E-Business Technologies

Craig Van Slyke and France Bélanger
John Wiley & Sons, Inc.

Slides by Fred Niederman

Privacy and Security in E-Business

Chapter 10

Key Ideas

- Privacy is the confidentiality of data collected about individuals using the services of government, businesses, and non-profit organizations.
- A security threat is "a circumstance, condition or event with the potential to cause economic hardship to data or network resources in the form of destruction, dislocation, modification of data, denial of service, and/or fraud, waste, and abuse." (Kalakota and Whinston 1996)

Secure E-Commerce requires

- Confidentiality or anonymity
- Data Integrity
  - Encryption, digital signatures & certificates
  - Secure network protocols
- Mutual authentication
- Authorization
- non-repudiation

Some useful technologies

- SET
- PKI
- SSL
- OS Security
  - RBAC, ACL, buffer overflow prevention, ...
- Firewalls (Maginot Lines)

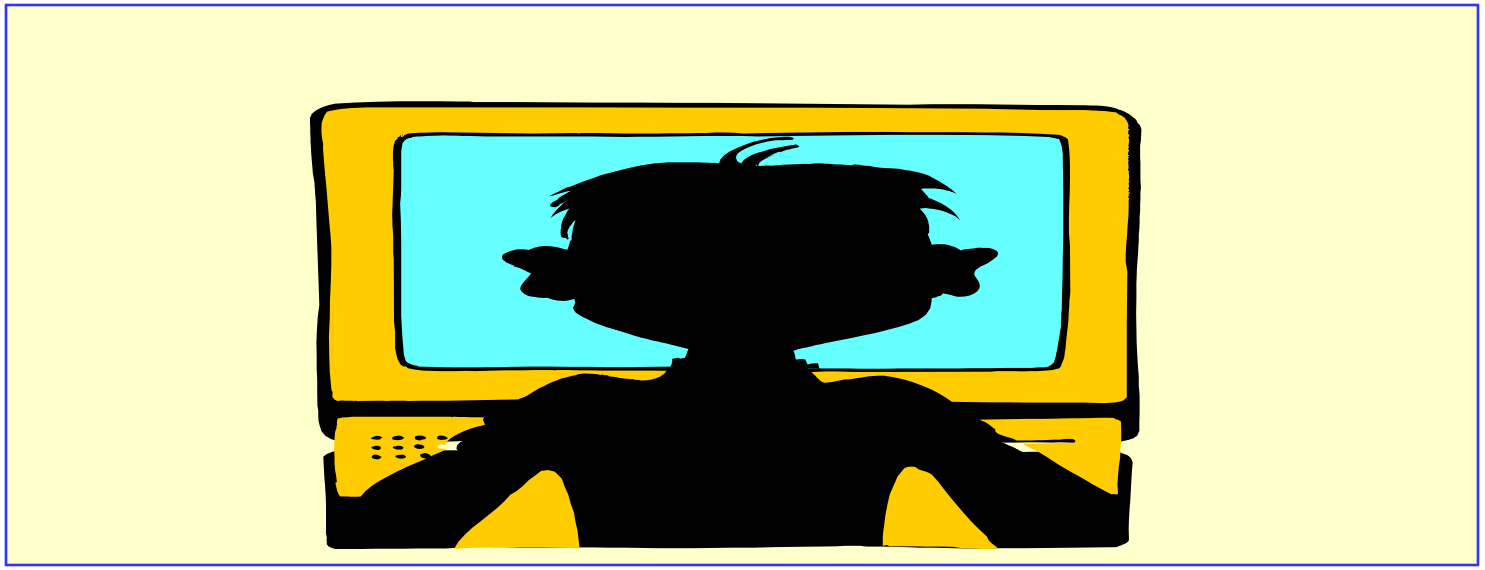
Privacy Threats

Major Privacy Threats -- 1

- Data collection
  - Faster and easier data collection
  - Cross-referencing (aggregation)
  - Hidden data collection
- Usage tracking
  - Patterns of activity lead to inferences about the user
- Is this legal?

Major Privacy Threats -- 2

- Information sharing
  - Opt-in versus opt-out affiliations with partners
- Various surveys show public concern for privacy



Ways to Add Customer Value

- Customer reviews
- Sense of community
- Customer preferences database
- Info about products and services
- Features to attract customers and influence decisions
- Consider Amazon...

Technologies and Solutions for Privacy

Cookies

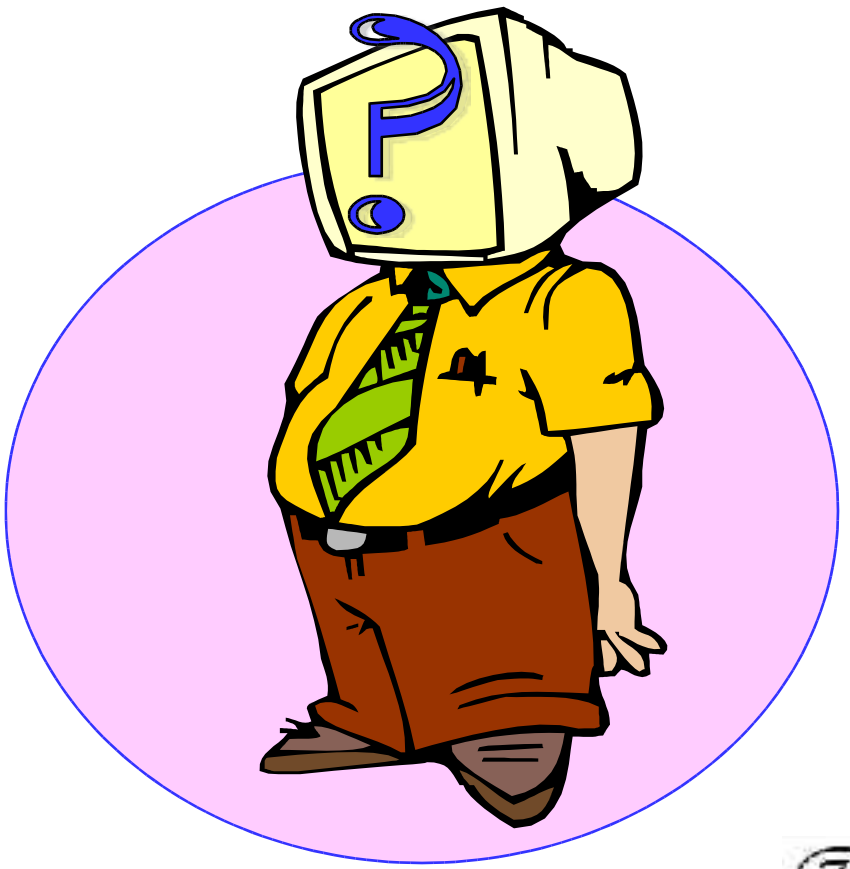
- Text file on user's hard disk
  - Information sent by HTTP protocol
  - When browser contacts URL, cookie information sent from hard disk
  - Contains…
    - Main user ID
    - Anything URL server chooses to put in!
      - Identifying information and demographic information
  - Cookie management tools

Concern for User Privacy

- Privacy statement or policy
- Trust seals
  - BBBOnLine, subsidiary of Better Business Bureau
  - AICPA WebTrust, examination by CPA
  - TRUSTe, administered by non-profit group

Government Regulation

- Users
  - Awareness
  - Empowerment
  - Redress
- Providers
  - Impact assessment
  - Only reasonably necessary
  - Notice
  - Security
  - Limited use
  - Education



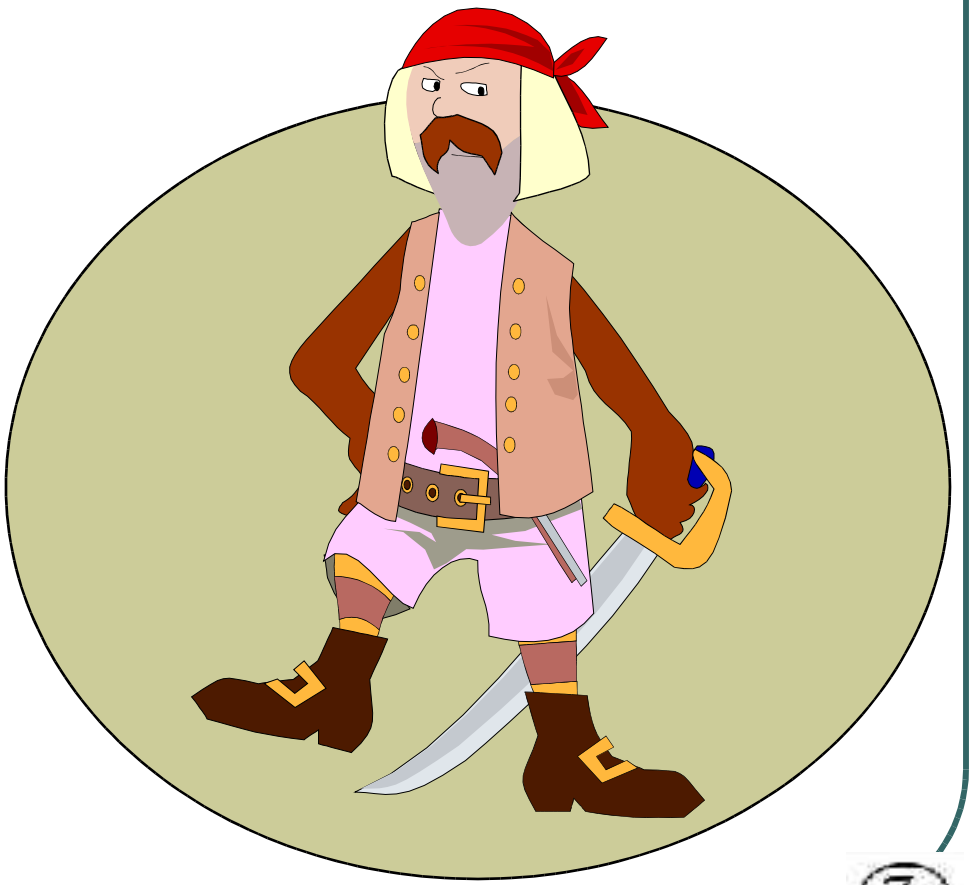
Your Turn

- Recall the 2 websites that you return to most frequently
  - What information about you would you find acceptable for them to collect about you?
- Suppose that the owners of these websites were acquired by a company against which you have a pending lawsuit?
  - Would your view of what information you would find acceptable for them to have about you change? How so?

Security Threats

Three Categories of Security Threats

- Denial of Service
- Unauthorized access
- Theft and fraud

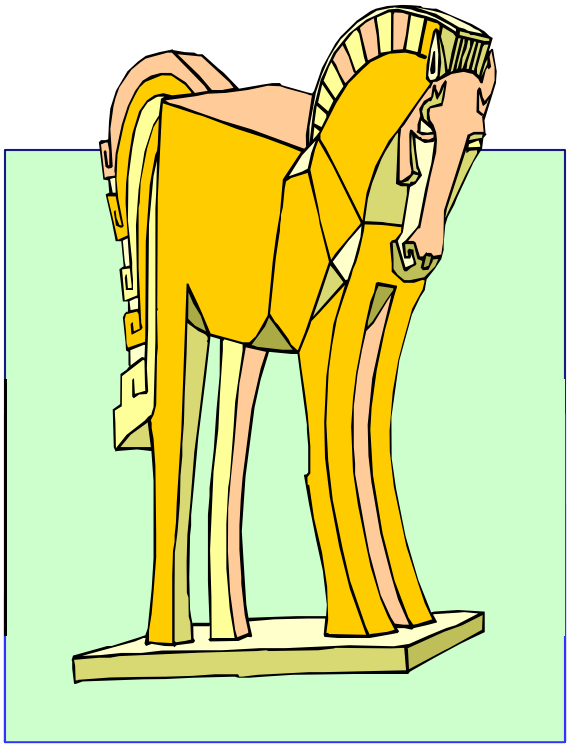


Denial of Service

- Can result from disruptions, natural disasters or malicious acts
- Spamming
  - Unsolicited commercial email
  - E-mail bombing
  - Smurfing
  - DDOS (distributed denial of service attacks)

Viruses, Worms, and Trojan Horses

- Viruses are computer programs designed to perform unwanted events
  - Worms are special viruses that spread using direct Internet connections
  - Trojan horses are disguised as legitimate software and trick users into running the program
- Common viruses
  - Parasitic virus
  - Boot sector virus
  - Stealth virus
  - Polymorphic virus
  - Macro virus
- Virus hoaxes



Unauthorized Access -- 1

- Illegal access to systems, applications or data
- Passive unauthorized access
  - May use content for damaging purposes
- Active unauthorized access
  - Modifying system or data
  - Message stream modification
    - Changes content of messages

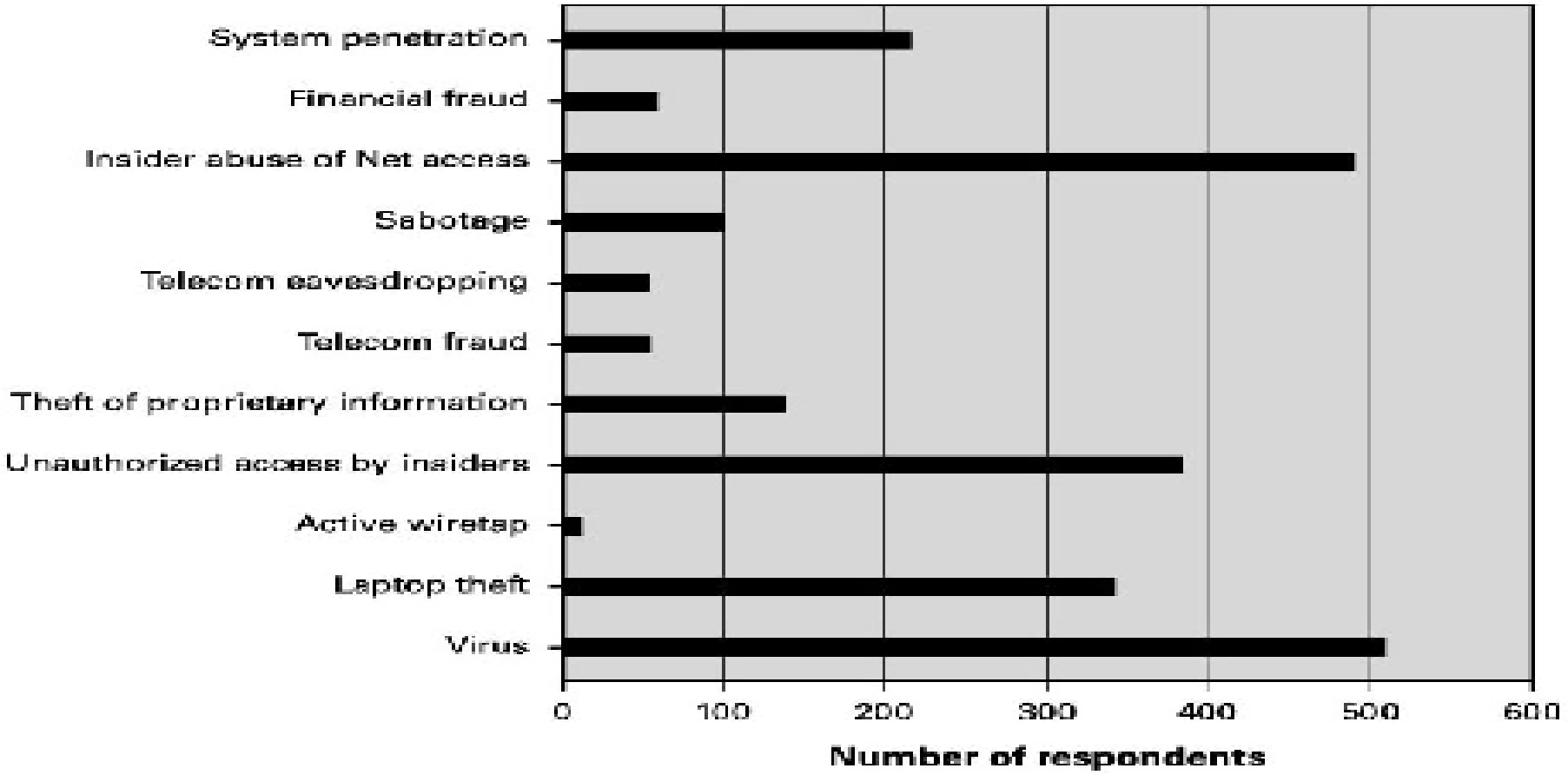
Unauthorized Access -- 2

- Masquerading or spoofing
  - Impersonating another user at the “name” or IP levels
- Sniffers
- Software and operating systems’ security holes

Theft and Fraud

- Unlicensed copies of software
- Laptops and handhelds

Threat Statistics



Security Technologies and Solutions

Disaster Recovery

- Disaster recovery planning
- Important features:
  - Fault-tolerant systems
  - Mirrored disks
  - Disk duplexing
  - Multiple lines
  - Different networks
  - Additional devices
  - Uninterrupted power supply (UPS)
- Incremental backups, “fingerprint” database

Physical Access Control

- Three basic points of access
  - Accessing from within the firm (physical access)
  - Dialing into an organization's servers (logical access)
  - Remotely accessing organization's network (logical access)
- Responses
  - Lock computers away, where possible
  - Set up policies to protect equipment
  - Selection of personnel
  - Call-back modems

Logical Access Controls

- Three levels
  - Possession – owned identification (e.g. cards)
  - Knowledge – PIN, password, background
  - Trait – fingerprint, retinal image
- User Profiles

Biometrics

- Facial recognition
- Fingerprints
- Hand recognition
- Iris/retina recognition
- Signature recognition
- Thermal imaging
- Voice recognition

Important Notes

- Policies must be enforced
- “social engineering” can defeat technical security
- Need to balance convenience against security

Firewalls

- A computer or router that controls access in and out of the internal computer network of an organization
- Work by reading control portion of messages and deciding whether to allow the messages in or out of the network
  - Stateful or stateless packet filtering
    - By source, destination, type

Types of Firewalls

- Packet-level firewall
  - Examines source and destination addresses of data packets
- Application-level firewall
  - Requires log-in to access applications (from outside)
  - Proxy server – keeps external transactions outside network itself
  - Network address translation
  - Better security, more complex to install and may slow down performance

Additional Types of Firewalls

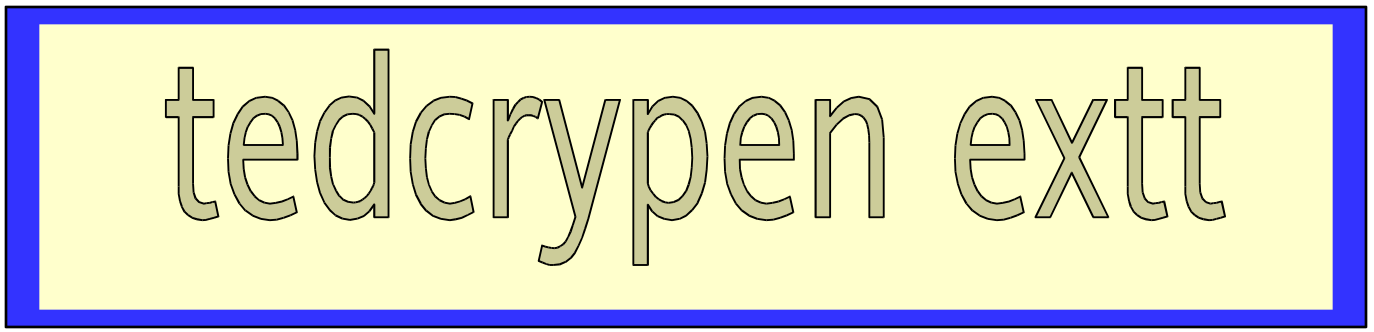
- Static firewall
  - Pre-determined ways of dealing with transmission requests
  - Default-permit
  - Default-deny
- Dynamic firewall
  - Decides on requests as they occur – more flexible, more work
- Internal firewall
- Personal firewall

Detecting Unauthorized Access

- Audit logs – search for suspicious activities
  - Event oriented
  - Keystroke oriented
  - Can generate large log files
- Entrapment server (honeypot)
  - Provide false information
  - Allows tracking of the intruder

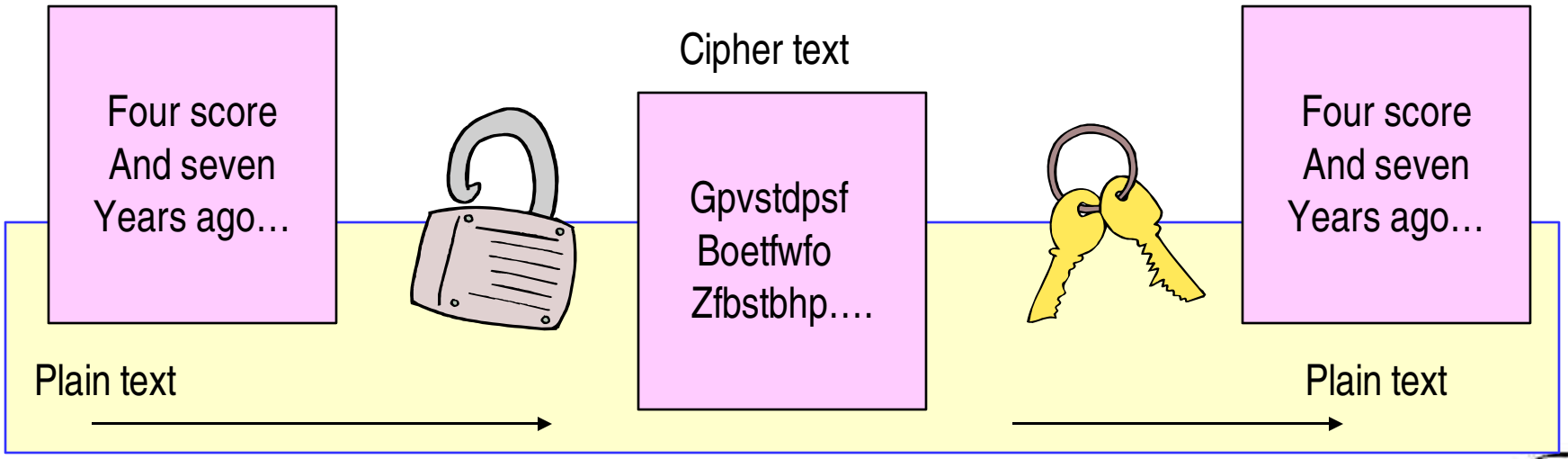
Rendering Data Unreadable: Encryption

- The application of a mathematical algorithm to scramble a message or information to make it unreadable, without using the reverse algorithm
- Cryptography – the study of creating and using encryption and decryption techniques



Encryption Concepts

- Encryption key
- Decryption key
- Ciphertext
- Algorithms called ciphers



Additional Cryptography Concepts

- Key length
- Asymmetric Cryptography
  - Public key
  - Private key
  - Passphrase
  - Example: PGP (Pretty Good Privacy)
    - Available through MIT
- Symmetric Cryptography
  - Difficulty in distributing single key
  - DES (Data Encryption Standard), AES (Advanced Encryption Standard)
  - Triple encryption – more security, requires more processing time

Virus Protection

- Antivirus software
  - Reactive
  - New viruses appear constantly
- Behavioral-based protection tools
  - Look for suspicious behavior
- Self-protection
  - Be careful opening executable files
  - Scan media before loading
  - Avoid opening attachments

Wireless Security

- M-commerce fast growing but susceptible to security breaches
  - Easy to intercept airwave transmission
- Security remedies
  - Digital provides better encryption than analog
  - Authentication of both parties
  - Firewalls to wireless gateways
  - Cautious handling of wireless devices

Managerial Issues

Developing an E-Business Privacy Policy Statement

- Know the local laws
  - Provide clear and conspicuous notice about collection and use of personal information and related user choices
  - Offer choices (opt-in or opt-out)
  - Assure users regarding transfer of information
  - Assure users regarding security of data
  - Assure users regarding data integrity and accuracy
  - Provide access to personal data; opportunity to amend if inaccurate
  - Assure users regarding enforcement of these principles

Basic Content Elements of a Privacy Statement

- Commitment to privacy
- Description of personal information and how used
- Not responsible for 3rd party use
- Level of sharing with 3rd party
- How users can opt out
- Not responsible for info posted on bulletin boards
- How IP addresses are handled
- Use of cookies
- Overview of security measures
- Services for (or not for) children
- How to correct or delete personal information
- That privacy policy may be amended
- Contact information
- Users agree to terms when using site

Security Myths in E-business

- “I’m not on a network, so my PC is safe”
- “I just use a dial-up connection, so my PC is safe”
- “I use an antivirus application, so my PC is safe”
- “I use a firewall, so my PC is safe”

Developing an E-business Security Plan

- Assess risks to the company's computing environments
- Develop a security plan
  - Who can access?
  - What systems are in place to counter each threat?
  - Discussion of all security measures and procedures
- Evaluate the security plan

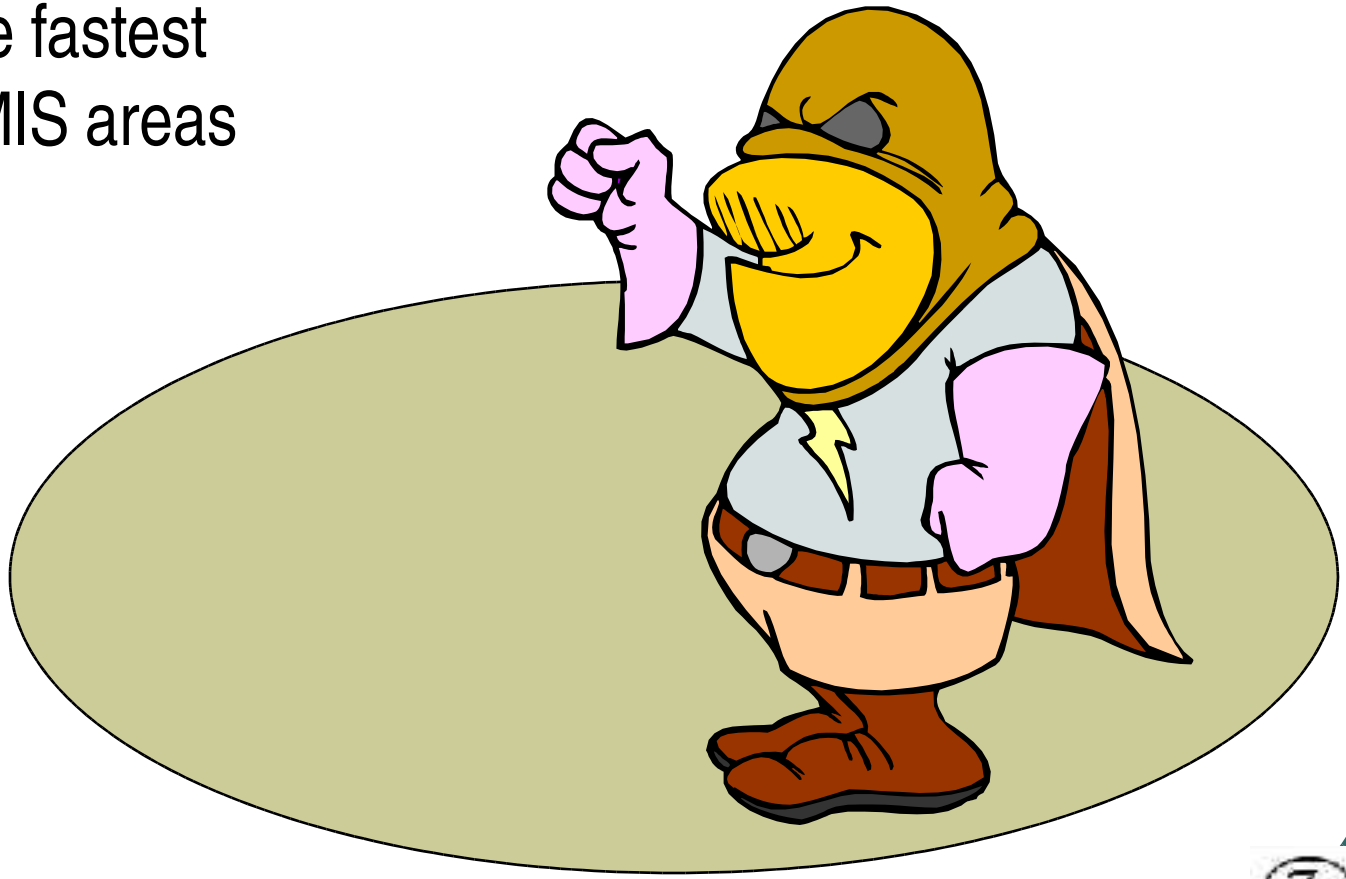
Top Ten Security Mistakes

- The sticky note
- We know better than you (turning off security measures)
- Leaving the computer on while unattended
- Opening email attachments
- Poor password selection
- Loose lips sink ships
- Laptops have legs
- Poorly enforced security policies
- Failing to consider the staff
- Being slow to update

A. S. Horowitz, 2001

Security Jobs

- One of the fastest growing MIS areas



Summary

- Privacy is the confidentiality of data collected by businesses or government about the individuals using their services. Threats to privacy have grown as a result of the collection and integration of huge amounts of data.
- Security threats including unauthorized access, denial of service, theft and fraud pose significant difficulties for organizations. Though not perfect, many devices and strategies have been created to respond to these threats.

Expanding the Domain

- For examples of privacy and security for e-business see:
  - Cookie Central Home Page
    - http://www.cookiecentral.com
  - EPIC Online Guide to Privacy Resources
    - http://www.epic.org/privacy/privacy_resources_faq.html
  - Computer Security Institute
    - http://www.gocsi.com

Copyright © 2003 John Wiley & Sons, Inc.