IWOSI: The Information Warfare, Cyber Warfare and Open Sources Intelligence

Yasar University Izmir, Turkey 2012

business. technology. society.

Kenneth C. Laudon

Carol Guercio Traver

Rosalina Babo

INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO

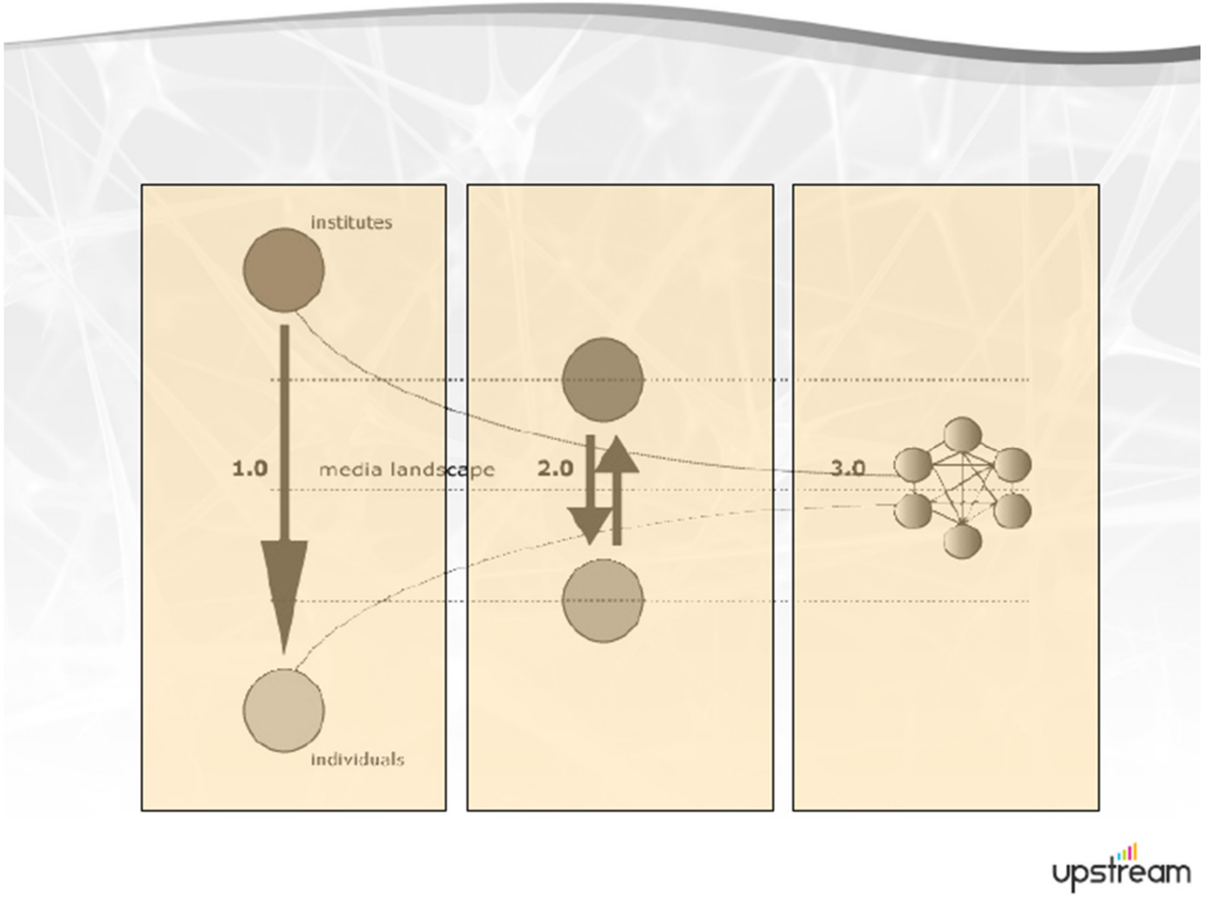
Learning Objectives

- Explain the scope of crime and security problems.
- Describe the key dimensions of security.
- Explain the tension between security and other values.
- Identify the key security threats.
- Describe how technology helps protect the security of messages sent over the Internet.

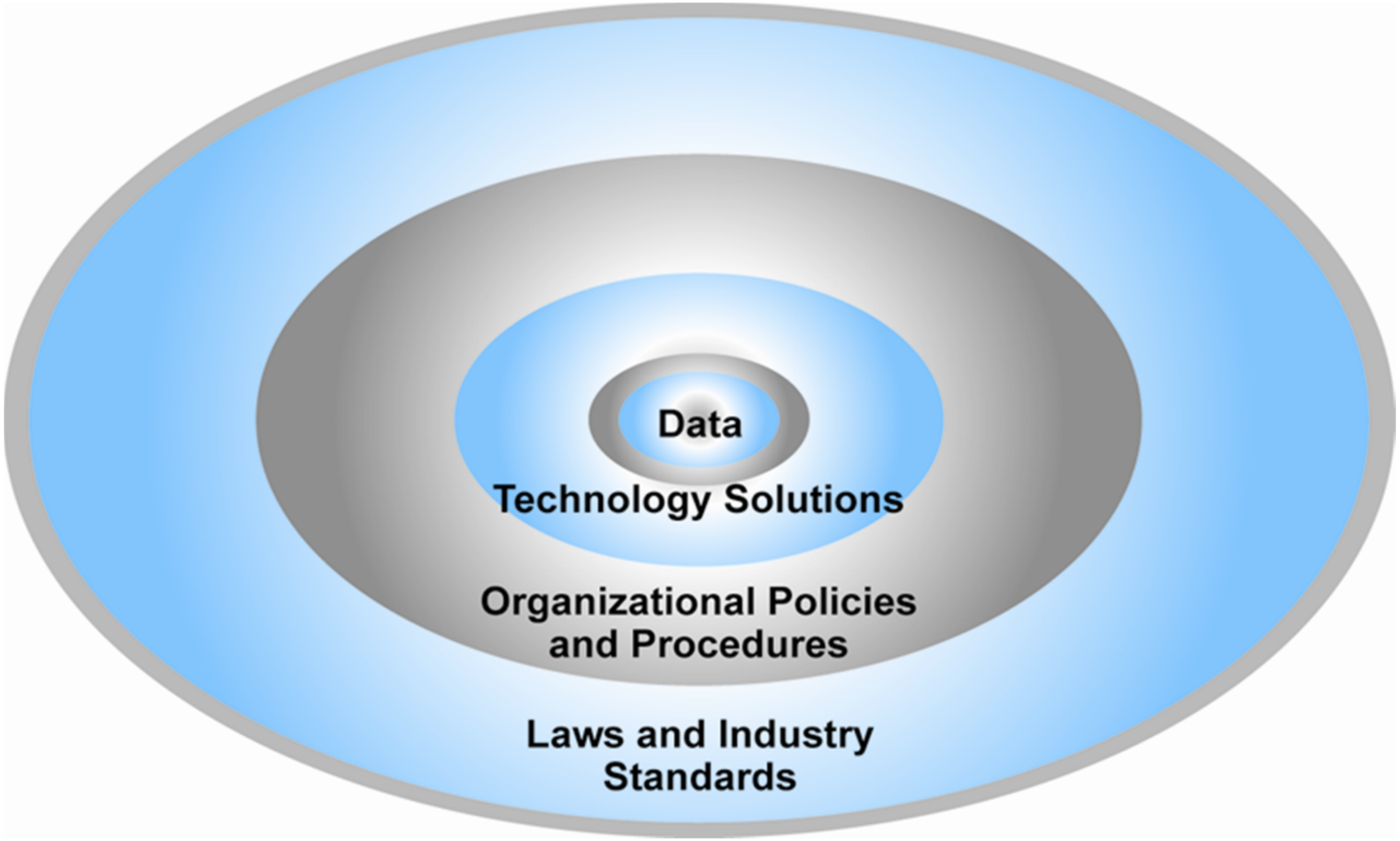
http://www.azimuth-interactive.com/ecommerce8e/ch05.html

http://www.iscap.ipp.pt/~wwwpaol2/moodleformar//

Online Connection



The Security Environment



Data

Technology Solutions

Organizational Policies and Procedures

Laws and Industry Standards

Figure 4.2, Page 249

Cyberwar: Mutually Assured Destruction (MAD)

Class Discussion

- What is the difference between hacking and cyberwar?
- Why has cyberwar become more potentially devastating in the past decade?
- What percentage of computers have been compromised by stealth malware programs?
- Will a political solution to MAD 2.0 be effective enough?

The Security Environment

- Overall size and losses of cybercrime unclear
  - Reporting issues
- 2011 CSI survey: 46% of respondent firms detected breach in last year
- Underground economy marketplace:
  - Stolen information stored on underground economy servers

The scope of the problem

- Crime complaint center (2009)
- 336 000 Internet crime complains (+22% 2008)
  - 146 000 To Federal, state and local law enforcement agencies (+100% 2008)
- $559 Million loss (+100% 2008)

Types of Attacks Against Computer Systems (Cybercrime)

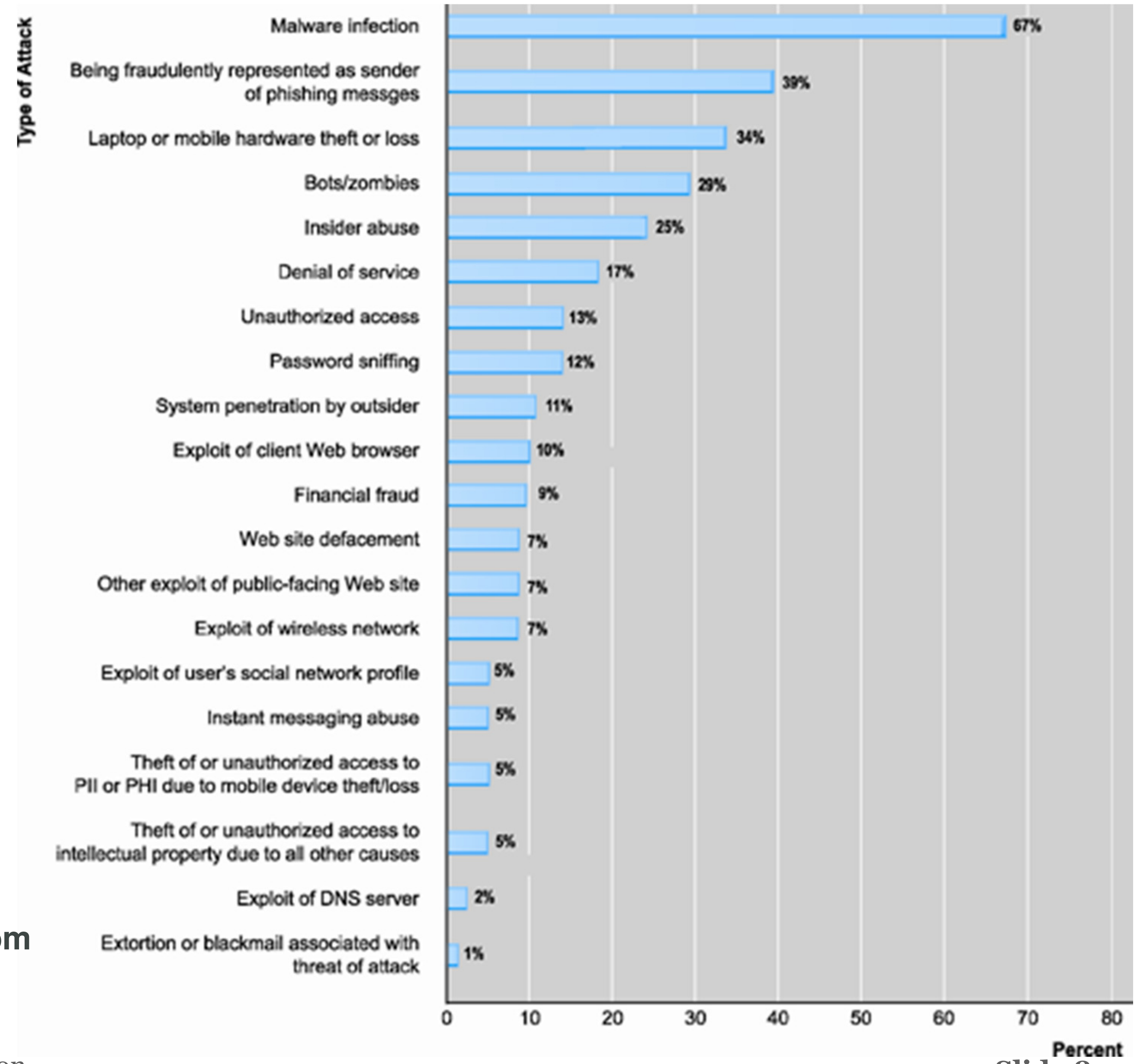


Figure 4.1, Page 246

SOURCE: Based on data from Computer Security Institute, 2011

Insight on Society: Class Discussion

- How your daily life might be affected as a result?
- Discuss whether you yourselves or anyone you know has ever been a victim of a computer crime.
- Do you think computer crime is being overplayed or underplayed in the popular press, given the statistics available and discussed in this section?

The Security Environment

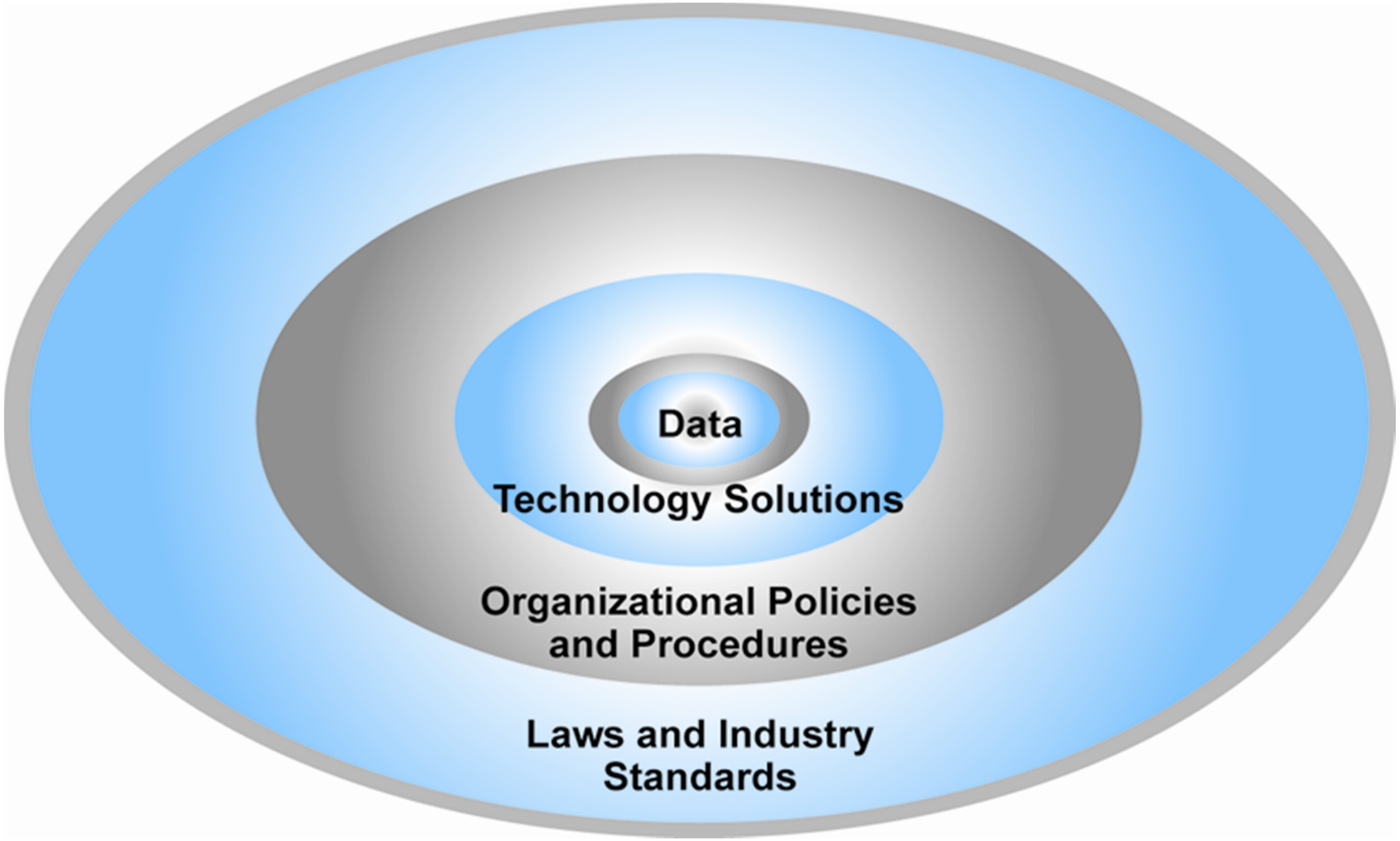

Data
Technology Solutions
Organizational Policies and Procedures
Laws and Industry Standards

Figure 4.2, Page 249

What Is Good Security?

- **To achieve highest degree of security**
  - New technologies
  - Organizational policies and procedures
  - Industry standards and government laws
- **Other factors**
  - Time value of money
  - Cost of security vs. potential loss
  - Security often breaks at weakest link

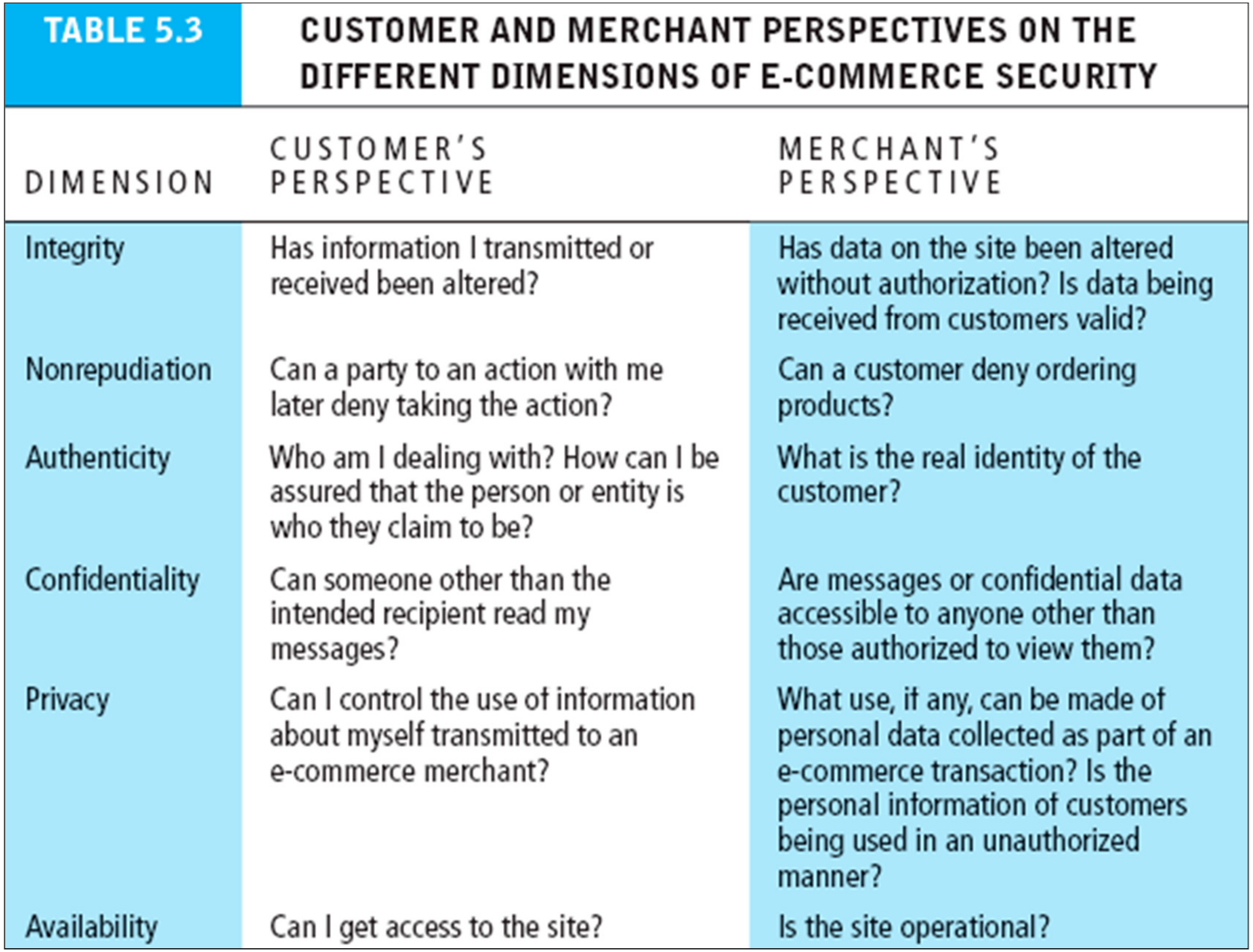


TABLE 5.3 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

Table 4.3, Page 250

The Tension Between Security and Other Values

- **Ease of use:**
  - The more security measures added, the more difficult a site is to use, and the slower it becomes
- **Public safety and criminal uses of the Internet**
  - Use of technology by criminals to plan crimes or threaten nation-state

Security Threats in the Environment

- **Three key points of vulnerability:**
  1. Client
  2. Server
  3. Communications pipeline (Internet communications channels)

A Typical E-commerce Transaction

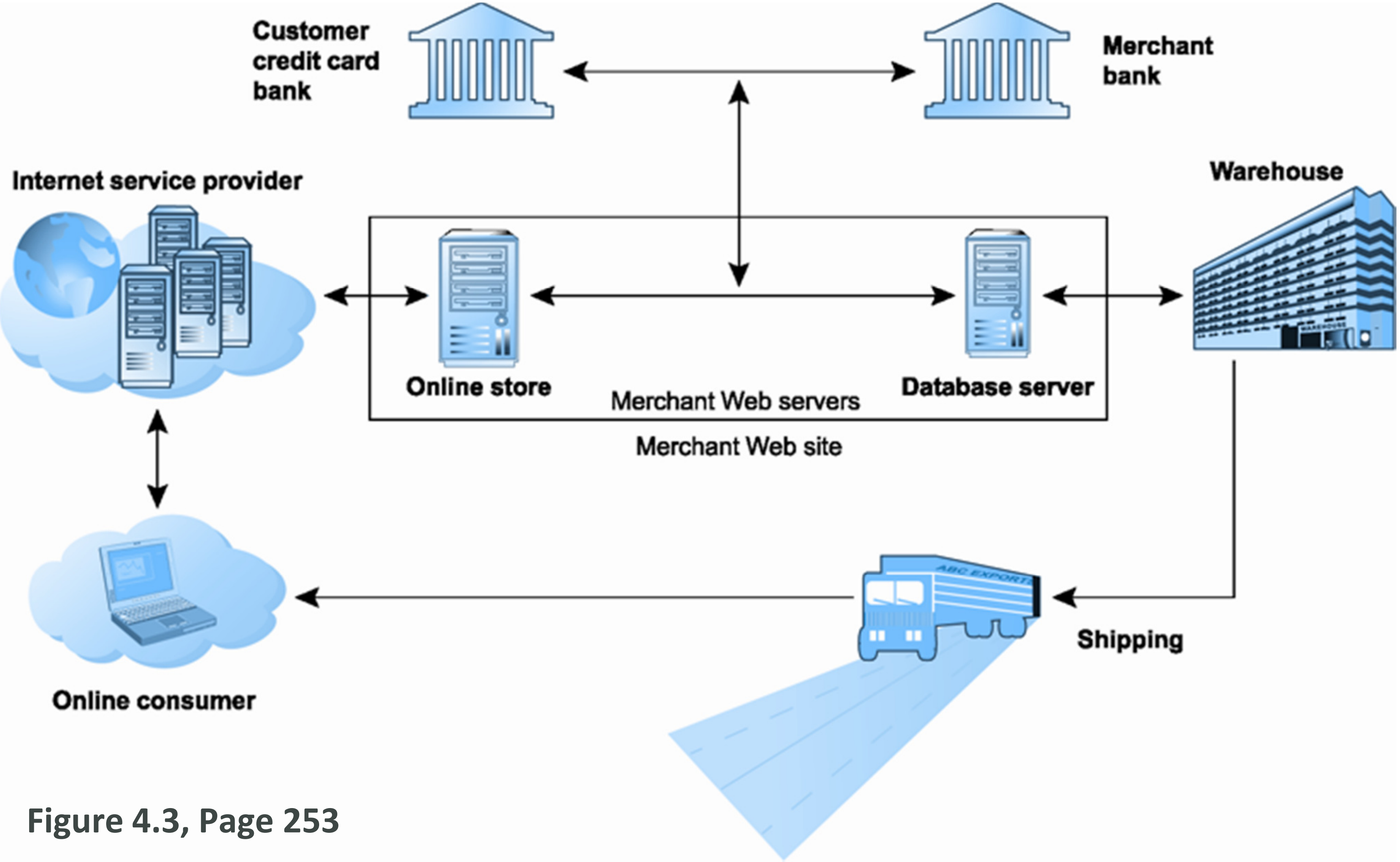
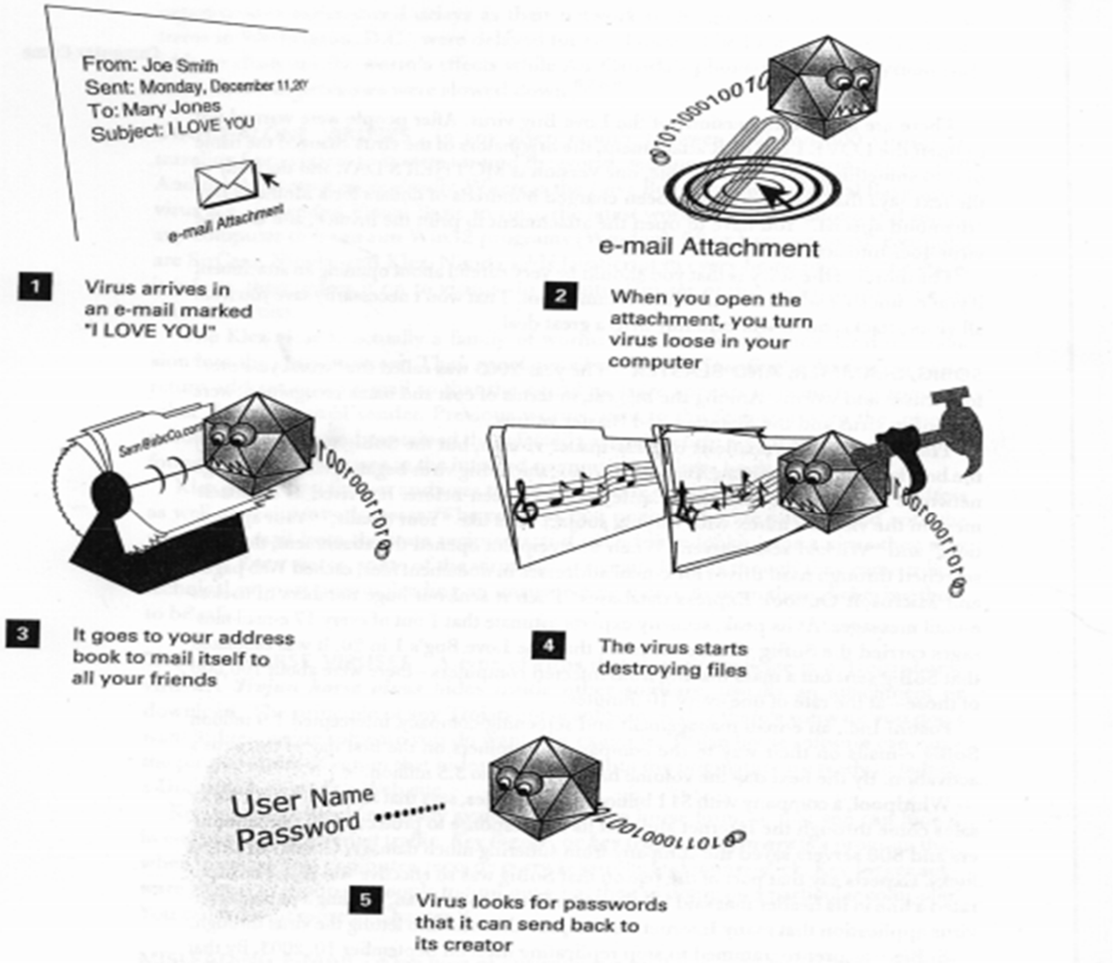


Figure 4.3, Page 253

Security Threats



From: Joe Smith
Sent: Monday, December 11,20
To: Mary Jones
Subject: I LOVE YOU

1 Virus arrives in an e-mail marked "I LOVE YOU"

2 When you open the attachment, you turn virus loose in your computer

3 It goes to your address book to mail itself to all your friends

4 The virus starts destroying files

5 Virus looks for passwords that it can send back to its creator

igure H.3
he Love Bug Worm

Most Common Security Threats

- **Malicious code**
  - Viruses
  - Worms
  - Trojan horses
  - Bots, botnets
- **Unwanted programs**
  - Browser parasites
  - Adware
  - Spyware

Most Common Security Threats (cont.)

- Social engineering
- Phishing
  - Deceptive online attempt to obtain confidential information
    - E-mail scams
    - Spoofing legitimate Web sites
    - Use of information to commit fraudulent acts (access checking accounts), steal identity

Most Common Security Threats (cont.)

- **Hacking**
  - Hackers vs. crackers
  - Types of hackers: White, black, grey hats
- **Cybervandalism:**
  - Intentionally disrupting, defacing, destroying Web site
- **Data breach**
  - When organizations lose control over corporate information to outsiders

Most Common Security Threats (cont.)

- Credit card fraud/theft
  - Hackers target merchant servers; use data to establish credit under false identity
- Spoofing
- Pharming
- Spam/junk Web sites
- Denial of service (DoS) attack
  - Hackers flood site with useless traffic to overwhelm network
- Distributed denial of service (DDoS) attack

Most Common Security Threats (cont.)

- **Sniffing**
  - Eavesdropping program that monitors information traveling over a network
- **Insider jobs**
- **Poorly designed server and client software**
- **Social network security**
- **Mobile platform threats**
  - Same risks as any Internet device
  - Malware, botnets, vishing/smishing

Projects and Exercises

Project 1: Is This Safe?

Visit Amazon, MSNBC, and Monster and find and read the pages on each site that discuss security. Then, prepare a 2–3 page report in which you discuss the security features and policies of these Web sites. How do they attempt to keep your personal information from being stolen? What aspects of the policies do or do not give you confidence as a consumer? What makes you wary of giving personal information such as a credit card number to an online store or service?

Projects and Exercises

Project 2: Dangerous Software

The section on poorly designed server and client software in the text on page 286 highlights the impact that such software has on security. The National Vulnerability Database compiles comprehensive data on software vulnerabilities it identifies. Use the Vulnerability Search Engine to search for software flaws from five vendors (such as Microsoft, Apple, Google, or another firm) during the last three months, Using this data, create a column chart using Excel or another program to illustrate the trends in software vulnerabilities identified during that time. What conclusions can you draw from this data?

Projects and Exercises

Project 3: Using Credit Cards Online

Ellen Longbow is the chief financial officer (CFO) at a startup e-commerce firm that sells products popular with college students. She has asked you to do some Internet research on three competing companies that permit credit-card purchases at their e-commerce sites. Create a table (or spreadsheet) that summarizes how each site handles the following issues: (a) What information does each site require before permitting you to use a credit card? (b) What steps must you go through to complete a transaction? (c) What features do they incorporate to facilitate overcoming the limits of security, merchant risk, cost, etc.? (d) How do they authenticate cardholder identities?

Videos

- **US claims cyber war is the new terrorism**

http://www.youtube.com/watch?v=mX9Oi4UnfAM

The mainstream media has been asking the question, is the US ready for a cyber war? Obama has emphasized the importance of being prepared for the new WMD's, weapons of mass disruption. According to Obama, terrorism can be acted with a few strokes of a keyboard. The Federal Bureau of Investigation has said that cyber threat will surpass terroristic threats. So could the next Pearl Harbor come in the form of a cyber attack? Conn Hallinan, columnist for Foreign Policy in Focus, helps us answer these looming questions.

- **Chinese Army Cyber Warfare Hack Attack**

http://www.youtube.com/watch?v=AFTB4NbN7AA&feature=player_embedded#!

The Chinese army and their cyber warfare department attacking websites in the United States. (Min. 4”36)

'Anonymous Hackers' Targets Pentagon Contractor (Video)

http://article.wn.com/view/WNATC7017378FBB308DFABEBF7FDEA407A12/

Prior to the ruling of British courts regarding the extradition of Julian Assange, founder of Wikileaks site, to Sweden, a group of hackers, known as Anonymous Hackers, attacked an American Military IT company.

The group threatened to seek American and British targets, in retatliation to the accusations of Mr. Assange and News International for spying on British residents.

The latest target of Anonymous is "Booz Allen Hamilton", the largest military contractor that deals with the Pentagon.

In an online statement, the group declared that it was able to hack the systems of the contracting company and steal ninety thousand e-mail addresses and passwords belonging to military staff from various ranks.

Moreover, leaders of this group threatened to target computer systems of the London police and British judicial, and warned that this day will be the biggest day in their history.

According to analysts, Anonymous is using its attacks as means to express its anger after the News International Company's phone hacking scandal, which forced the News of The World newspaper to shut down.

Furthermore, the group wants to show its stance regarding the extradition of Julian Assange, founder of Wikileaks, to authorities.

The group has already attacked the sites of Amazon, Bank of America, PayPal, Visa and Mastercard, for their refusal to transfer contributions to the Wikileaks account in compliance with U.S. government orders.

Cyber War - The Aurora Project (Video)

http://www.youtube.com/watch?v=rTkXgqK1l9A&feature=related

This Cyber War episode was on 60 minutes and belongs to CBS.

The Aurora Project proved that network control to a generator is very dangerous. This shows how drastically a 27-Ton Jenbacher 1 megawatt type power generator can be destroyed by simply hacking into it from a common laptop. Imagine getting access to all of the generators in the U.S. and then simply pushing the enter key on your keyboard by one man. After a little control by use of the internet and some skilled hacking by an evil programmer or an Al-Qaeda professional, this could be accomplished. With one malignant hacker on the power grid, a lot of our economy will die. What will we do without electricity for 4 months or maybe up to a year? Our electronic and software engineers that create these interfaces that control these generators need to care about these liabilities, and not just profits. Even if they did, its still too expensive. Microsoft makes billions and even they cant stop hackers. The Internet is for information, and should never be used for generator control.

Repository

In this course several presentation and a glossary were produced.

All the material produced by the students teams are available here:

http://www.iscap.ipp.pt/~wwwpaol2/moodleformar//

Key Terms

- public key cryptography
- hash function
- digital signature (e-signature)
- digital certificate
- certification authority (CA)
- public key infrastructure (PKI)
- Pretty Good Privacy (PGP)
- secure negotiated session
- session key
- virtual private network (VPN)
- firewall
- proxy server (proxy)
- risk assessment
- security policy
- implementation plan
- security organization
- access controls
- authentication procedures
- biometrics
- authorization policies
- authorization management system
- security audit
- CERT Coordination Center, p.312
- cash
- float
- checking transfer
- credit card
- credit card association
- issuing bank

Key Terms

- processing center (clearinghouse)
- stored-value payment system
- debit card
- merchant account
- digital wallet
- digital cash
- online stored value payment system
- smart card
- radio frequency identification (RFID)
- near field communications (NFC)
- digital accumulating balance payment system
- digital checking payment system
- electronic billing presentment and payment (EBPP) system