# Securing Information Systems

Barbarians at the Gateway

## Learning Objectives

- Security breaches are on the rise
- Understand the potentially damaging impact of security breaches
- Security must be made a top organizational priority
- Understand the source and motivation of those initiating information security attacks
- Recognize the potential entry points for security compromise

# Learning Objectives

- Understand infiltration techniques such as social engineering, phishing, malware, Web site compromises (such as SQL injection), and more
- Identify various methods and techniques to thwart infiltration
- Identify critical steps to improve your individual and organizational information security
- Recognize the major information security issues that organizations face; as well as the resources, methods, and approaches that can help make firms more secure

1-3

# Introduction

- Business establishments are increasingly under risk of information security threats
  - Network in TJX retail store was infiltrated via an insecure Wi-Fi base station
  - 45.7 million credit and debit card numbers were stolen
  - Driver's licenses and other private information pilfered from 450,000 customers
  - TJX suffered under settlement costs and court-imposed punitive action to the tune of $150 million
  - **Even without lawsuit liabilities, Forrester Research estimates that the cost to TJX for the data breach could surpass $1 billion over five years.**

1-4

# The TJX Breach

- Factors that amplified severity of TJX security breach are:
  - Personnel betrayal: An alleged FBI informant used insider information to mastermind the attacks
  - **Management** gaffe**:** Executives made conscious **decisions not to upgrade legacy systems that were vulnerable to security compromises**
  - **Technology** lapse: TJX *used WEP, a insecure wireless security technology*
    - failed to follow the **most basic security measures** like installing **antivirus software, upgrading wireless security, encrypting data, and creating and using access controls, and establishing information system controls** (general and application).
  - **Procedural** gaffes: TJX had received an *extension on the rollout of mechanisms that might have discovered and plugged the hole* before the hackers got in
    - **Also willfully violated the Payment Card Industry (PCI) Data Security Standard by holding onto data for years**

1-5

# Lessons Learned

- Information security must be a top organizational priority
- Information security isn't just a technology problem; a host of personnel and procedural factors can create and amplify a firm's vulnerability
- A constant vigilance regarding security needs to be part of individual skill sets and a key component of organizations' culture

1-6

## System Vulnerability and Abuse

- **An unprotected computer connected to Internet may be disabled within seconds**
- **Security:**
  - Policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems
- **Controls:**
  - Methods, policies, and organizational procedures that ensure safety of organization's assets; accuracy and reliability of its accounting records; and operational adherence to management standards



## Why Systems Are Vulnerable

- **Hardware problems**
  - Breakdowns, configuration errors, damage from improper use or crime
- **Software problems**
  - Programming errors, installation errors, unauthorized changes
- **Disasters**
  - Power failures, flood, fires, and so on
- **Use of networks and computers outside of firm's control**
  - E.g., with domestic or offshore outsourcing vendors

System Vulnerability and Abuse

## Contemporary Security Challenges and Vulnerabilities

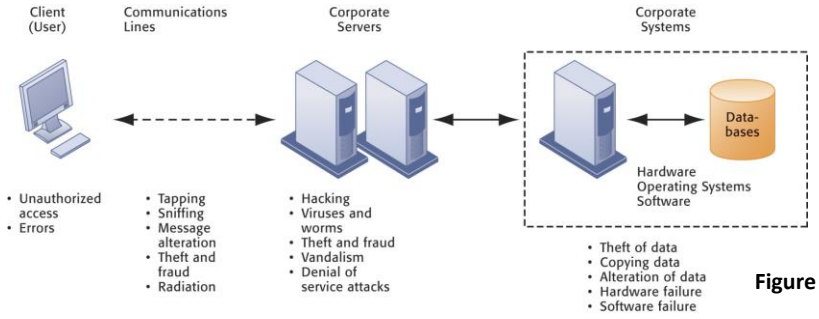


**Figure 7-1**

**The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.**

## System Vulnerability and Abuse

### Internet vulnerabilities

- **Network open to anyone**
- **Size of Internet means abuses can have wide impact**
- **Use of fixed Internet addresses with permanent connections to Internet eases identification by hackers**
- **E-mail attachments**
- **E-mail used for transmitting trade secrets**
- **IM messages lack security, can be easily intercepted**

## Compromising Web Sites

- **SQL injection technique** exploits sloppy programming practices that do not validate user input
  - input SQL statements in a web form to get a badly designed website to dump the database content to the attacker
  - IBM identifies SQL injection as the fastest growing security threat, with over half a million attack attempts recorded each day.
  - Firms have to check the integrity of their Web sites for vulnerabilities
- Related programming exploits:
  - **DNS cache poisoning exploits**
    - can redirect Internet address to IP address mapping and the consequences are huge.
  - Cross-site scripting attacks
    - may be used by attackers to bypass access controls accounted for roughly 80.5% of all security vulnerabilities documented by Symantec as of 2007

1-11

## Securing Wireless Networks - Challenges

- **Radio frequency bands easy to scan**
- **SSIDs (service set identifiers)**
  - **Identify access points.**
  - **Broadcast multiple times.**
- **War driving**
  - **Eavesdroppers drive by buildings and try to intercept network traffic**
  - **When hacker gains access to SSID, has access to network's resources**
- **WEP (Wired Equivalent Privacy)**
  - **Security standard for 802.11**
  - **The WEP specification calls for an access point and its users to share the same 40-bit encrypted password.**
  - **Basic specification uses shared password for both users and access point**
  - **Users often fail to use security features**
  - **Assigning unique name to network's SSID**
  - **TJX fiasco - used WPA**
- **Wi-Fi Alliance finalized WAP2 specification, replacing WEP with stronger standards**
  - **Continually changing keys**
  - **Encrypted authentication system with central server**

System Vulnerability and Abuse

## Wi-Fi Security Challenges

**Many Wi-Fi networks can be penetrated easily by intruders using sniffer programs to obtain an address to access the resources of a network without authorization.**

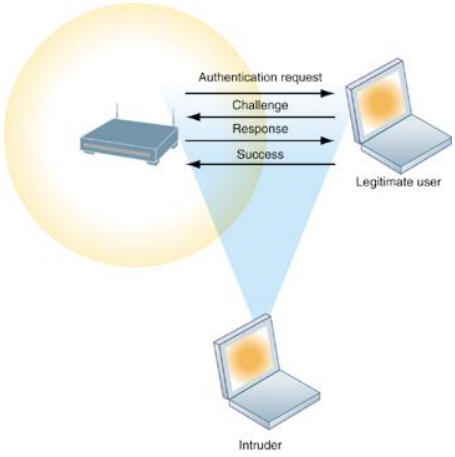


**Figure 7-2**

## Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

- **Malware**
  - **Viruses (email, IM, video, data files downloaded etc)**
    - **Rogue software program that attaches itself to other software programs or data files in order to be executed**
    - Most antivirus software is effective against only those viruses already known when the software is written.
  - **Worms**
    - **Independent computer programs that copy themselves from one computer to other computers over a network**
  - **Trojan horses**
    - **Software program that appears to be benign but then does something other than expected.**
    - In 2004, users were enticed by a sales message from a *supposed* anti-virus vendor.
    - On the vendor's site, a small program called Mitglieder was downloaded to the user's machine. The program enabled outsiders to infiltrate the user's machine.

## Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

- **Malware (cont.)**
  - **Spyware**
    - Small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising
  - **Key loggers**
    - Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks

## Cookies

- ***Cookie*** – a small file that contains information about you and your Web activities, which a Web site places on your computer
- Handle cookies by using
  - Web browser cookie management option
  - Buy a program that manages cookies
- Not executable, cannot deliver a virus or other malicious code
- Only web server that delivered it can read it
- Your computer can store cookies from many web sites
- May be a security risk if it is implemented poorly on site that you have shared personal information with and rely on cookies to access it
  - Anyone who can access the cookie on your hard drive can now access that personal information
  - Most reputable sites to not rely on cookies for authentication alone.

8-16

## Hackers and Computer Crime

- **Activities include:**
  - **System intrusion**
  - **System damage**
  - **Cybervandalism**
    - Intentional disruption, defacement, destruction of Web site or corporate information system

## Hackers and Computer Crime

- **Computer crime**
  - Defined as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution"
  - **Computer may be target of crime:**
    - Breaching confidentiality of protected computerized data
    - Accessing a computer system without authority
  - **Computer may be instrument of crime:**
    - Theft of trade secrets
    - Using e-mail for threats or harassment

## Hackers and Computer Crime

- **Sniffer / Packet sniffer**
  - Eavesdropping program that monitors information traveling over network
  - Enables hackers to steal proprietary information such as e-mail, company files, and so on
    - use your debit card information to purchase items illegally.
    - steal your logon and passwords for various accounts.
    - assume your identity.

## Hackers and Computer Crime

- **Denial-of-service attacks (DoS)**
  - Flooding server with thousands of false requests to crash the network.
- **Distributed denial-of-service attacks (DDoS)**
  - Use of numerous computers to launch a DoS
  - **Botnets**
    - Networks of "zombie" PCs infiltrated by bot malware
    - Zombie PCs used to initiate DDoS attacks
    - Extortionists might leverage botnets or hacked data to demand payment to avoid retribution

## Hackers and Computer Crime

- **Identity theft**
  - Theft of personal information (social security id, driver's license, or credit card numbers) to impersonate someone else
- **Phishing –** *perpetrates a majority of online credit card fraud*
  - Setting up fake Web sites or sending e-mail messages that look like legitimate businesses to ask users for confidential personal data
    - •Requests to reset passwords
    - •Requests to update information
    - •Requests to download malware
- **Evil twins (wireless version of phishing)**
  - Bogus wireless network access points that look legitimate to users
  - Pretend to offer trustworthy Wi-Fi connections to the Internet
  - An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider

## Hackers and Computer Crime

- **Pharming/ spoofing**
  - Redirects users to a bogus Web page, even when individual types correct Web page address into his or her browser
- **Click fraud**
  - Occurs when individual or computer program fraudulently clicks on online ad without any intention of learning more about the advertiser or making a purchase
  - Drives up competitors advertising costs
- **Link farming**
  - a type of online advertising fraud where fraudsters attempt to increase a page's results in organic search by creating a series of bogus Web sites linking back to it

## Internal Threats: Employees

- **Security threats often originate inside an organization.**
  - **Inside knowledge**
  - **Sloppy security procedures**
    - User lack of knowledge
    - Separation of duties, control
      - **San Francisco Hack: Where Was the Oversight?**

## Security Testing

- You may be aware that there are professional security firms that organizations can hire to break into their own networks to test security. BABank (pseudonym) was about to launch a new online banking application, so it hired such a firm to test its security before the launch. The bank's system failed the security test – badly.
- The security team began by mapping the bank's network. It used network security analysis software to test password security, and dialing software to test for dial-in phone numbers. This process found many accounts with default passwords (i.e. passwords set by the manufacturer that are supposed to be changed when the systems are first set up).
- The team then tricked several high-profile users into revealing their passwords to gain access to several high-privilege accounts. Once into these computers, the team used password-cracking software to find passwords on these computers and ultimately gain the administrator passwords on several servers.
- At this point, the team transferred $1000 into their test account. They could have transferred much more, but the security point was made.

## Internal Threats: Employees

- **Social engineering:**
- Con games trick employees into revealing information or performing other tasks that compromise a firm.
- Examples of social engineering methods include:
  - •Baiting someone to add, deny, or clarify information that can help an attacker
  - •Using harassment, guilt, or intimidation
- •Social media sites are a major source of information for social engineering scammers
- •**ChoicePoint** was penetrated through social engineering

## Software Vulnerability

- **Commercial software contains flaws that create security vulnerabilities.**
  - Hidden bugs (program code defects)
    - Zero defects cannot be achieved because complete testing is not possible with large programs
  - Flaws can open networks to intruders
- **Patches**
  - Vendors release small pieces of software to repair flaws.
  - However, amount of software in use can mean exploits created faster than patches can be released and implemented.

## Business Value of Security and Control

- **Failed computer systems can lead to significant or total loss of business function.**
- **Firms now more vulnerable than ever.**
- **A security breach may cut into firm's market value almost immediately.**
- **Inadequate security and controls also bring forth issues of liability.**



### Legal and Regulatory Requirements for Electronic Records Management

- Firms face new legal obligations for the retention and storage of electronic records as well as for privacy protection
  - **HIPAA:** medical security and privacy rules and procedures
  - **Gramm-Leach-Bliley Act:** requires financial institutions to ensure the security and confidentiality of customer data
  - **Sarbanes-Oxley Act:** imposes responsibility on companies and their management to safeguard the accuracy and integrity of financial information that is used internally and released externally

Business Value of Security and Control

## Electronic Evidence and Computer Forensics

- **Evidence for white collar crimes often found in digital form**
  - Data stored on computer devices, e-mail, instant messages, e-commerce transactions
- **Proper control of data can save time, money when responding to legal discovery request**
- **Computer forensics:**
  - Scientific collection, examination, authentication, preservation, and analysis of data from computer storage media for use as evidence in court of law
  - Includes recovery of ambient and hidden data

## Establishing a Framework for Security and Control

- **Types of general controls**
  - **Software controls**
  - **Hardware controls**
  - **Computer operations controls**
  - **Data security controls**
  - **Implementation controls**
  - **Administrative controls**

## Establishing a Framework for Security and Control

- **Application controls**
  - Specific controls unique to each computerized application, such as payroll or order processing.
  - Include both automated and manual procedures.
  - Ensure that only authorized data are completely and accurately processed by that application.
  - Include:
    - **Input controls**
    - **Processing controls**
    - **Output controls**

## Establishing a Framework for Security and Control

- **Risk assessment**
  - Determines level of risk to firm if specific activity or process is not properly controlled
    - **Types of threat**
    - **Probability of occurrence during year**
    - **Potential losses, value of threat**
    - **Expected annual loss**

| EXPOSURE | PROBABILITY | LOSS RANGE | EXPECTED ANNUAL LOSS |
|---|---|---|---|
| Power failure | 30% | $5K - $200K | $30,750 |
| Embezzlement | 5% | $1K - $50K | $1,275 |
| User error | 98% | $200 - $40K | $19,698 |

## Disaster Recovery Planning and Business Continuity Planning

- **Disaster recovery planning:** devises plans for restoration of disrupted services
- **Business continuity planning:** focuses on restoring business operations after disaster
  - Both types of plans needed to identify firm's most critical systems
  - Business impact analysis to determine impact of an outage
  - Management must determine which systems restored first



## The Role of Auditing

- **MIS audit**
  - Examines firm's overall security environment as well as controls governing individual information systems
  - Reviews technologies, procedures, documentation, training, and personnel
  - May even simulate disaster to test response of technology, IS staff, other employees
  - Lists and ranks all control weaknesses and estimates probability of their occurrence.
  - Assesses financial and organizational impact of each threat

## Technologies and Tools for Security

### Access Control

- **Policies and procedures to prevent improper access to systems by unauthorized insiders and outsiders**
  - **Authorization**
  - **Authentication**
    - **Password systems**
    - **Tokens** - may be a physical device or software that an authorized user of computer services is given to ease authentication.
    - **Smart cards**
    - **Biometric authentication**

### Firewalls, Intrusion Detection Systems, and Antivirus Software

- Lock down networks
  - Firewalls control network traffic, block unauthorized traffic and permit acceptable use
  - *Intrusion detection systems* monitor network use for hacking attempts and take preventive action
    - use scanning software to look for known problems such as bad passwords, the removal of important files, security attacks in progress, and system administration errors.
  - Honeypots are seemingly tempting, bogus targets meant to lure hackers

Technologies and Tools for Security

## Encryption and Public Key Infrastructure

- **Encryption:**
  - **Transforming text or data into cipher text that cannot be read by unintended recipients**
  - **Two methods for encryption on networks**
    - **Secure Sockets Layer (SSL) and successor Transport Layer Security (TLS)**
    - **Secure Hypertext Transfer Protocol (S-HTTP)**

## Ensuring System Availability

- **Online transaction processing requires 100 percent availability, no downtime.**
- **Fault-tolerant computer systems**
  - For continuous availability, e.g., stock markets
  - Required for 100% availability, online transaction processing
  - Contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service
- **High-availability computing**
  - Helps recover quickly from crash
  - Minimizes, does not eliminate, downtime

# Hot Site

- A hot site is a commercial disaster recovery service that allows a business to continue computer and network operations in the event of a computer or equipment disaster.
- If an firm's data center becomes inoperable it can move all data processing operations to a hot site.
- A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data.
  - The site has all the equipment needed for the enterprise to continue operation, including office space and furniture, telephone jacks and computer equipment.
- Real time synchronization between the two sites may be used to completely mirror the data environment of the original site.
- Following a disruption to the original site, the hot site exists so that the organization can relocate with minimal losses to normal operations.
- Ideally, a hot site will be up and running within a matter of hours or even less.
- Example – Hurricane Katrina - oil company hot sites

# Cold Site

- A cold site is the most inexpensive type of backup site for an organization to operate.
- Does not include backed up copies of data and information from the original location of the organization,
- Does not include hardware already set up.
  - The lack of hardware contributes to the minimal startup costs of the cold site,
  - Requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.
- Typically, a business has an annual contract with a company that offers hot and cold site services with a monthly service charge.
- Some disaster recovery services offer backup services so that all company data is available regardless of whether a hot site or cold site is used.