Major Concepts

- Describe the principles of secure network design.
- Describe the Cisco Self Defending Network.
- Describe the role of operations security in a network.
- Describe the various techniques and tools to use for network security testing.
- Describe the principles of business continuity planning and disaster recovery.
- Describe the SDLC and how to use it to design a Secure Network Life Cycle management process.
- Describe the functions, goals, role, and structure of a comprehensive security policy.
Lesson Objectives

Upon completion of this lesson, the successful participant will be able to:

1. Describe the high-level considerations for ensuring that a network is secure.
2. Describe how to identify threats, risks, and consequences of exploited services.
3. Describe the benefits of risk management and the measures to take to optimize risk management.
4. Describe the CSDN and describe the phases, benefits, and collaborative systems of a CSDN.
5. Describe the Cisco Threat Control Solution and the Cisco Secure Communications Solution.
Lesson Objectives

7. Describe the overarching concepts of operations security.
8. Describe the core principles of operations security.
9. Describe the role of and the techniques used in network security testing.
10. Describe the tools used in network security testing.
11. Describe business continuity planning and disaster recovery.
12. Describe the degrees of disruption to business operations and the types of backup.
13. Describe the SDLC.
14. Describe the 5 phases of the SDLC.
15. Describe the goals of a security policy.
Lesson Objectives

16. Describe the structure of a security policy.
17. Describe the standards, guidelines, and procedures of a security policy.
18. Describe the roles and responsibilities entailed within a security policy.
19. Describe the concepts of security awareness and how to achieve security awareness through education and training.
20. Describe in brief major laws and ethical guidelines for network security.
21. Describe how to respond to a security breach.
Developing Security Policies

- **Business needs:** What does the organization want to do with the network? What are the needs of the organization?
- **Threat identification:** What threats are most likely to occur, given the organization’s purpose and systems?
- **Risk analysis:** What is the cost versus benefit analysis of mitigating, transferring and accepting various security risk?
- **Security needs:** What are the policies, procedures, standards, and guidelines needed to address business needs and risks?
- **Industry-recommended practices:** What are the security practices that similar organizations currently employ?
- **Security operations:** What are the current procedures for system hardening, incident response, monitoring, maintenance, and auditing of the system for compliance?
Risk Management Guidelines

• Expect that any aspect of a security system might fail.
• Identify any elements that fail-open. Fail-open occurs when a failure results in a complete bypass of the security function.
• Try to identify all attack possibilities.
• Evaluate the probability of exploitation. The focus should be on the resources that are needed to create an attack.
• Assume that people will make mistakes.
• Attackers will not use common and well-established techniques to compromise a system.
• Check all assumptions with other people. They might have a fresh perspective on potential threats and their probability.
Identified Threats

- Internal system compromise
- Insider attack on the system
- Stolen customer data
- Phony transactions
- Data Center Destruction
- Data Input errors
Risk Analysis

- Evaluate each threat to determine its severity and probability
- Quantitative Risk Analysis uses a mathematical model
- Qualitative Risk Analysis uses a scenario-based model
Quantitative Risk Analysis

• Asset Value (AV) is the cost of an individual asset.

• Hard Drive Failure Rate .002

• Total Cost of replacement 20K

\[ SLE = AV \times EF \]

• Flood threat

Data entry error

• Exposure Factor is .001 percent
  - AV of data and databases is US$1,000,000
    - SLE is US$1,000,000 * .000001 = US$10

• Exposure Factor is 60 percent
  - AV of the enterprise is US$10,000,000
    - SLE is US$10,000,000 * .60 = US$6,000,000
• **Annualized Rate of Occurrence (ARO)** - estimated frequency that a threat is expected to occur.

  
  **Flood threat**
  
  - SLE is US$6,000,000
  - ARO is .01
  - ALE is US$6,000,000 * .01 = US$60,000

• **Single Loss**

• **Annualized financial loss** - expected financial loss that an organization will cause if an event occurs.

  - SLE is US$10
  - ARO is 125,000
  - ALE is US$10 * 125,000 = US$1,250,000

  \[ \text{ALE} = \text{SLE} \times \text{ARO} \]
Ways to Handle Risk

• **Risk management**—Uses the deployment of protection mechanisms to reduce risks to acceptable levels. Risk management is the most basic and the most difficult aspect of building secure systems, because it requires good knowledge of risks, risk environments, and mitigation methods.

• **Risk avoidance**—Eliminates risk by avoiding the threats altogether, which is usually not an option in the commercial world, where controlled (managed) risk enables profits.
Risk Management Scenario

- **Internal system compromise**—Provide the least amount of privilege access possible to the inside, and utilize a secure multi-tiered application which minimizes inside access.
- **Stolen customer data**—Keep all of the customer data on inside servers, and only transfer data to the outside on demand.
- **Phony transactions if external server is broken into**—Allow only man-in-the-middle attacks on the external server and design the external server application so that it does not allow arbitrary transactions to be called for any customer account.
- **Phony transactions if customer PIN or smart card is stolen**—Use a quick refresh of revocation lists and have a contract with the user which forces the user to assume responsibility for stolen token cards.
• **Insider attack on the system**—Strictly limit inside access to the application and provide strict auditing of all accesses from the inside.

• **Data input error**—enhance the security of database applications and provide redundant checking system in order to reduce data entry errors

• **Data Center destruction**—Ensure backups are kept off campus and that additional equipment is on-hand. Enhance defenses against flooding by raising equipment and other precautions.
Risk Avoidance Scenario

Using the risk avoidance approach, a company would decide not to offer e-banking service at all because it would be deemed too risky.
Introduction to Cisco Self-Defending Network

- Least Privilege Concept
- Cisco Self-Defending Network Principles
- Cisco Self-Defending Network Defined
- Collaborative Systems Enabling Unparalleled Security
• Inside and outside users only need access to the web server program on the exposed host.
  – The web server does not need to open any connections to the inside or outside.
  – The firewall enforces those minimal permissions.
Cisco Self-Defending Network Principles

**Integrated**
Enabling every element to be a point of defense and policy enforcement

**Collaborative**
Collaboration among the services and devices throughout the network to thwart attacks

**Adaptive**
Proactive security technologies that automatically prevent threats
Cisco Self-Defending Network Defined

Efficient security management, control, and response

Advanced technologies and security services that:
- Mitigate the effects of outbreaks
- Protect critical assets
- Ensure privacy

Security as an integral, fundamental network feature

Operational Control and Policy Management

Threat Control and Containment

Secure Communications

Secure Network Platform
Collaborative Systems Enabling Unparalleled Security

- **360° visibility and protection:**
  - Delivering comprehensive and proactive network defense
- **Simplified control:**
  - Streamlining policy and threat management across the network
- **Business resiliency:**
  - Ensuring the enterprise operations
• **Threat control for endpoints**: This element defends against threats most commonly introduced by Internet use, such as viruses, spyware, and other malicious content.

• **Threat control for infrastructure**: This element safeguards the server and application infrastructure against attacks and intrusions. It also defends against internal and external attempts to penetrate or attack servers and information resources through application and operating system vulnerabilities.

• **Threat control for e-mail**: This element protects business productivity, resource availability, and confidential information by stopping e-mail initiated threats.
Benefits to implementing a secure communication structure:

- Improve business productivity and efficiency
- Enable new business applications
- Help comply with information privacy regulations

<table>
<thead>
<tr>
<th>Secure Communications for Remote Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides highly secure, customizable access to corporate networks and applications by establishing an encrypted tunnel across the Internet</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secure Communications for Site-to-Site Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides an Internet-based WAN infrastructure for connecting branch offices, home offices, or the sites of business partners to all or portions of a network</td>
</tr>
</tbody>
</table>
The Cisco Security Management Suite provides a number of benefits:

- Increases speed and accuracy of policy deployment
- Improves visibility to monitor end-to-end security
- Provides more rapid response to threats
- Enforces corporate policy compliance
- Enhances proper workflow management
Cisco Security Manager

- Responds faster to threats by allowing an administrator to define and assign new security policies
- Provide flexible methods to manage devices and policies
- Contains extensive animated help for the new user
- Allows an administrator to centrally specify which policies are shared and inherited
- It integrates with Cisco Security MARS to correlate events with the associated firewall rules
- It provides the ability to assign specific tasks to each administrator during the deployment of a policy
Cisco Security MARS

- Greatly reduces false positives
- Defines the most effective mitigation responses
- Promotes awareness of environmental anomalies
- Provides quick and easy access to audit compliance reports
- Makes precise recommendations for threat removal,
Secure Network Platform
Security Services Integrated into the Network

Integrate Advanced Services

Advanced Technologies and Services

- Automated Threat Response
- Virtualized Security Services
- Behavioral-Based Protection
- Endpoint Posture Control
- Dynamic DDoS Mitigation
- Endpoint and Application-Layer Inspection

Integrate Advanced Security Services Where Needed

IPsec and SSL

Security Point Products
- IPS
- Firewall
- Access Control

IP Network
- IPS
- Firewall
- Access Control

Network Antivirus
- IPsec and SSL VPN

© 2009 Cisco Learning Institute.
Operations Security

- Cisco Self-Defending Network design provides products that can deploy independently of one another.
- All networks will be vulnerable to attack if the planning, implementation, operations, and maintenance of the network do not adhere to operational security practices.
- Operations security starts with the planning and implementation process of a network.
Core Principles

- Separation of duties: two-man control and dual operator
- Rotation of duties
- Trusted recovery: failure preparation and system recovery
- Change and configuration controls
Separation of Duties
Rotation of Duties

- Technical support: Week 1
- Data Center Support: Week 2
- Data Entry: Week 3
Practices:

- A junior staff member is responsible for loading blank media.
- Backup software uses an account that is unknown to individuals to bypass file security.
- A different staff member removes the backup media and securely stores it on site while being assisted by another member of the staff.
- A separate copy of the backup is stored off site and is handled by a third staff member who is accompanied by another staff member.
There are five steps in a change control process:

1. Apply to introduce the change.
2. Catalogue the proposed change.
3. Schedule the change.
4. Implement the change.
5. Report the change to relevant parties.
Objectives of Security Testing and Evaluation

**Objectives of ST&E:**

- Uncover design, implementation, and operational flaws that could lead to the violation of the security policy.

- Determine the adequacy of security mechanisms, assurances, and device properties to enforce the security policy.

- Assess the degree of consistency between the system documentation and its implementation.
Assessing the Operational Status

- Network scanning
- Vulnerability scanning
- Password cracking
- Log review
- Integrity checkers
- Virus detection
- War dialing
- War driving (802.11 or wireless LAN testing)
- Penetration testing
Using Testing Results

• As a reference point for corrective action
• To define mitigation activities to address identified vulnerabilities
• As a benchmark to trace the progress of an organization in meeting security requirements
• To assess the implementation status of system security requirements
• To conduct cost and benefit analysis for improvements to system security
• To enhance other activities such as risk assessments, Certification and Authorization (C&A), and performance improvement efforts
Security Testing Tools

- Nmap: – discovers computers and services on a computer network, thus creating a map of the network.
- GFI LANguard: network and security scanner which detects vulnerabilities.
- Tripwire: assesses and validates IT configurations against internal policies, compliance standards, and security best practices.
- Nessus: vulnerability scanning software, focusing on remote access, misconfiguration passwords, and DoS against the TCP/IP stack.
- L0phtcrack: password auditing and recovery application.
- Metasploit: provides information about vulnerabilities and aids in penetration testing and IDS signature development.
- SuperScan: port scanning software designed to detect open TCP and UDP ports and what services are running on those ports.
Basic functionality

- Classic TCP and UDP port scanning
- Classic TCP and UDP port sweeping
- Stealth TCP and UDP port scans and sweeps
- Remote operating system identification, known as OS fingerprinting.
• Improved host detection using multiple ICMP methods
• TCP SYN scanning
• UDP scanning (two methods)
• Source port scanning
• Fast hostname resolving
• Extensive banner grabbing
• IP and port scan order randomization
• Extensive Windows host enumeration capability
• Moving or relocating critical business components and people to a remote location while the original location is being repaired
• Utilizing different channels of communication to deal with customers, shareholders, and partners until operations return to normal
Disaster Recovery

- The process of regaining access to the data, hardware, and software necessary to resume critical business operations after a disaster.

- Plan for coping with unexpected or sudden loss of key personnel.
Disruptions

- Identify types of disasters or disruptions possible
- Take into account the magnitude of the disruption
Backups

- **Redundancy**
  - Replacement components owned by the organization or a server provider
  - Service level agreement (SLA)

- **Redundant facility**
  - Hot Site
  - Warm Site
  - Cold Site
Security categorization: This task defines three levels of potential impact on organizations or individuals should there be a breach of security: low, moderate, and high,. Security categorization standards help organizations make the appropriate selection of security controls for their information systems.

Preliminary risk assessment: This task results in an initial description of the basic security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.
Risk assessment: an analysis that identifies the protection requirements for the system through a formal risk assessment process.

Security functional requirements: an analysis of requirements

Security assurance requirements: an analysis of the requirements that address the developmental activities that are required and the assurance evidence that is needed to produce the desired level of confidence

Security cost considerations and reporting: determines how much of the development cost to attribute to information security

Security planning: new and current agreed upon security controls should be fully documented.

Security control development: ensures that the security controls that the respective security plans describe are designed, developed, and implemented.

Developmental security test and evaluation: ensures that security controls that are developed for a new information system are working properly and are effective.
**Implementation**

**Inspection and acceptance:** ensures that the organization validates and verifies that the functionality that the specification describes is included in the deliverables.

**System integration:** ensures that the system is integrated at the operational site where the information system is deployed for operation.

**Security certification:** ensures that one effectively implements the controls through established verification techniques and procedures.

**Security accreditation:** provides the necessary security authorization of an information system to process, store, or transmit information that is required.
Configuration management and control: ensures that there is adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment.

Continuous monitoring: ensures that controls continue to be effective in their application through periodic testing and evaluation.
Information preservation: ensures that information is retained, as necessary, to conform to current legal requirements and to accommodate future technology changes that can render the retrieval method obsolete.

Media sanitization: ensures that data is deleted, erased, and written over, as necessary.

Hardware and software disposal: ensures that hardware and software is disposed of as directed by the information system security officer.
Determining an Organization’s Assets

Ask the following questions:

- What does the organization have that others want?
- What processes, data, or information systems are critical to the organization?
- What would stop the organization from doing business or fulfilling its mission?

Security Policies are designed to protect assets
Security Policy Benefits

• Demonstrates an organization’s commitment to security.

• Sets the rules for expected behavior.

• Ensures consistency in system operations, software and hardware acquisition and use, and maintenance.

• Defines the legal consequences of violations.

• Gives security staff the backing of management.
Anyone with access to the network
  - Internal audience
  - External audience

Determines the content of the policy
Hierarchy of Policies

- Governing Policy
  - Technical Policies
  - End-User Policies
Important components:

• A statement of the issue that the policy addresses.

• How the policy applies in the environment.

• The roles and responsibilities of those affected by the policy.

• The actions, activities, and processes that are allowed and those that are not.

• The consequences of noncompliance.
Technical Policies

• General policies
• E-mail policies
• Remote access policies
• Telephony policy
• Application policies
• Network policies
• Wireless communication policy
End User Policy

• Cover all rules pertaining to information security that end users should know about, comply with, and implement.

• May overlap with technical policies.
Standards, Guidelines, and Procedures

- The security policy documents are high-level overview documents.
- Standards, guidelines, and procedures contain the actual details defined in the policies.
- Each document serves a different function, covers different specifications and targets a different audience.
Standards documents include the technologies that are required for specific uses, hardware and software versioning requirements, program requirements, and any other organizational criteria.
Guideline Documents

- Provide a list of suggestions
- Provide flexibility
- Not usually mandatory
- Sources:
  - National Institute of Standards and Technology (NIST) Computer Security Resource Center
  - National Security Agency (NSA) Security Configuration Guides
  - The Common Criteria standard
Procedure Documents

Procedure documents include the details of implementation, usually with step-by-step instructions and graphics
Executive-level management must always be consulted during security policy creation in order to ensure the policy is comprehensive, cohesive, and legally binding.
• Chief Technology Officer (CTO)—Identifies and evaluates new technologies and drives new technology development. Maintains and enhances current enterprise systems.

• Chief Information Officer (CIO)—Responsible for the information technology and computer systems that support enterprise goals, to include successful deployment of new technologies and work processes.

• Chief Security Officer (CSO)—Develops, implements and manages the organization’s security strategy, programs, and processes associated with all aspects of business operation including intellectual property.

• Chief Information Security Officer (CISO)—Develops and implements security policy.
Security Awareness Program

- Reflects the business needs of an organization
- Informs users of their IT security responsibilities
- Explains all IT security policy and procedures
- Explains proper rules of behavior for the use of the IT systems and data
- Details sanctions for noncompliance
- Components
  - Awareness campaigns
  - Training and education
Awareness

Methods for increasing awareness:

- Lectures, videos
- Posters, newsletter articles, and bulletins
- Awards for good security practices
- Reminders such as login banners, mouse pads, coffee cups, and notepads
From: IT department
To: all Employees
Subject: Course Offerings

We are currently offering several training opportunities. Please see the list below and contact your manager if interested.

- **Computer Security.** This one-hour mandatory session is presented during orientation week and details user account security and password guidelines, network security and bandwidth guidelines, early recognition of potential virus attacks and phishing attacks, and protection from identity theft.

- **Networking.** Four classes are devoted to Carnegie Mellon–specific networking information: Introduction to Andrew File Space, MyFiles, UNIX, and FTP.

- **Responsible Computing.** Bandwidth, academic integrity, and copyright guidelines are covered in this session. It includes a section that explains safe and secure use of social networking sites such as Facebook. We present recorded case scenarios, review related policies and guidelines, and facilitate discussions to enhance the comprehension of students’ responsibilities.
A successfully implemented security awareness program measurably reduces unauthorized actions by insiders, increases the effectiveness of existing controls, and helps fight waste, fraud, and abuse of information systems resources.
Laws and Ethics

- Types of Laws
  - Criminal
  - Civil
  - Administrative

- Ethics
  - Computer Ethics Institute
  - Internet Activities Board (IAB)
  - Generally Accepted System Security Principles (GASSP)
  - International Information Systems Security Certification Consortium, Inc (ISC)² Code of Ethics
The ISC2 Code of Ethics

• Code of Ethics Preamble

   Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior. Therefore, strict adherence to this Code is a condition of certification.

• Code of Ethics Canons

   - Protect society, the commonwealth, and the infrastructure.
   - Act honorably, honestly, justly, responsibly, and legally.
   - Provide diligent and competent service to principals.
   - Advance and protect the profession.
Motive answers the question of why a person (or persons) committed the illegal act.

Opportunity answers the question of when and where the person committed the crime.

Means answers the question of how the person committed the crime.
Forensics Procedures

- Proper data collection
- Data chain of custody
- Data storage
- Data backups