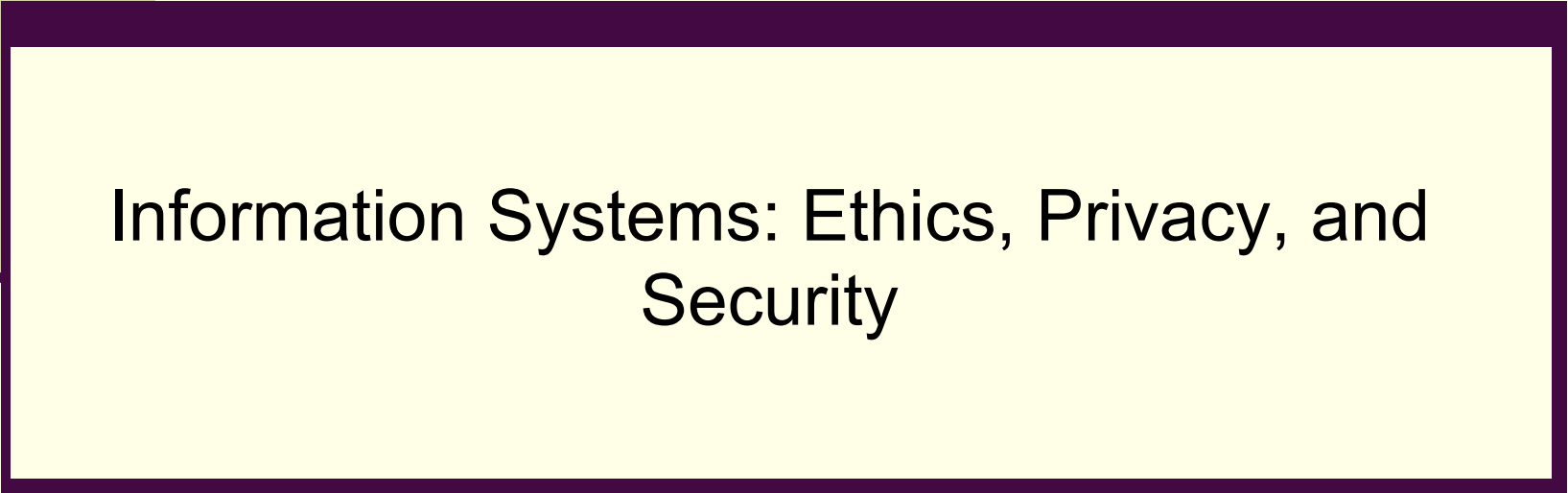




CHAPTER 3



Information Systems: Ethics, Privacy, and
Security

CHAPTER OUTLINE

3.1 Ethical Issues

3.2 Threats to Information Security

3.3 Protecting Information Resources

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.

TJX: The Worst Data Breach Ever?



Ethical Issues

- Ethics
- Code of Ethics

Fundamental Tenets of Ethics

- Responsibility
- Accountability
- Liability

Unethical vs. Illegal

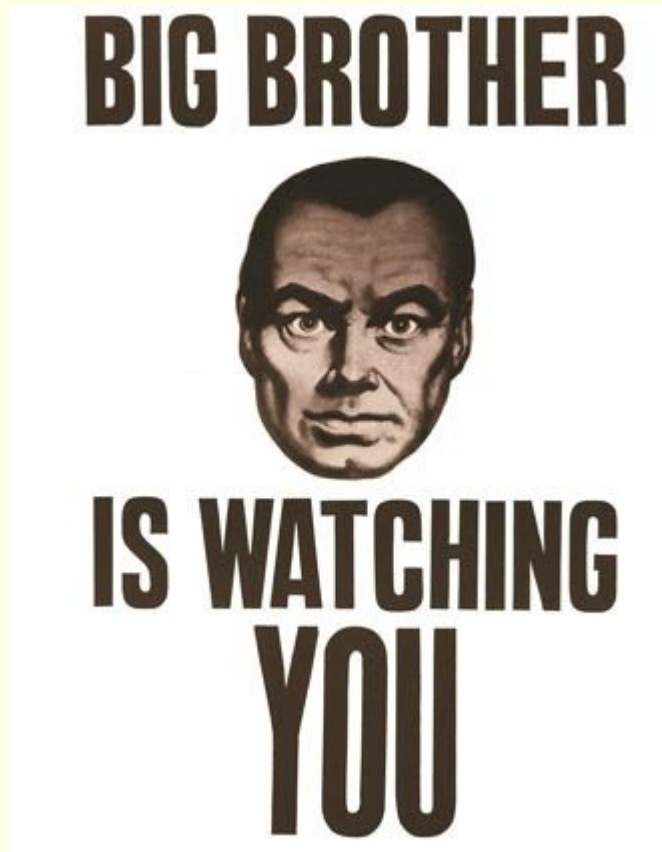
What is unethical is not necessarily illegal.

Ethics scenarios

The Four Categories of Ethical Issues

- Privacy Issues
- Accuracy Issues
- Property Issues
- Accessibility Issues

Privacy Issues



How much privacy
do we have left?

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, digital dossiers, and profiling
- Electronic Surveillance
- Personal Information in Databases
- Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites

Data Aggregators, Digital Dossiers, and Profiling



Electronic Surveillance



Electronic Surveillance

- See "[The State of Surveillance](#)" article in *BusinessWeek*
- See the [surveillance slideshow](#)
- See additional surveillance [slides](#)
- And you think you have privacy? ([video](#))
- [Sense-through-the-Wall](#)

Personal Information in Databases

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



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



Social Networking Sites Can Cause You Problems

Anyone can post derogatory information about you *anonymously*.

(See this Washington Post [article](#).)



You can also hurt yourself, as this [article](#) shows.

What Can You Do?

First, be careful what information you post on social networking sites.

Second, a company, ReputationDefender, says it can remove derogatory information from the Web.



Protecting Privacy

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



3.2 Threats to Information Security



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

Factors Increasing the Threats to Information Security (continued)

- International organized crime turning to cybercrime
- Downstream liability
- Increased employee use of unmanaged devices
- Lack of management support

A Look at Unmanaged Devices



Wi-Fi at McDonalds



Hotel Business Center

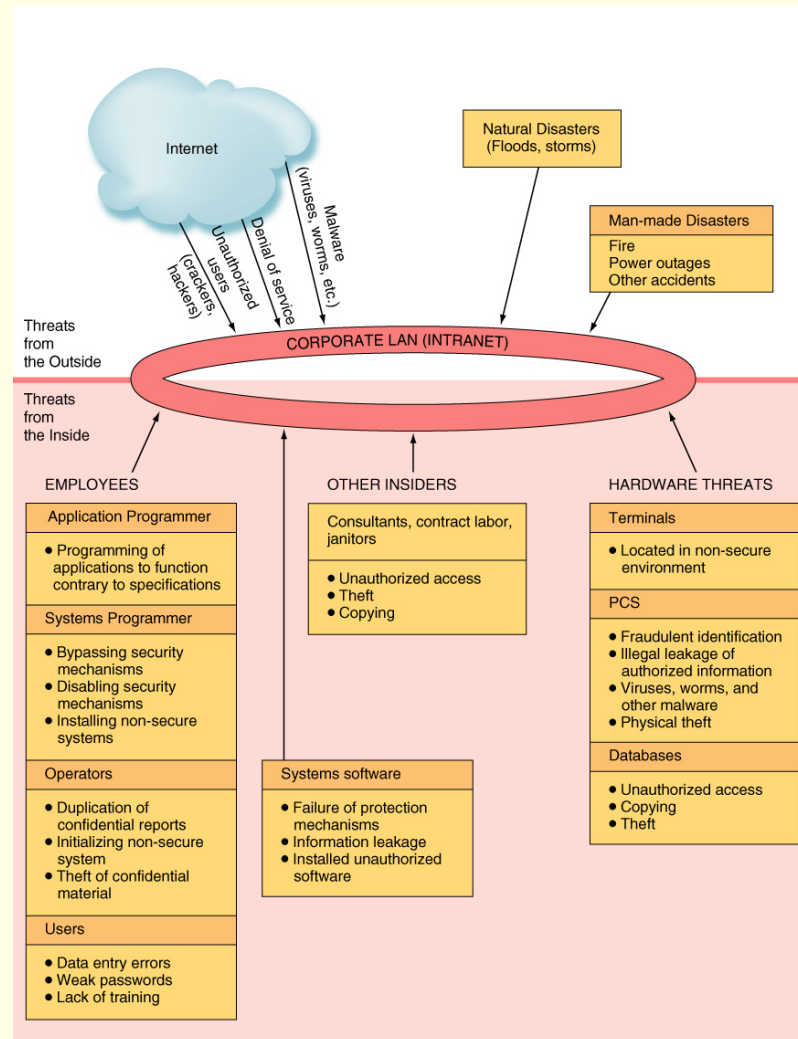


Wi-Fi at Starbucks

Key Information Security Terms

- Threat
- Exposure
- Vulnerability
- Risk
- Information system controls

Security Threats (Figure 3.1)



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)

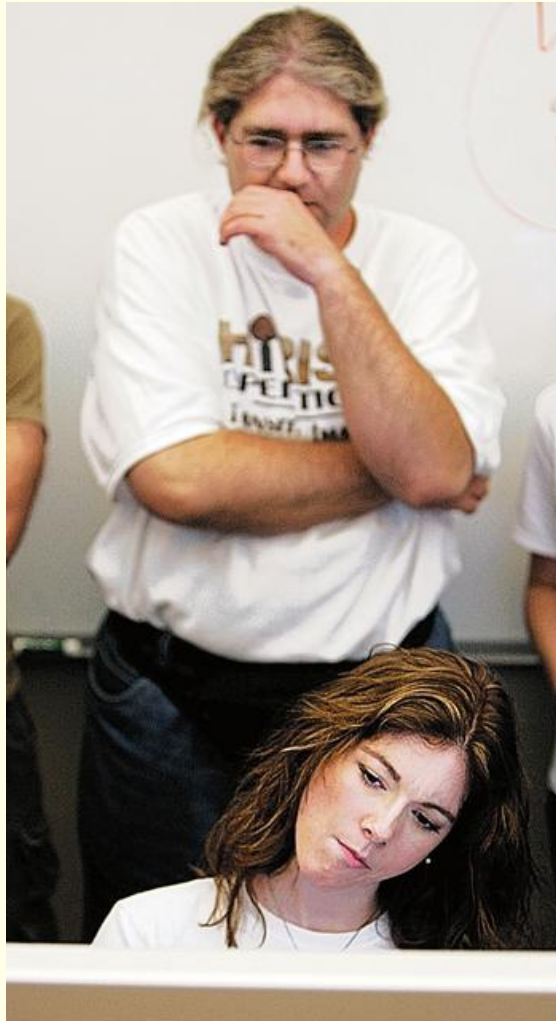
Human Errors

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

Anti-Tailgating Door



Shoulder Surfing



Most Dangerous Employees

Human resources and MIS



Remember, these employees hold ALL the information

Social Engineering

- 60 Minutes Interview with Kevin Mitnick, the “King of Social Engineering”
- Kevin Mitnick served several years in a federal prison. Upon his release, he opened his own consulting firm, advising companies on how to deter people like him,
 - See his company [here](#)

Natural Disasters



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

Deliberate Acts (continued)

- Software attacks

- Virus

- Worm

- 1988: first widespread worm, created by Robert T. Morris, Jr.

- (see the rapid spread of the Slammer worm)

- Trojan horse

- Logic Bomb

Deliberate Acts (continued)

- Software attacks (continued)
 - Phishing attacks
 - Phishing [slideshow](#)
 - Phishing [quiz](#)
 - Phishing [example](#)
 - Phishing [example](#)
 - Distributed denial-of-service attacks
 - See botnet [demonstration](#)

Deliberate Acts (continued)

- Software attacks (continued)

Can you be Phished?



How to Detect a Phish E-mail



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

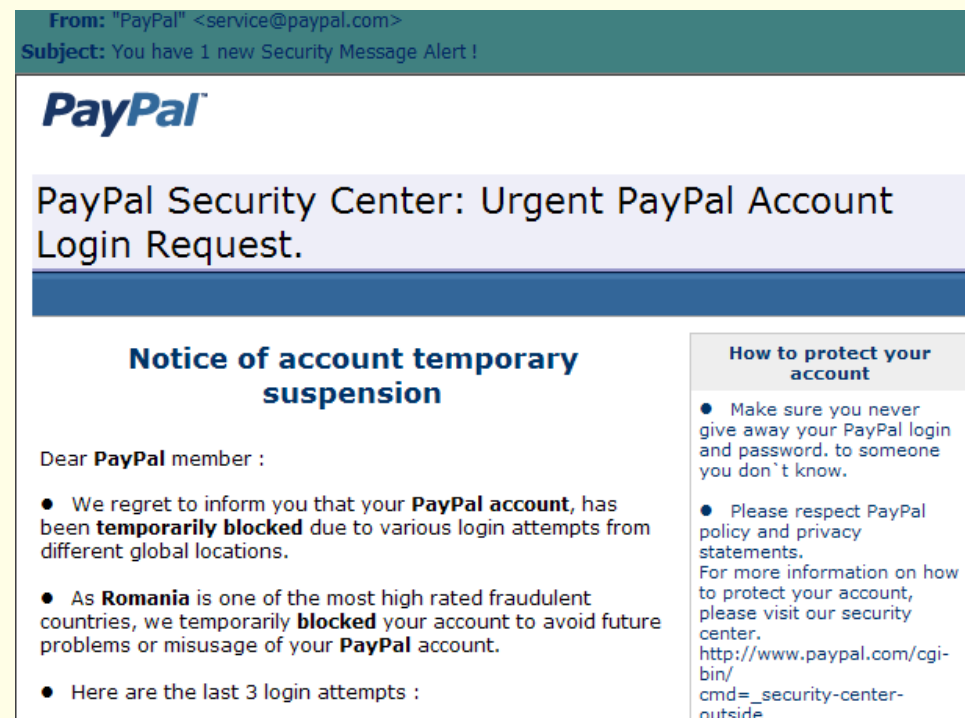
As Spammers get better, their emails look more genuine. How do you tell if it's a scam and phishing for personal information? Here's how ...

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](#)

011/
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, \$coo!place2ll
ve or 2Barry5Bonds#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%" 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="pp_sansserif" align="center"><a  
href="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="ftp://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

From: "Amazon.Inc" <webmaster@security.com> 10/3
BC: Houston Carr
Subject: { SPAM 2 }:New ALERT message:

You have 1 new ALERT message
Please login to your **Amazon**
and Confirm Billing And your Information.

To Login, please click the link below:

[Go To www.amazon.com/login.asp](http://www.amazon.com/login.asp)

Copyright ? 2007 Amazon.Inc Customer

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)

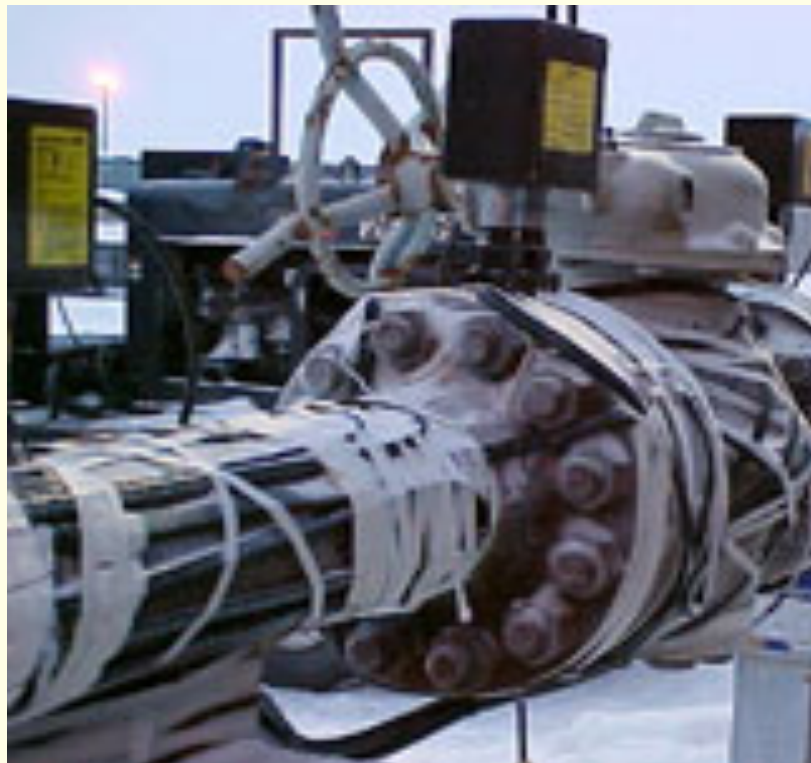
- Alien Software
 - Spyware (see [video](#))
 - Spamware
 - Cookies
 - Cookie [demo](#)



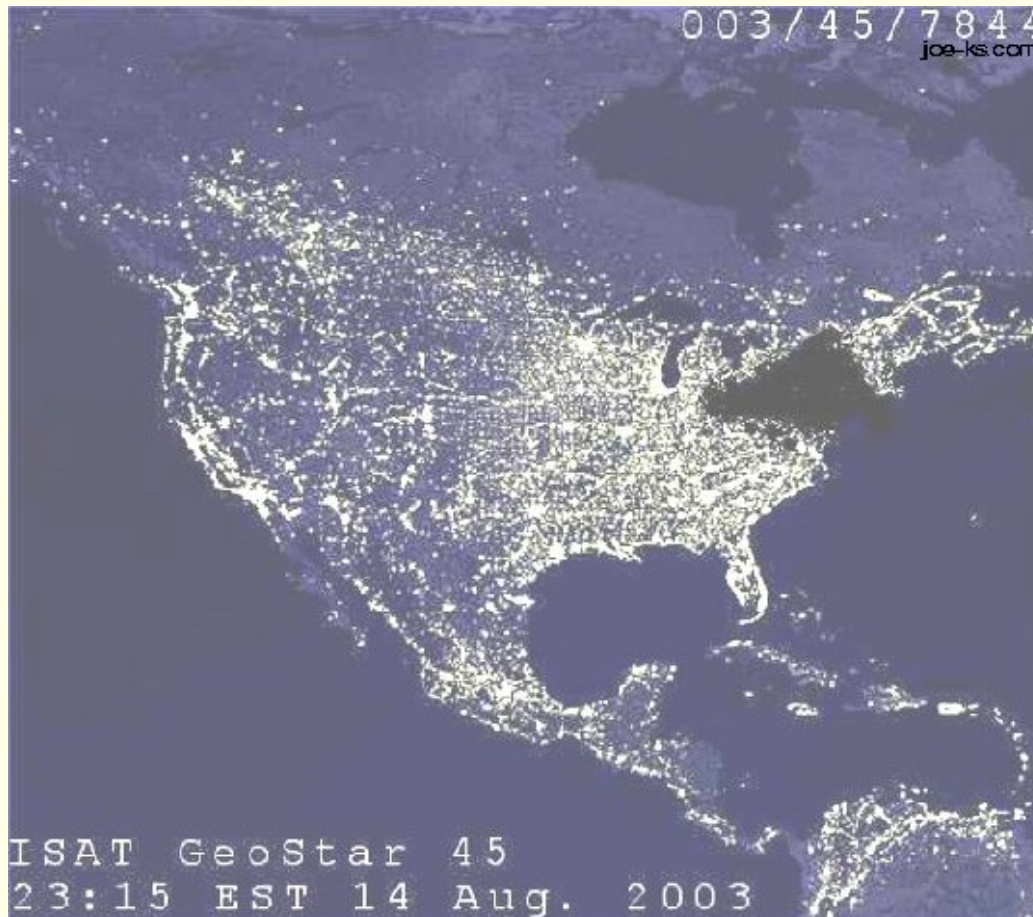
Deliberate Acts (continued)

- Supervisory control and data acquisition (SCADA) attacks

Wireless
sensor



What if a SCADA attack were successful?



Northeastern
U.S. power
outage in 2003

Results of the power outage in NYC



More results of power outage in NYC



A Successful (Experimental) SCADA Attack

Video of an experimental SCADA attack
that was successful



3.3 Protecting Information Resources



Risk!



There is
always
risk!

And then there is real risk!



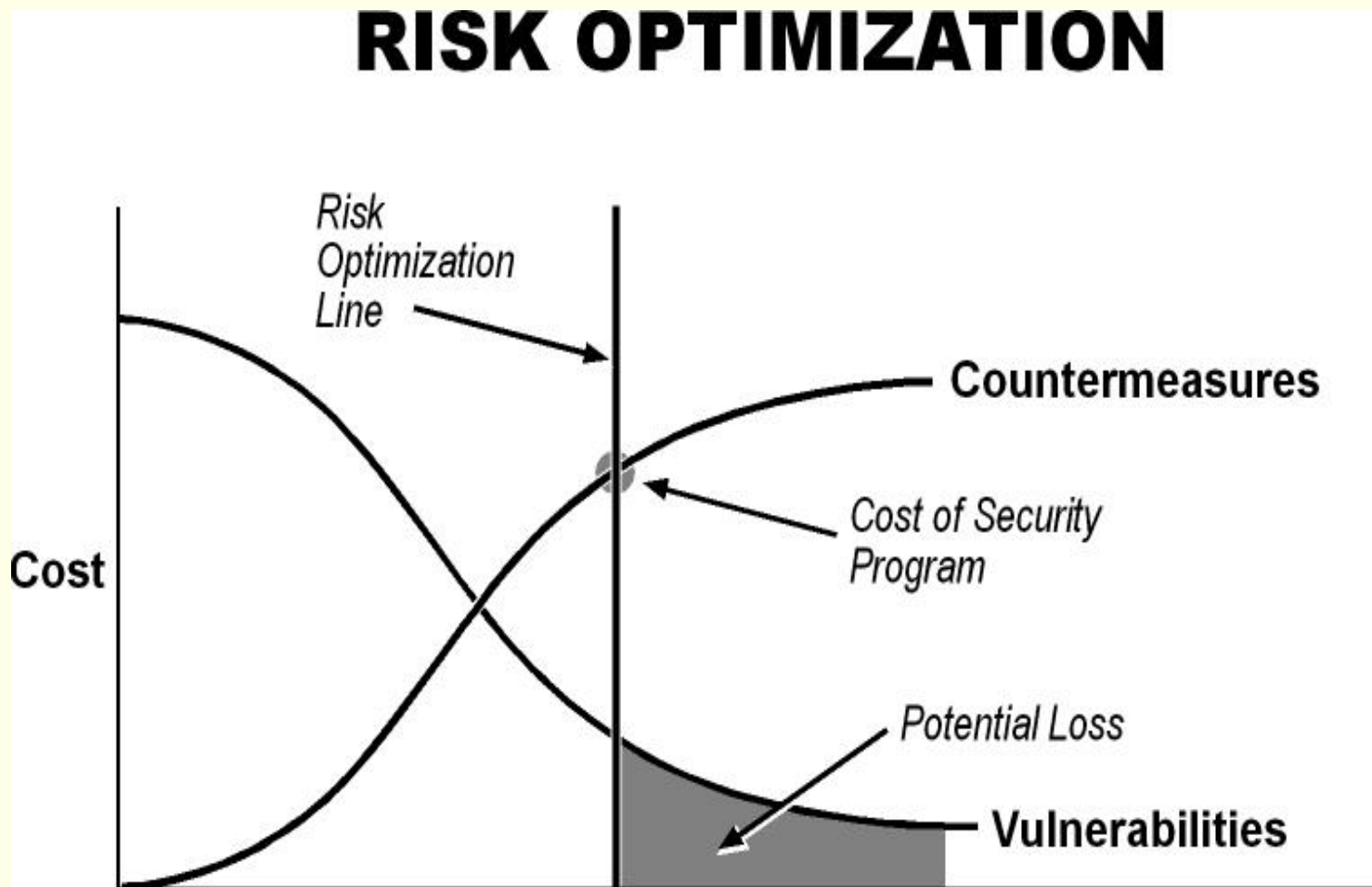
Risk Management

- Risk
- Risk management
- Risk analysis
- Risk mitigation

Risk Mitigation Strategies

- Risk Acceptance
- Risk limitation
- Risk transference

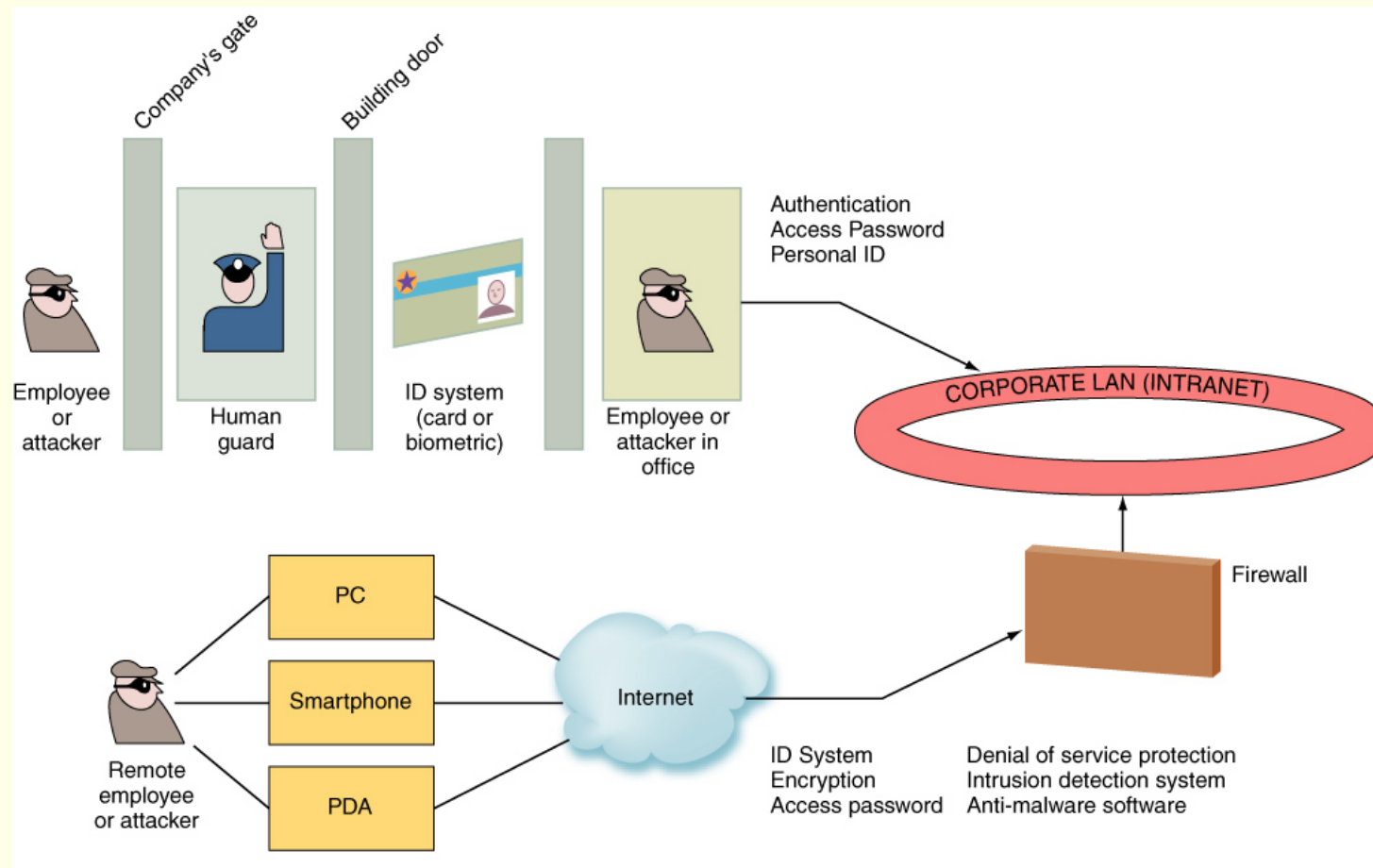
Risk Optimization



Controls

- Physical controls
- Access controls
- Communications (network) controls
- 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
 - passwords
 - passphrases

Access Controls (continued)

- Authorization
 - Privilege
 - Least privilege

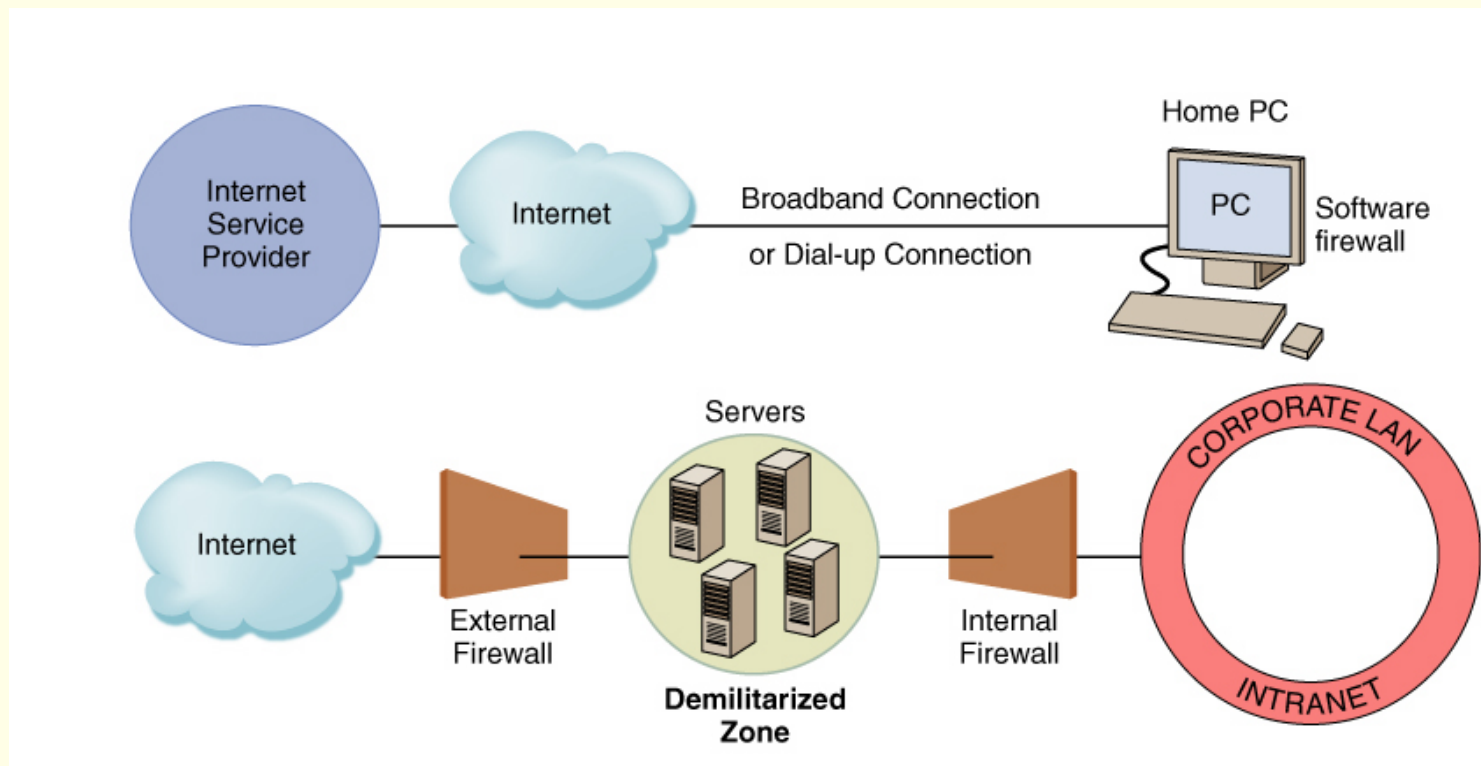
Communication or Network Controls

- Firewalls
- Anti-malware systems

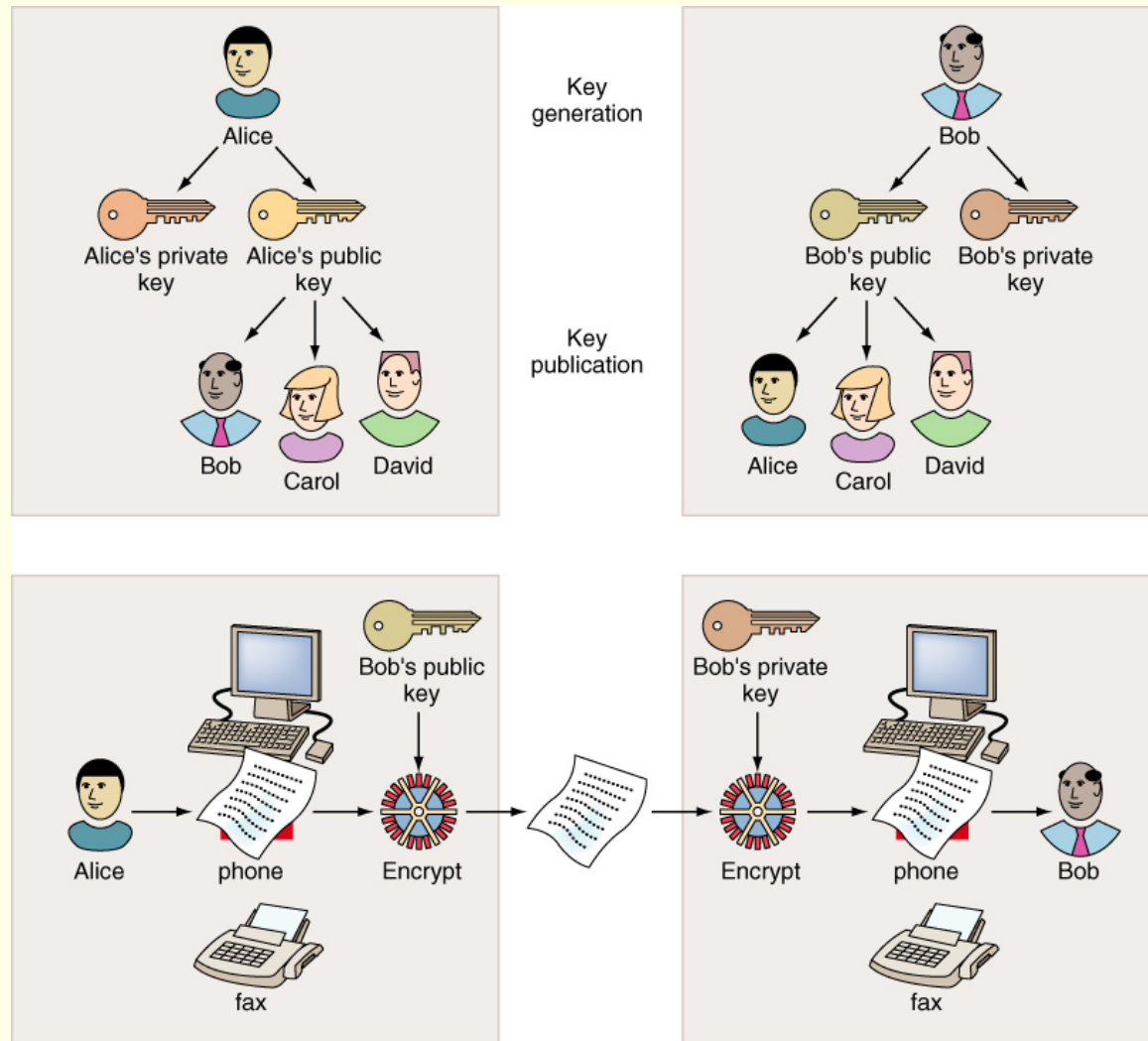


- Whitelisting and Blacklisting
- Intrusion detection systems
- Encryption

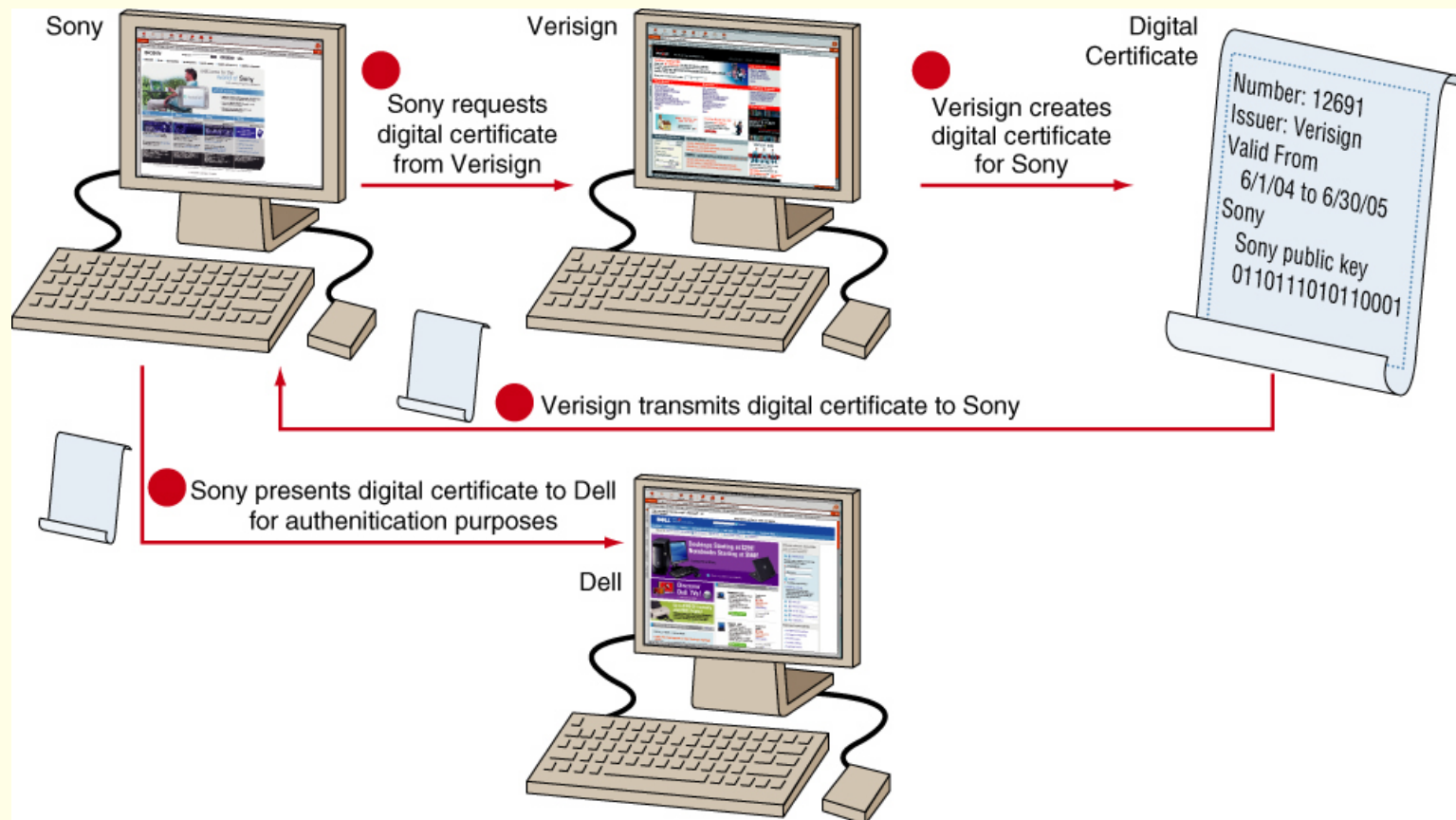
Basic Home Firewall (top) and Corporate Firewall (bottom)



How Public Key Encryption Works



How Digital Certificates Work



Communication or Network Controls

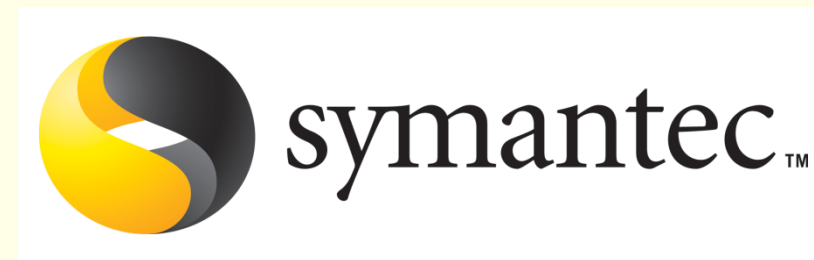
(continued)

- Virtual private networking
- Secure Socket Layer (now transport layer security)
- Vulnerability management systems
- Employee monitoring systems

Virtual Private Network and Tunneling



Popular Vulnerability Management Systems



Popular Employee Monitoring Systems



Employee Monitoring System



Business Continuity Planning, Backup, and Recovery

- Hot Site
- Warm Site
- Cold Site

Information Systems Auditing

- Types of Auditors and Audits
 - **Internal**
 - **External**

IS Auditing Procedure

- Auditing around the computer
- Auditing through the computer
- Auditing with the computer

Chapter Closing Case

