Securing Information Systems

Part II

Information Technology Infrastructure

Paulo Faroleiro

Information Systems

Topic 8

Part II
Information Technology Infrastructure

Learning Objectives

1. Why are information systems vulnerable to destruction, error, and abuse?
2. What is the business value of security and control?
3. What are the components of an organizational framework for security and control?
4. What are the most important tools and technologies for safeguarding information resources?

Topic 8: Securing Information Systems

- Case 1: Stuxnet and Cyberwarfare
- Case 2: BYOD: A Security Nightmare?

Case Study:

Why Systems Are Vulnerable (1 of 2)

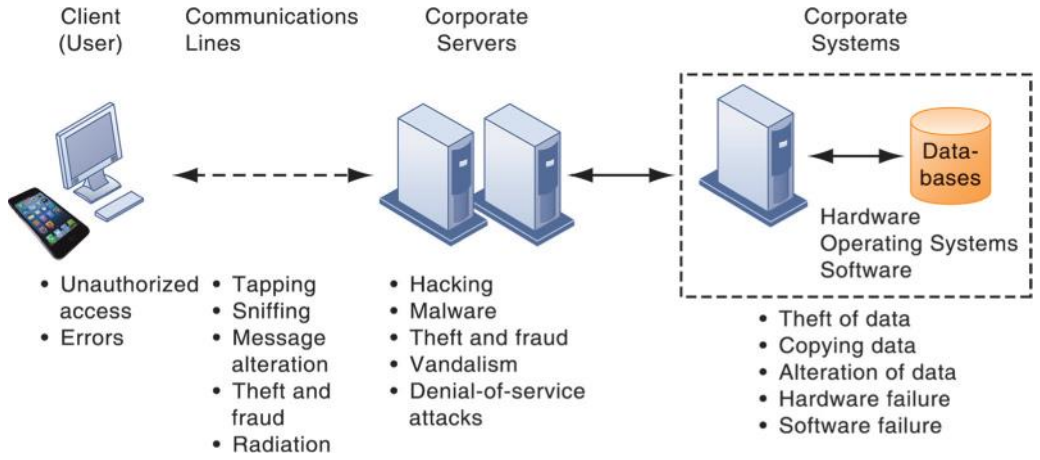
- **Security**
  - **Policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems**
- **Controls**
  - **Methods, policies, and organizational procedures that ensure safety of organization's assets; accuracy and reliability of its accounting records; and operational adherence to management standards**

Why Systems Are Vulnerable (2 of 2)

- Accessibility of networks
- Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
- Software problems (programming errors, installation errors, unauthorized changes)
- Disasters
- Use of networks/computers outside of firm's control
- Loss and theft of portable devices

Internet Vulnerabilities

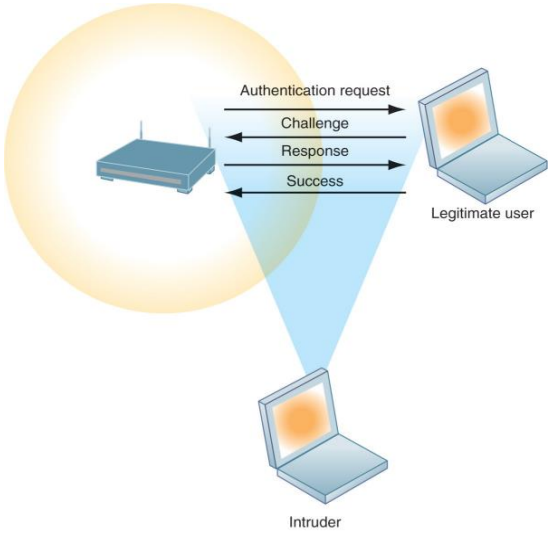
- **Network open to anyone**
- **Size of Internet means abuses can have wide impact**
- **Use of fixed Internet addresses with cable / DSL modems creates fixed targets for hackers**
- **Unencrypted VOIP**
- **E-mail, P2P, IM**
  - **Interception**
  - **Attachments with malicious software**
  - **Transmitting trade secrets**

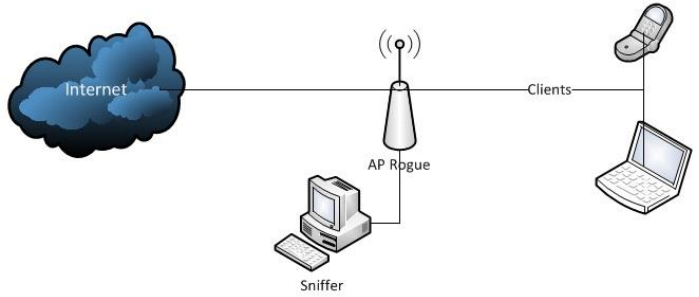


Contemporary Security Challenges and Vulnerabilities

Wireless Security Challenges

- **Radio frequency bands easy to scan**
- **SSIDs (service set identifiers)**
  - **Identify access points, broadcast multiple times, can be identified by sniffer programs**
- **War driving**
  - **Eavesdroppers drive by buildings and try to detect SSID and gain access to network and resources**
  - **Once access point is breached, intruder can gain access to networked drives and files**
- **Rogue access points**





Wi-Fi Security Challenges

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

- **Malware (malicious software)**
- **Viruses**
- **Worms**
- **Worms and viruses spread by**
  - **Downloads and drive-by downloads**
  - **E-mail, IM attachments**
- **Mobile device malware**
- **Social network malware**
- **Trojan horse**
- **SQL injection attacks**
- **Ransomware**
- **Spyware**
  - **Key loggers**
  - **Other types**
    - Reset browser home page
    - Redirect search requests
    - Slow computer performance by taking up memory

Hackers and Computer Crime

- **Hackers vs. crackers**
- **Activities include:**
  - **System intrusion**
  - **System damage**
  - **Cybervandalism**
    - Intentional disruption, defacement, destruction of website or corporate information system
- **Spoofing and sniffing**
- **Denial-of-service attacks (DoS)**
- **Distributed denial-of-service attacks (DDoS)**
- **Botnets**
- **Spam**
- **Computer crime**
  - **Computer may be target of crime**
  - **Computer may be instrument of crime**
- **Identity theft**
  - **Phishing**
  - **Evil twins**
  - **Pharming**
- **Click fraud**
- **Cyberterrorism, Cyberwarfare**

Internal Threats: Employees

- Security threats often originate inside an organization
- Inside knowledge
- Sloppy security procedures
  - User lack of knowledge
- Social engineering
- Both end users and information systems specialists are sources of risk

Software Vulnerability

- **Commercial software contains flaws that create security vulnerabilities**
  - **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**

What Is the 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**

Legal and Regulatory Requirements for Electronic Records Management

- **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**

Electronic Evidence and Computer Forensics

- **Electronic evidence**
  - **Evidence for white collar crimes often in digital form**
  - **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**
  - **Recovery of ambient data**

Information Systems Controls

- **May be automated or manual**
- **General controls**
  - **Govern design, security, and use of computer programs and security of data files in general throughout organization**
  - **Software controls, hardware controls, computer operations controls, data security controls, system development controls, administrative controls,**
- **Application controls**
  - **Controls unique to each computerized application**
  - **Input controls, processing controls, output controls**

Interactive Session: Organization

Stuxnet and the Changing Face of Cyberwarfare

Read the Interactive Session and discuss the following questions

- **Class discussion**
  - 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?

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 OF OCCURRENCE	LOSS RANGE (AVERAGE) ($)	EXPECTED ANNUAL LOSS ($)
Power failure	30%	$5,000 - $200,000 ($102,500)	$30,750
Embezzlement	5%	$1,000 - $50,000 ($25,500)	$1275
User error	98%	$200 - $40,000 ($20,100)	$19,698

Online Order Processing Risk Assessment

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
- **Identity management**
  - **Identifying valid users**
  - **Controlling access**

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

Access Rules for a Personnel System

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

- **Information systems audit**
  - **Examines firm's overall security environment as well as controls governing individual information systems**
- **Security audits**
  - **Review technologies, procedures, documentation, training, and personnel**
  - **May even simulate disaster to test responses**
- **List and rank control weaknesses and the probability of occurrence**
- **Assess financial and organizational impact of each threat**

Function: Loans Location: Peoria, IL	Prepared by: J. Ericson Date: June 16, 2016		Received by: T. Benson Review date: June 28, 2016	
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	5/10/16	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	5/10/16	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		

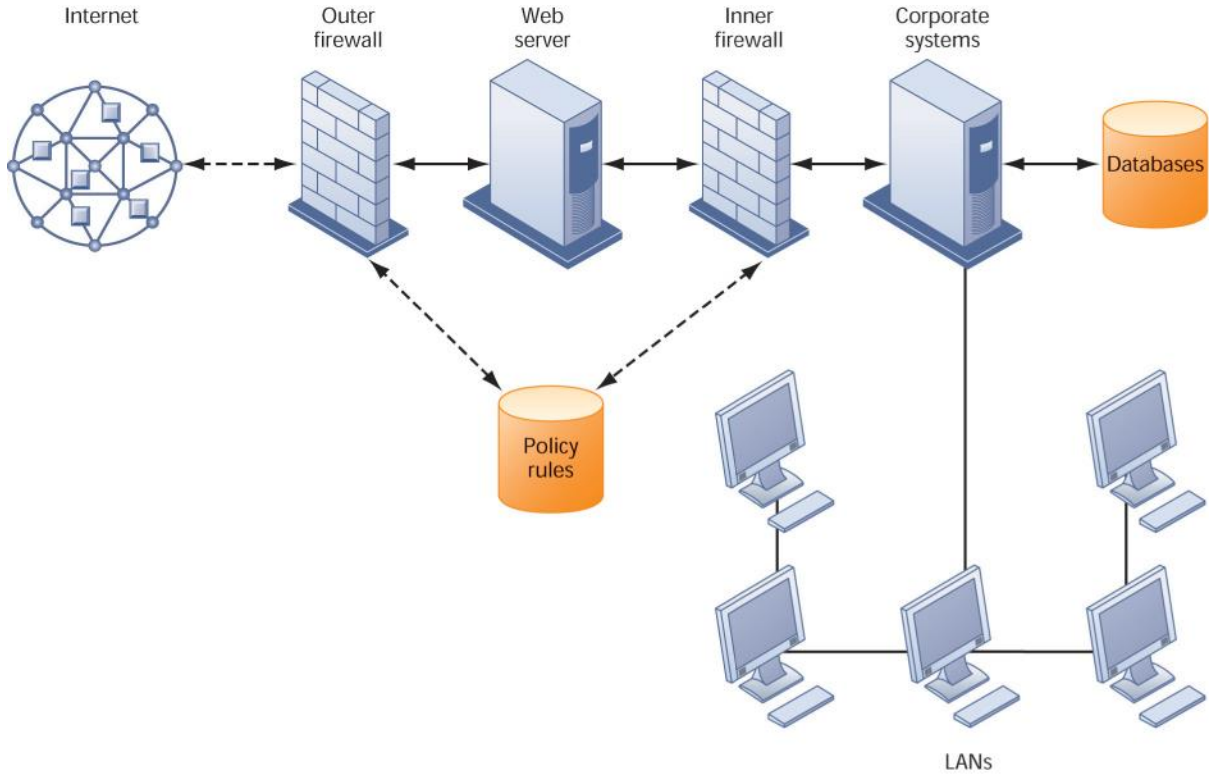
Sample Auditor's List of Control Weaknesses

What Are the Most Important Tools and Technologies for Safeguarding Information Systems? (1 of 2)

- **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
  - Two-factor authentication

What Are the Most Important Tools and Technologies for Safeguarding Information Systems? (2 of 2)

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



A Corporate Firewall

Securing Wireless Networks

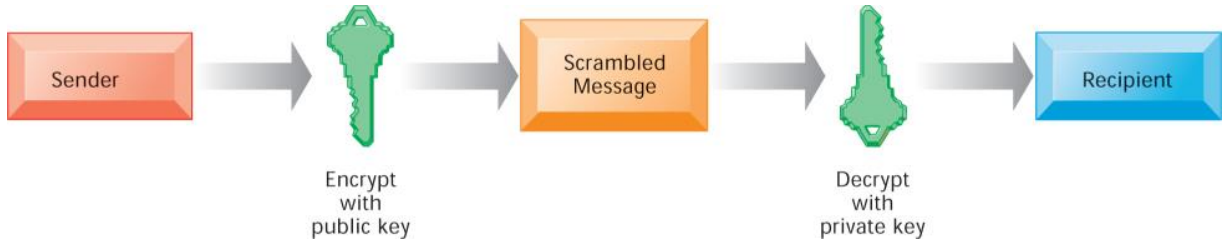
- **WEP security**
  - **Static encryption keys are relatively easy to crack**
  - **Improved if used in conjunction with VPN**
- **WPA2 specification**
  - **Replaces WEP with stronger standards**
  - **Continually changing, longer encryption keys**

Encryption and Public Key Infrastructure (1 of 3)

- **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)

Encryption and Public Key Infrastructure (2 of 3)

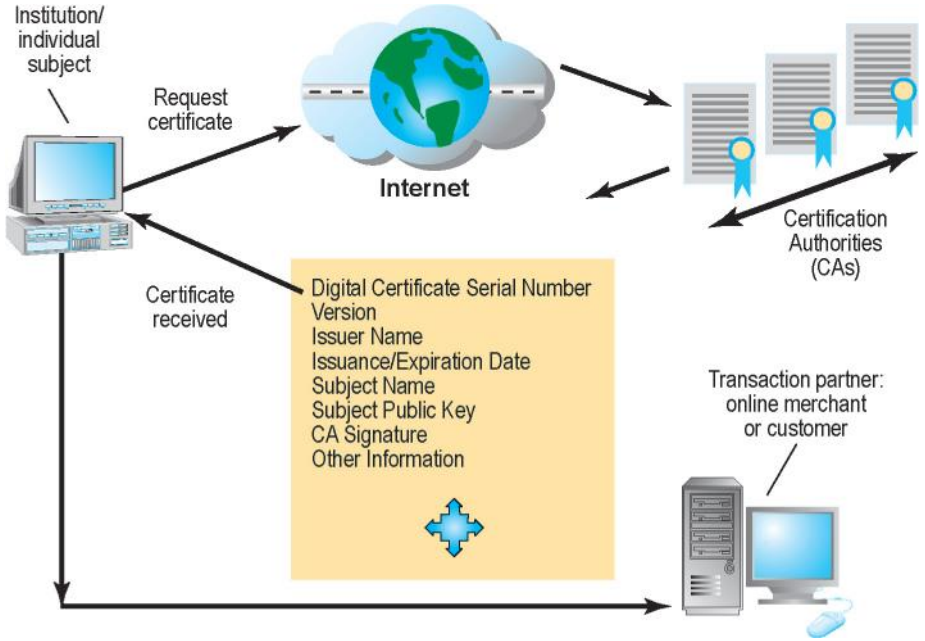
- **Two methods of encryption**
  - **Symmetric key encryption**
    - Sender and receiver use single, shared key
  - **Public key encryption**
    - Uses two, mathematically related keys: public key and private key
    - Sender encrypts message with recipient's public key
    - Recipient decrypts with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



Public Key Encryption

Encryption and Public Key Infrastructure (3 of 3)

- **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

Ensuring System Availability

- **Online transaction processing requires 100% availability**
- **Fault-tolerant computer systems**
  - **Contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service**
- **Deep packet inspection**
- **Security outsourcing**
  - **Managed security service providers (MSSPs)**

Security Issues for Cloud Computing and the Mobile Digital Platform (1 of 2)

- **Security in the cloud**
  - **Responsibility for security resides with company owning the data**
  - **Firms must ensure providers provide 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)**

Security Issues for Cloud Computing and the Mobile Digital Platform (2 of 2)

- **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**

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**

Interactive Session: Technology

BYOD: A Security Nightmare?

Read the Interactive Session and discuss the following questions

- **Class discussion**
  - It has been said that a smartphone is a computer in your hand. Discuss the security implications of this statement.
  - What kinds of security problems do mobile computing devices pose?
  - What management, organizational, and technology issues must be addressed by smartphone security?
  - What steps can individuals and businesses take to make their smartphones more secure?

Part II
Information Technology Infrastructure

Next Steps

- Answer the Moodle quiz
- Prepare for 9th chapter