Chapter 11
Managing Information Security

• Data Theft – Occurs when information is illegally copied or taken from a business or individual.
• Data theft is the top security concern across all organizations.
• Insiders account for between 20 to 80 percent of security problems.

Chapter 11
Managing Information Security

• Scope of Security
  – Personnel – who has access to what
  – Application – Mission critical software access is controlled
  – Operating Systems – Security policy is tied to OS
    • Memory Mgt. – Access to I/O devices – File mgt. – Hardware Configuration
  – Network – Wire / routers – switches / servers
  – Middleware and Web services – Complex systems often allowing outside access
  – Facility – physical security
  – Egress – removing sensitive data on a laptop or on paper

Chapter 11
Managing Information Security

• Security Breaches (p. 402-403)
  – Password cracking – guessing, brute force, shoulder surfing
  – Social Engineering – misleading someone into giving up their password
  – Network Sniffing – monitoring network traffic to search for clear text information (encryption is the best defense).
  – Trojan horse – malicious software hidden inside a potentially useful utility
  – Denial of Service – flooding a Website or server with traffic so that it is unresponsive to legitimate requests.

Chapter 11
Managing Information Security

• 5 Security Pillars
  – Authentication – Verifying that a user is who they say they are.
  – Identification – Identifying a certain user as having proper rights, access, and roles on the system/network.
  – Privacy – Protecting information from unauthorized access
  – Integrity – Keeping information in its original (or correct) form
  – Nonrepudiation – Preventing parties from denying actions that they have taken

Chapter 11
Managing Information Security

• UT Austin Case
  – Summary
  – Successes
  – Challenges
  – Questions