# Bảo đảm An toàn Hệ thống thông tin

# Mục tiêu

- Tại sao hệ thống thông tin dễ bị ảnh hưởng bởi lỗi, phá hoại và tống tiền!
- Giá trị của An ninh và Đảm bảo an ninh
- Các thành phần của giải pháp đảm bảo và kiểm soát an ninh
- Các công cụ và công nghệ sử dụng trong bảo vệ tài nguyên thông tin

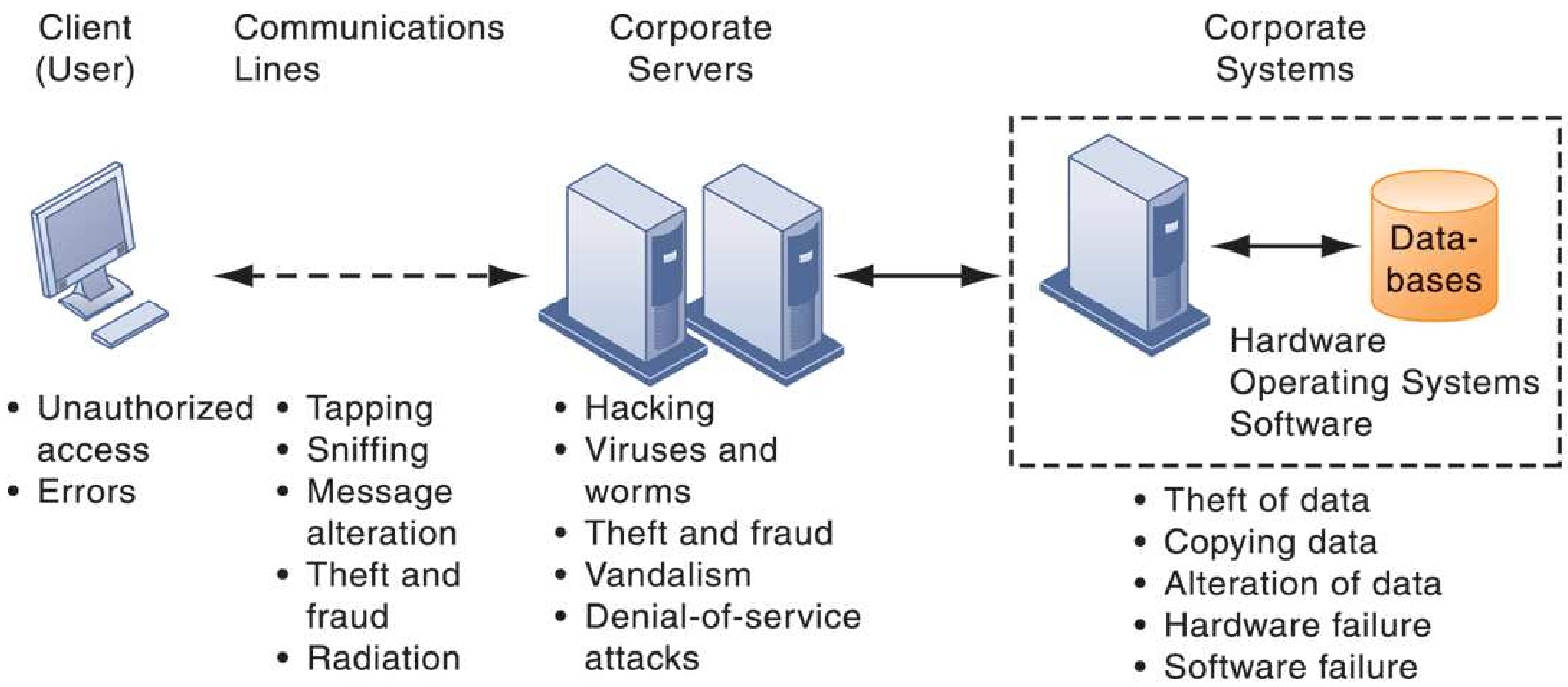
# Mục tiêu

- **Tại sao hệ thống thông tin dễ bị ảnh hưởng bởi lỗi, phá hoại và tống tiền!**
- **Giá trị của An ninh và Đảm bảo an ninh**
- **Các thành phần của giải pháp đảm bảo và kiểm soát an ninh**
- **Các công cụ và công nghệ sử dụng trong bảo vệ tài nguyên thông tin**

# Tại sao Hệ thống thông tin có lỗ hổng

- Truy cập mạng
- Vấn đề phần cứng (hỏng hóc, cấu hình lỗi, sử dụng sai hoặc bị tấn công)
- Vấn đề phần mềm (lỗi lập trình, lỗi cài đặt, thay đổi bất hợp pháp)
- Thảm họa tự nhiên (thiên tai)
- Sử dụng máy tính/mạng ngoài phạm vi kiểm soát của cơ quan of firmʼ s control
- Trộm/cướp các thiết bị di động

## *Thách thức an ninh với Hệ thống thông tin*



Client (User)

- Unauthorized access
- Errors

Communications Lines

- Tapping
- Sniffing
- Message alteration
- Theft and fraud
- Radiation

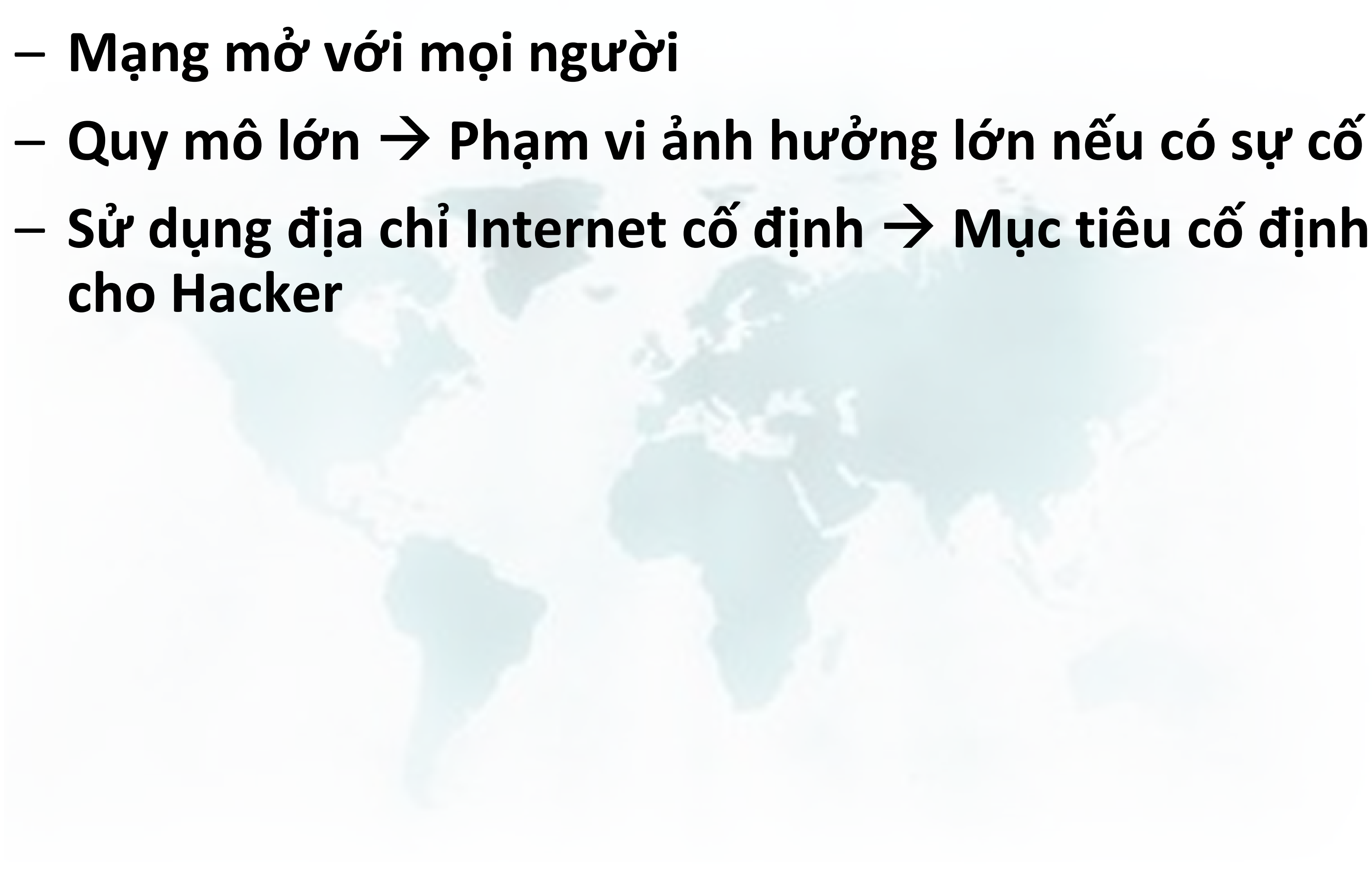
Corporate Servers

- Hacking
- Viruses and worms
- Theft and fraud
- Vandalism
- Denial-of-service attacks

Corporate Systems

- Theft of data
- Copying data
- Alteration of data
- Hardware failure
- Software failure

# Lỗ hổng Internet



- Mạng mở với mọi người
- Quy mô lớn → Phạm vi ảnh hưởng lớn nếu có sự cố
- Sử dụng địa chỉ Internet cố định → Mục tiêu cố định cho Hacker

# Malware

- **Viruses**
- **Worms**
- **Worms và viruses được phát tán bởi**
  - Downloads (drive-by downloads)
  - E-mail,  attachments
  - Downloads on Web sites and social networks

# Malware

- **Malware (cont.)**
  - **Smartphones có lỗ hổng như PC**
    - Study finds 13,000 types of smartphone malware
  - **Trojan horses**
    - Software that appears benign but does something other than expected. Ex : MMarketPay.A
  - **SQL injection attacks**
    - Hackers submit data to Web forms that exploits siteʼ s unprotected software and sends rogue SQL query to database

## System Vulnerability and Abuse

- **Malware (cont.) :** **salah satu bentuk program berbahaya yang memasang dirinya sendiri ke dalam sebuah sistem untuk mencuri data pengguna atau merusak sistem pengguna tersebut**
  - **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
    - Other types:
      - Reset browser home page
      - Redirect search requests
      - Slow computer performance by taking up memory

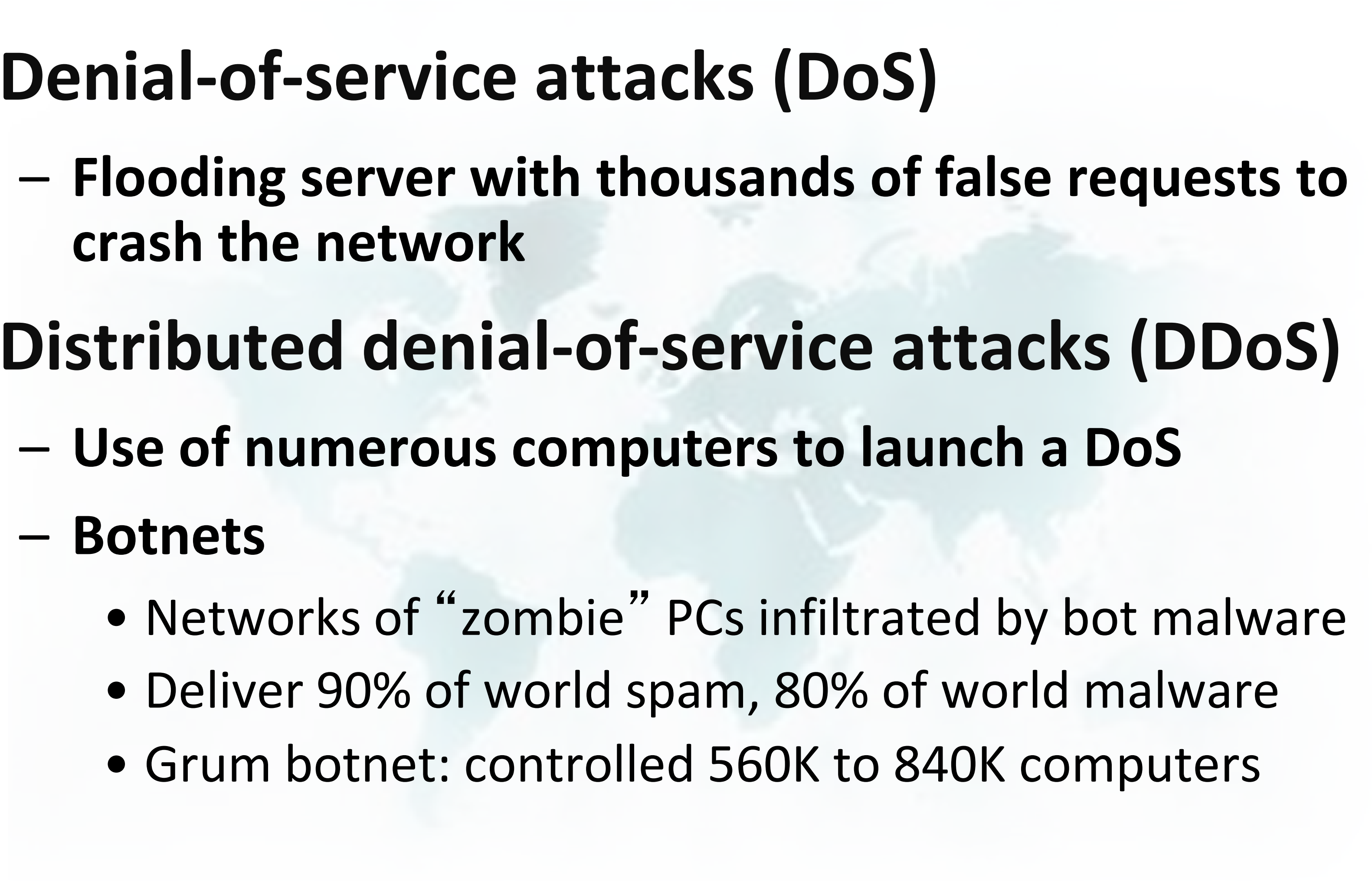
## System Vulnerability and Abuse

- **Hackers and computer crime**
  - **Hackers vs. crackers**
  - **Activities include:**
    - System intrusion
    - System damage
    - Cybervandalism
      - destruction of Web site or corporate information system

## System Vulnerability and Abuse

- Spoofing
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Redirecting Web link to address different from intended one, with site masquerading as intended destination
- Sniffer
  - Eavesdropping program that monitors information traveling over network
  - Enables hackers to steal proprietary information such as e-mail, company files, and so on

# System Vulnerability and Abuse



- **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
    - Deliver 90% of world spam, 80% of world malware
    - Grum botnet: controlled 560K to 840K computers

## System Vulnerability and Abuse

- **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, for example:**
    - Breaching confidentiality of protected computerized data
    - Accessing a computer system without authority
  - **Computer may be instrument of crime, for example:**
    - Theft of trade secrets
    - Using e-mail for threats or harassment

# System Vulnerability and Abuse

- Identity theft
  - Theft of personal Information (social security ID, driver' s license, or credit card numbers) to impersonate someone else
- Phishing
  - Setting up fake Web sites or sending e-mail messages that look like legitimate businesses to ask users for confidential personal data.
- Evil twins
  - Wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet

## System Vulnerability and Abuse

- Pharming
  - 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
- Cyberterrorism and Cyberwarfare

# Stuxnet and the Changing Face of Cyberwarfare

- Is cyberwarfare a serious problem? Why or why not?
- Assess the management, organization, and technology factors that have created this problem.
- What makes Stuxnet different from other cyberwarfare attacks? How serious a threat is this technology?
- What solutions have been proposed for this problem? Do you think they will be effective? Why or why not?

## System Vulnerability and Abuse

- **Internal threats: Employees**
  - **Security threats often originate inside an organization**
  - **Inside knowledge**
  - **Sloppy security procedures**
    - User lack of knowledge
  - **Social engineering:**
    - Tricking employees into revealing their passwords by pretending to be legitimate members of the company in need of information

# System Vulnerability and Abuse

- **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**
    - Small pieces of software to repair flaws
    - Exploits often created faster than patches can be released and implemented

# Mục tiêu

- Tại sao hệ thống thông tin dễ bị ảnh hưởng bởi lỗi, phá hoại và tống tiền!
- **Giá trị của An ninh và Đảm bảo an ninh**
- Các thành phần của giải pháp đảm bảo và kiểm soát an ninh
- Các công cụ và công nghệ sử dụng trong bảo vệ tài nguyên thông tin

# Business Value of Security and Control

- Failed computer systems can lead to significant or total loss of business function.
- Firms now are more vulnerable than ever.
  - Confidential personal and financial data
  - Trade secrets, new products, strategies
- A security breach may cut into a firm’ s market value almost immediately.
- Inadequate security and controls also bring forth issues of liability.

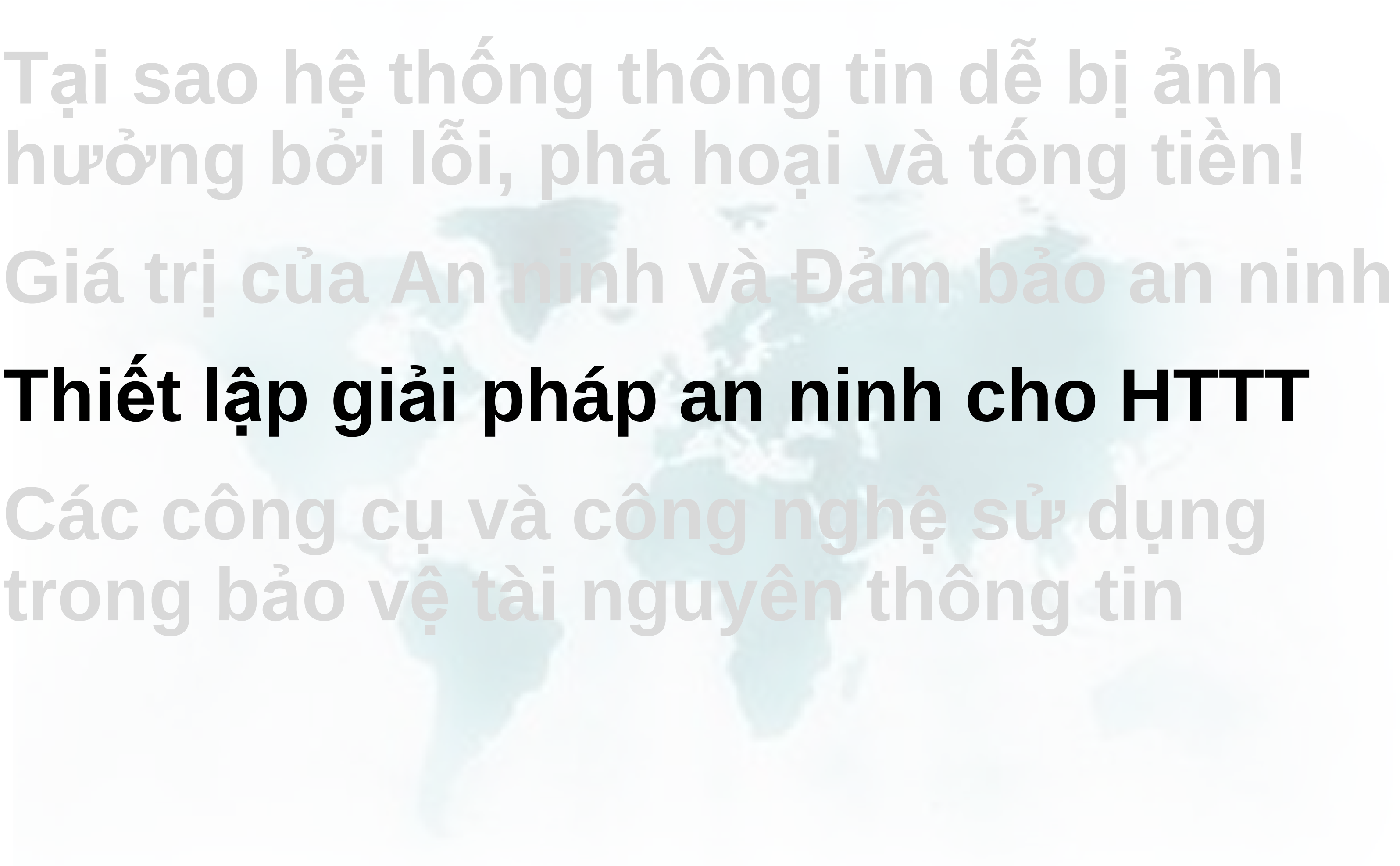
## Business Value of Security and Control

- **Legal and regulatory requirements for electronic records management and 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**
  - **Evidence for white collar crimes often in digital form**
    - Data on computers, e-mail, instant messages, e-commerce transactions
  - **Proper control of data can save time and 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**

# Mục tiêu



- Tại sao hệ thống thông tin dễ bị ảnh hưởng bởi lỗi, phá hoại và tống tiền!
- Giá trị của An ninh và Đảm bảo an ninh
- **Thiết lập giải pháp an ninh cho HTTT**
- Các công cụ và công nghệ sử dụng trong bảo vệ tài nguyên thông tin

## Establishing a Framework for Security and Control

- **Information systems controls (kiểm soát)**
  - Manual and automated controls
  - General and application controls
- **General controls (kiểm soát)**
  - **Govern design, security, and use of computer programs and security of data files in general throughout organization’ s information technology infrastructure**
  - **Apply to all computerized applications**
  - **Combination of hardware, software, and manual procedures to create overall control environment**

## Establishing a Framework for Security and Control

- Types of general controls (kiểm soát)
  - Software controls
  - Hardware controls
  - Computer operations controls
  - Data security controls
  - Implementation controls
  - Administrative controls

# Establishing a Framework for Security and Control

- Application controls (kiểm soát)
  - 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 (AVG) | EXPECTED ANNUAL LOSS |
|---|---|---|---:|
| Power failure | 30% | $5K–$200K ($102,500) | $30,750 |
| Embezzlement | 5% | $1K–$50K ($25,500) | $1,275 |
| User error | 98% | $200–$40K ($20,100) | $19,698 |

# Establishing a Framework for Security and Control

- **Security policy**
  - **Ranks information risks, identifies acceptable security goals, and identifies mechanisms for achieving these goals**
  - **Drives other policies**
    - Acceptable use policy (AUP)
      - Defines acceptable uses of firm’s information resources and computing equipment
    - Authorization policies
      - Determine differing levels of  user access to information assets

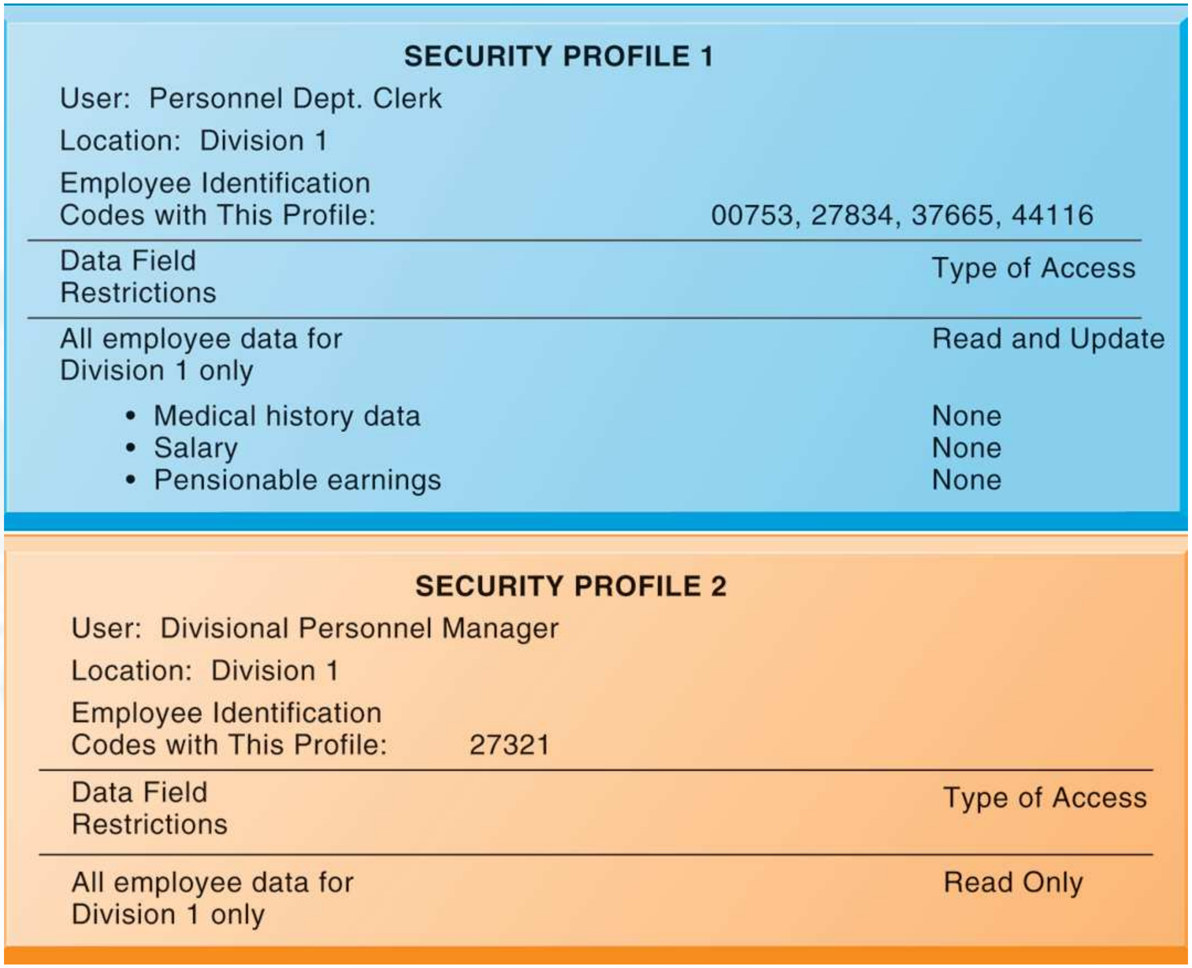
## Establishing a Framework for Security and Control

- **Identity management**
  - **Business processes and tools to identify valid users of system and control access**
    - Identifies and authorizes different categories of users
    - Specifies which portion of system users can access
    - Authenticating users and protects identities
  - **Identity management systems**
    - Captures access rules for different levels of users

# SECURITY PROFILES FOR A PERSONNEL SYSTEM

These two examples represent two security profiles or data security patterns that might be found in a personnel system. Depending on the security profile, a user would have certain restrictions on access to various systems, locations, or data in an organization.

**FIGURE 8-3**



**SECURITY PROFILE 1**

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

| Data Field Restrictions | Type of Access |
|---|---|
| All employee data for Division 1 only | Read and Update |
| • Medical history data | None |
| • Salary | None |
| • Pensionable earnings | None |

**SECURITY PROFILE 2**

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile: 27321

| Data Field Restrictions | Type of Access |
|---|---|
| All employee data for Division 1 only | Read Only |

## Establishing a Framework for Security and Control

- **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**

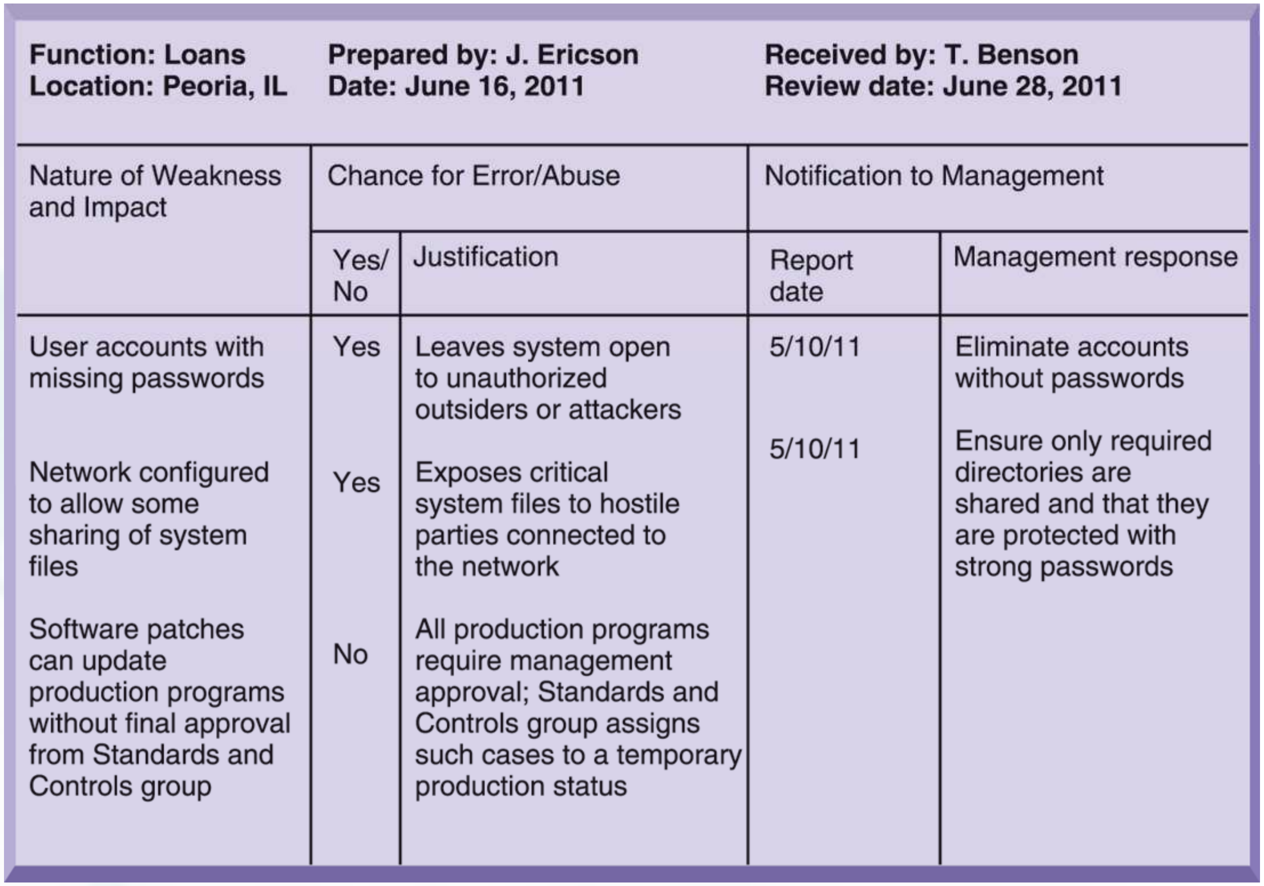
## Establishing a Framework for Security and Control

- **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

# SAMPLE AUDITOR 'S LIST OF CONTROL WEAKNESSES

This chart is a sample page from a list of control weaknesses that an auditor might find in a loan system in a local commercial bank. This form helps auditors record and evaluate control weaknesses and shows the results of discussing those weaknesses with management, as well as any corrective actions taken by management.

**FIGURE 8-4**



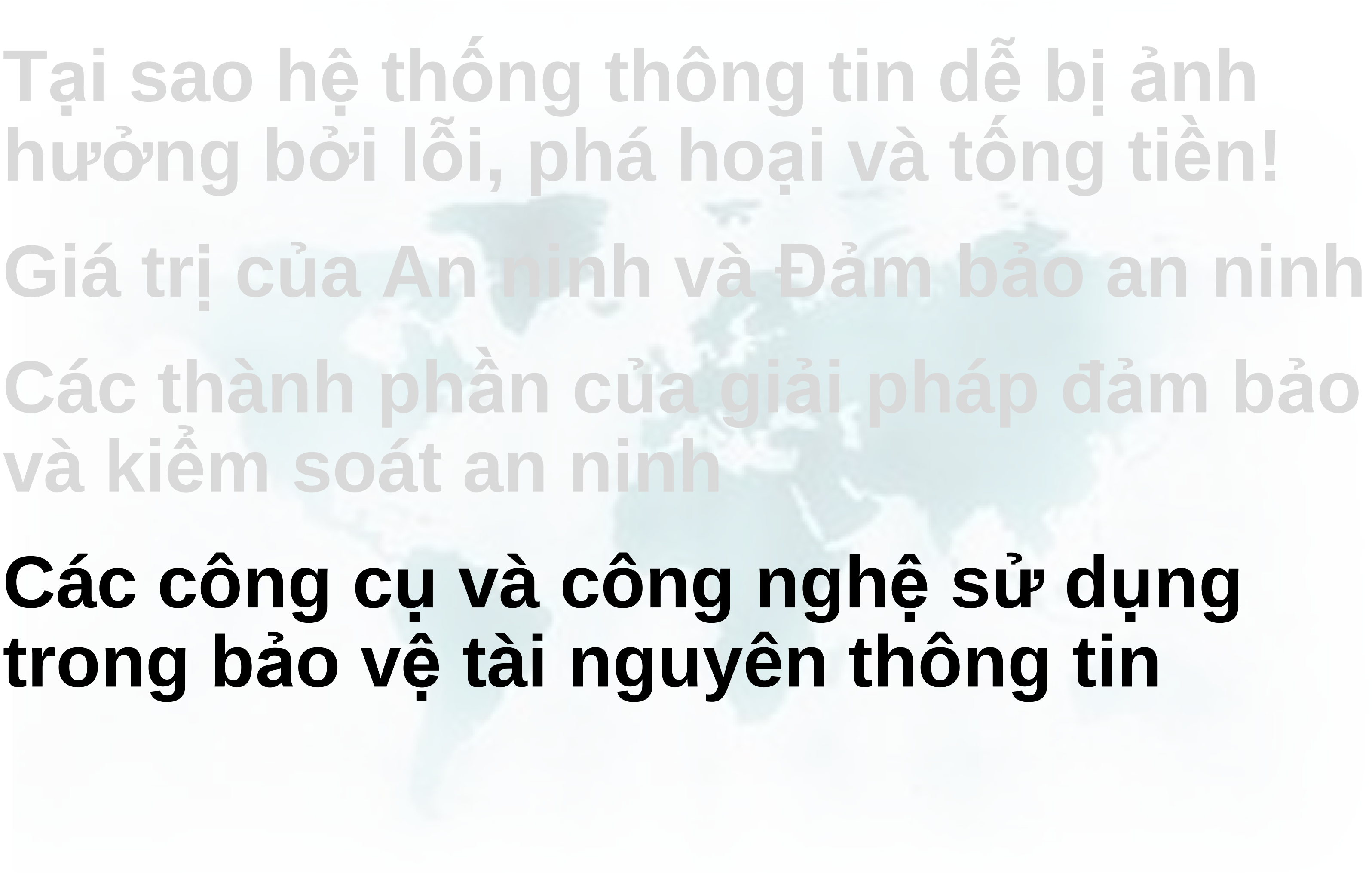
**Function: Loans**
**Location: Peoria, IL**

**Prepared by: J. Ericson**
**Date: June 16, 2011**

**Received by: T. Benson**
**Review date: June 28, 2011**

| Nature of Weakness and Impact | Chance for Error/Abuse | | Notification to Management | |
|---|---|---|---|---|
| | Yes/ No | Justification | Report date | Management response |
| User accounts with missing passwords | Yes | Leaves system open to unauthorized outsiders or attackers | 5/10/11 | Eliminate accounts without passwords |
| Network configured to allow some sharing of system files | Yes | Exposes critical system files to hostile parties connected to the network | 5/10/11 | Ensure only required directories are shared and that they are protected with strong passwords |
| Software patches can update production programs without final approval from Standards and Controls group | No | All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status | | |

# Mục tiêu



- Tại sao hệ thống thông tin dễ bị ảnh hưởng bởi lỗi, phá hoại và tống tiền!
- Giá trị của An ninh và Đảm bảo an ninh
- Các thành phần của giải pháp đảm bảo và kiểm soát an ninh
- **Các công cụ và công nghệ sử dụng trong bảo vệ tài nguyên thông tin**

# Technologies and Tools for Protecting Information Resources

- Identity management software
  - Automates keeping track of all users and privileges
  - Authenticates users, protecting identities, controlling access
- Authentication
  - Password systems
  - Tokens
  - Smart cards
  - Biometric authentication

Hospital LOGO & Name

Patient
SUSAN B JONES-SMITH

DOB 11/14/1978
Issued 5/14/10

Confidential Patient ID
808400 123456 789012

Provider (80840)
1234 567 893

## Technologies and Tools for Protecting Information Resources

- **Firewall:**
  - **Combination of hardware and software that prevents unauthorized users from accessing private networks**
  - **Technologies include:**
    - Static packet filtering
    - Stateful inspection
    - Network address translation (NAT)
    - Application proxy filtering

# *A CORPORATE FIREWALL*

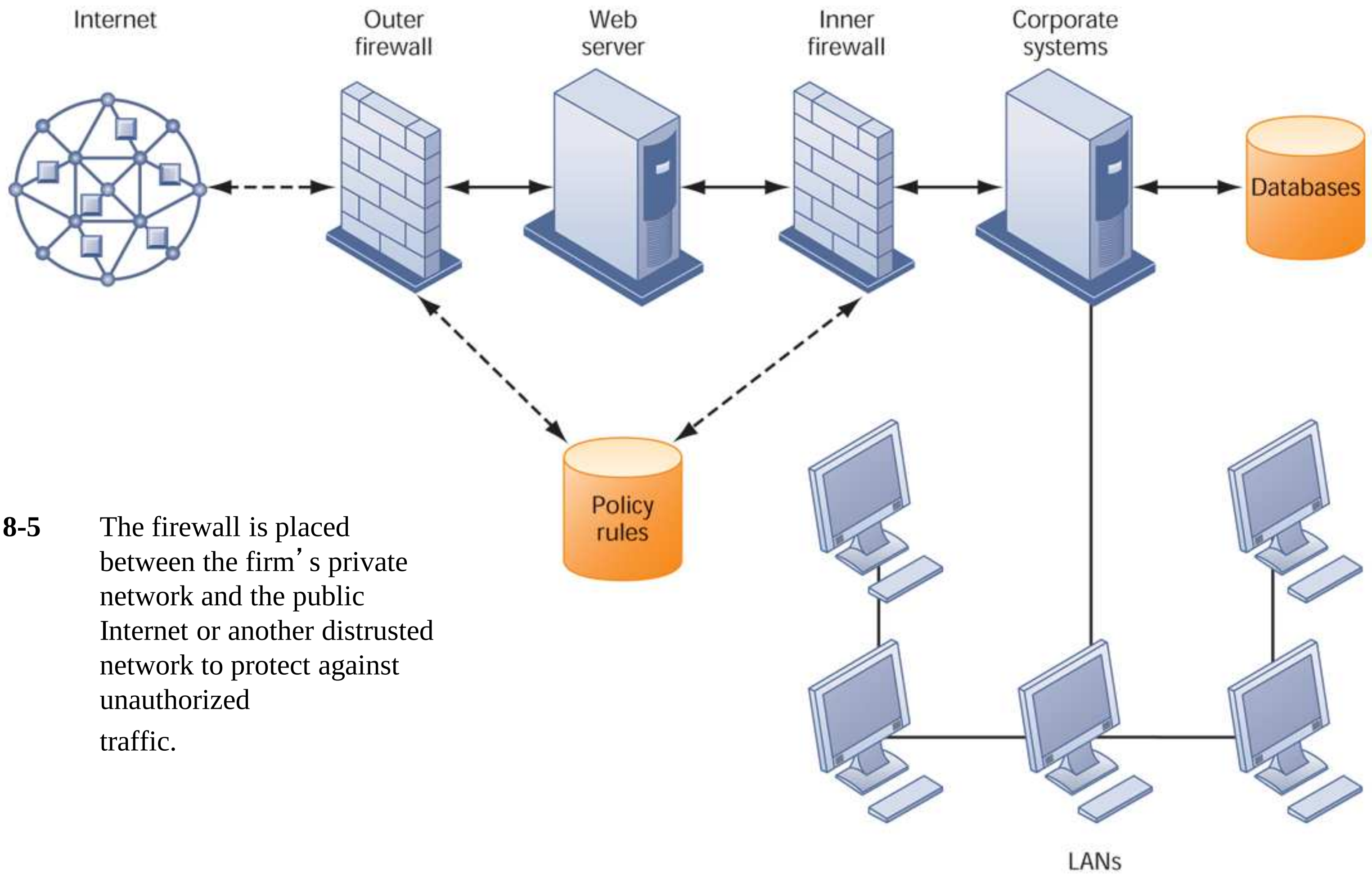


**FIGURE 8-5** The firewall is placed between the firm's private network and the public Internet or another distrusted network to protect against unauthorized traffic.

## Technologies and Tools for Protecting Information Resources

- **Intrusion detection systems:**
  - – Monitors hot spots on corporate networks to detect and deter intruders
  - – Examines events  as they are happening to discover attacks in progress
- **Antivirus and antispyware software:**
  - – Checks computers for presence of malware and can often eliminate it as well
  - – Requires continual updating
- **Unified threat management (UTM) systems**

## Technologies and Tools for Protecting Information Resources

- **Securing wireless networks**
  - **WEP security can provide some security by:**
    - Assigning unique name to network’ s SSID and not broadcasting SSID
    - Using it with VPN technology
  - **Wi-Fi Alliance finalized WAP2 specification, replacing WEP with stronger standards**
    - Continually changing keys
    - Encrypted authentication system with central server

## Technologies and Tools for Protecting Information Resources

- **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)

## Technologies and Tools for Protecting Information Resources

- **Two methods of encryption**
  - **Symmetric key encryption**
    - Sender and receiver use single, shared key
  - **Public key encryption**
    - Uses two, mathematically related keys: Public key and private key
    - Sender encrypts message with recipient's public key
    - Recipient decrypts with private key

# *PUBLIC KEY ENCRYPTION*

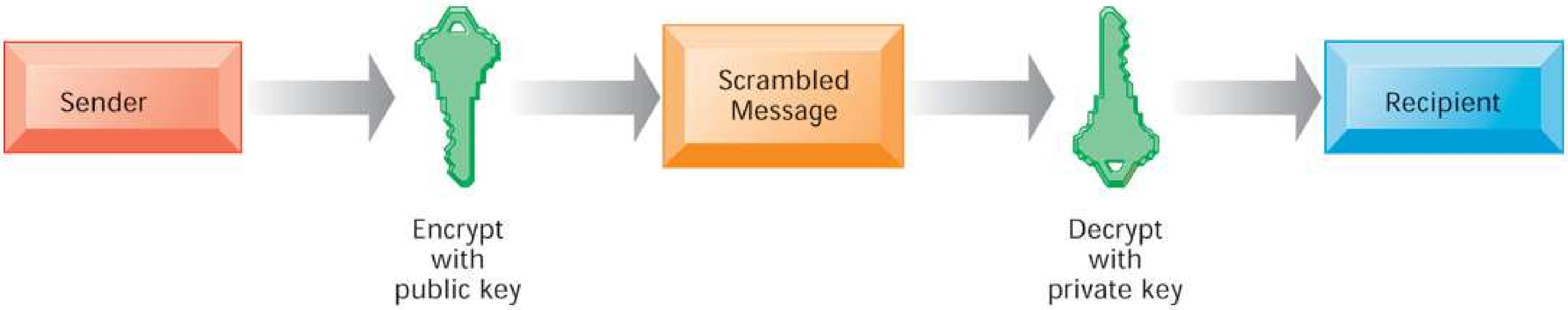


**FIGURE 8-6** A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message is sent in encrypted form over the Internet or a private network. When the encrypted message arrives, the recipient uses his or her private key to decrypt the data and read the message.

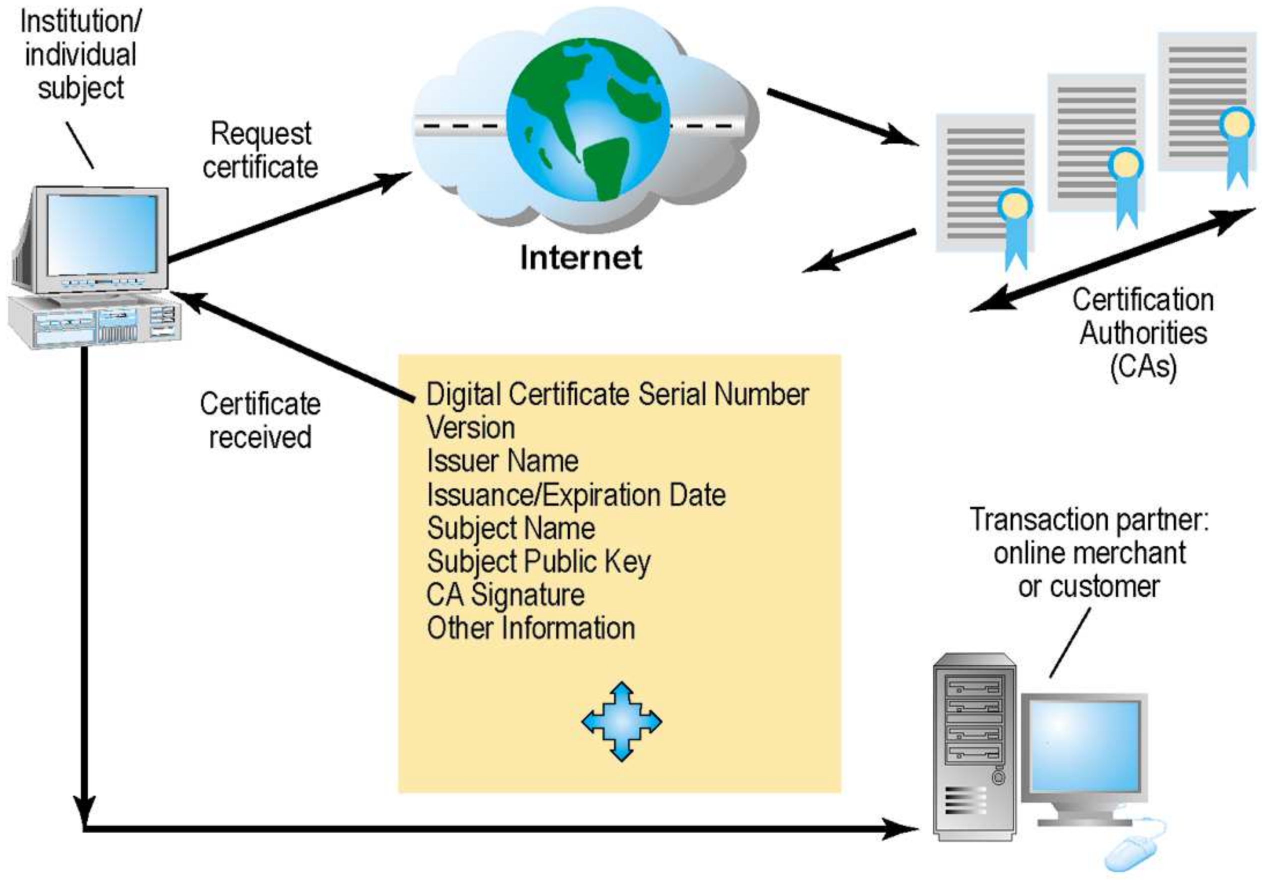
## Technologies and Tools for Protecting Information Resources

- **Digital certificate:**
  - Data file used to establish the identity of users and electronic assets for protection of online transactions
  - Uses a trusted third party, certification authority (CA), to validate a user’ s identity
  - CA verifies user’ s identity, stores information in CA server, which generates encrypted digital certificate containing owner ID information and copy of owner’ s public key
- **Public key infrastructure (PKI)**
  - Use of public key cryptography working with certificate authority
  - Widely used in e-commerce

# DIGITAL CERTIFICATES

Digital certificates help establish the identity of people or electronic assets. They protect online transactions by providing secure, encrypted, online communication.

**FIGURE 8-7**


Institution/ individual subject
Request certificate
Internet
Certification Authorities (CAs)
Certificate received
Transaction partner: online merchant or customer

Digital Certificate Serial Number
Version
Issuer Name
Issuance/Expiration Date
Subject Name
Subject Public Key
CA Signature
Other Information

## Technologies and Tools for Protecting Information Resources

- **Ensuring system availability**
  - Online transaction processing requires 100% availability, no downtime
- **Fault-tolerant computer systems**
  - For continuous availability, for example, stock markets
  - 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

## Technologies and Tools for Protecting Information Resources

- **Recovery-oriented computing**
  - **Designing systems that recover quickly with capabilities to help operators pinpoint and correct faults in multi-component systems**
- **Controlling network traffic**
  - **Deep packet inspection (DPI)**
    - Video and music blocking
- **Security outsourcing**
  - **Managed security service providers (MSSPs)**

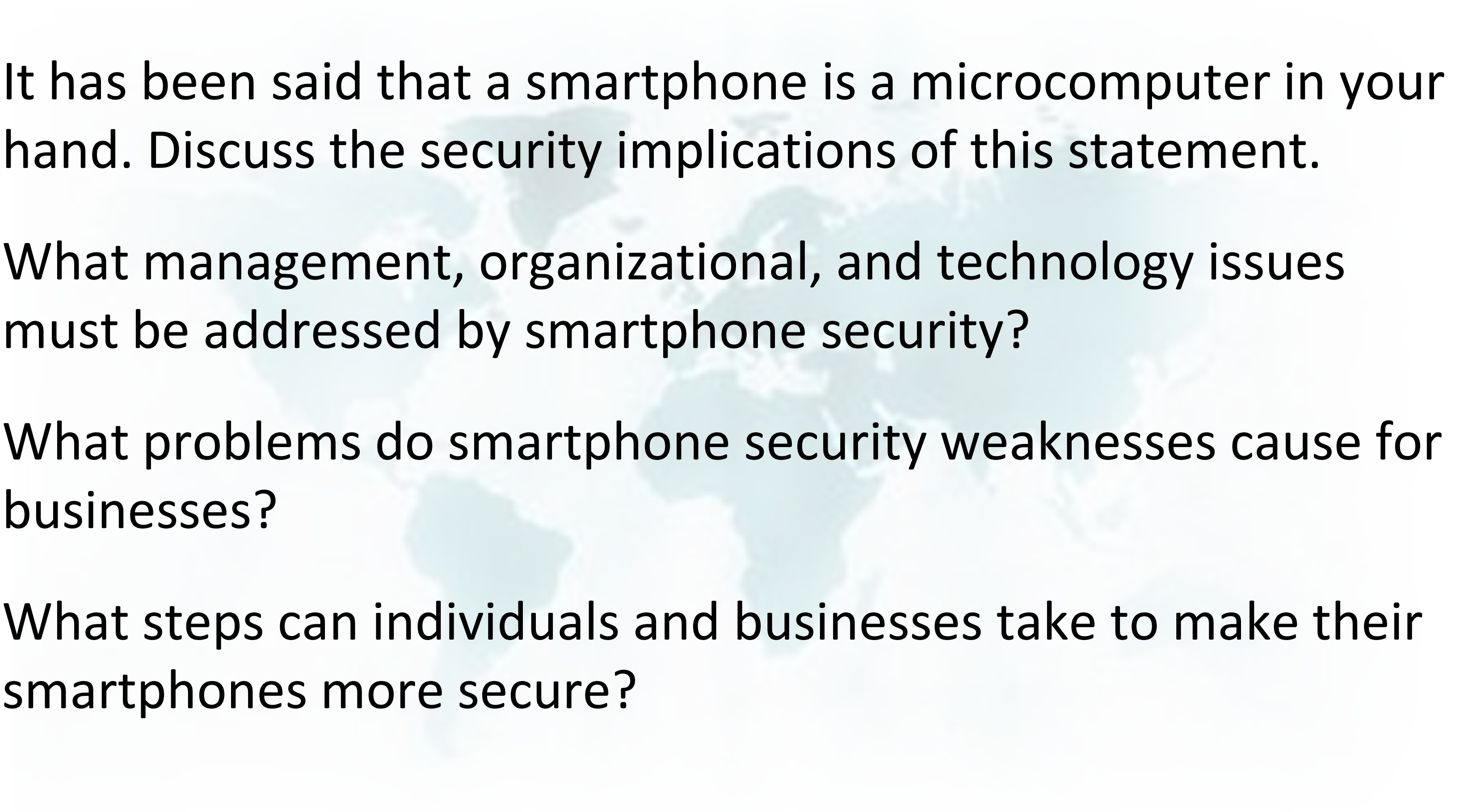
## Technologies and Tools for Protecting Information Resources

- **Security in the cloud**
  - **Responsibility for security resides with company owning the data**
  - **Firms must ensure providers provides adequate protection:**
    - Where data are stored
    - Meeting corporate requirements, legal privacy laws
    - Segregation of data from other clients
    - Audits and security certifications
  - **Service level agreements (SLAs)**

## Technologies and Tools for Protecting Information Resources

- **Securing mobile platforms**
  - **Security policies should include and cover any special requirements for mobile devices**
    - Guidelines for use of platforms and applications
  - **Mobile device management tools**
    - Authorization
    - Inventory records
    - Control updates
    - Lock down/erase lost devices
    - Encryption
  - **Software for segregating corporate data on devices**

# How Secure Is Your Smartphone?



- It has been said that a smartphone is a microcomputer in your hand. Discuss the security implications of this statement.
- What management, organizational, and technology issues must be addressed by smartphone security?
- What problems do smartphone security weaknesses cause for businesses?
- What steps can individuals and businesses take to make their smartphones more secure?

## Technologies and Tools for Protecting Information Resources

- **Ensuring software quality**
  - **Software metrics: Objective assessments of system in form of quantified measurements**
    - Number of transactions
    - Online response time
    - Payroll checks printed per hour
    - Known bugs per hundred lines of code
  - **Early and regular testing**
  - **Walkthrough: Review of specification or design document by small group of qualified people**
  - **Debugging: Process by which errors are eliminated**