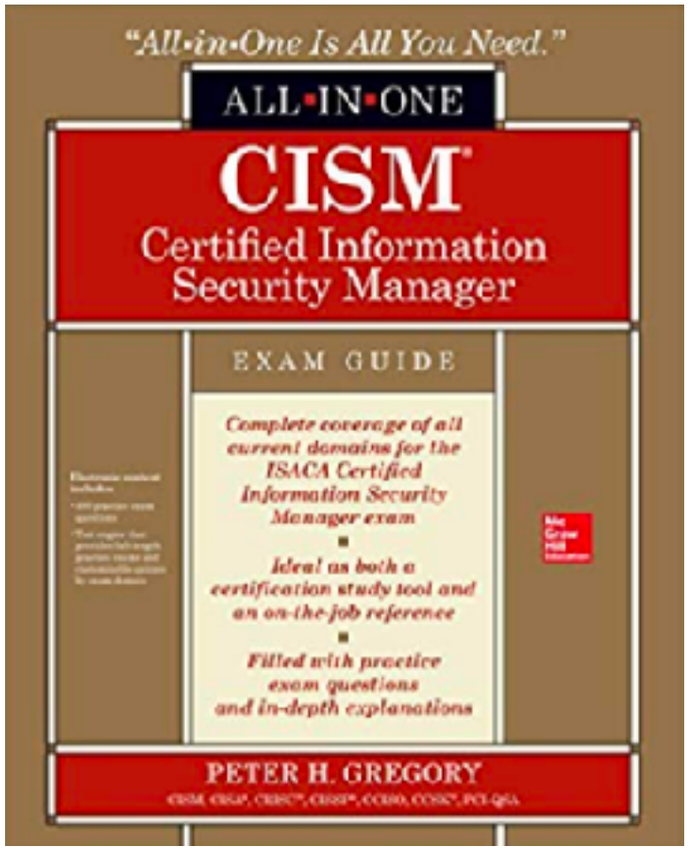
CNIT 160: Cybersecurity Responsibilities

4. Information Security Program Development and Management Part 5

Pages 275-296



Topics
in this Lecture

- **Security Program Operations**
  - **Secure Engineering and Development**
  - **Network Protection (p. 277)**
  - **Endpoint Protection and Management (p. 288)**
  - **Identity and Access Management (p. 292)**

Chapter Topics
For Later Lectures

- **Security Program Operations**
  - **Security Incident Management (p. 296)**
  - **Security Awareness Training**
  - **Managed Security Services Providers**
  - **Data Security (p. 302)**
  - **Business Continuity Planning**

Chapter Topics
For Later Lectures

- **IT Service Management (p. 322)**
- **Controls**
- **Metrics and Monitoring**
- **Continuous Improvement**

Security Program Operations

Secure Engineering and Development

Role of Security Management

- **For decades, IT organizations employed no security personnel**
- **Did not include security in design, engineering, or development**
- **Now security should be invoved as early as possible in development life cycle**

Security in the Development Cycle

- **Consider data protection, regulations, compliance, privacy and risk in each stage**
  - **Conceptual**
  - **Requirements**
  - **Design**
  - **Engineering and Development**
  - **Testing**

Computer Science Programs

- **None of the top ten require any security class at all**
- **Many programs don't offer a single security class as an option**

Network Protection Topics

- **Firewalls**
- **Application firewalls**
- **Intrusion prevention systems**
- **Network anomaly detection**
- **Packet sniffers**

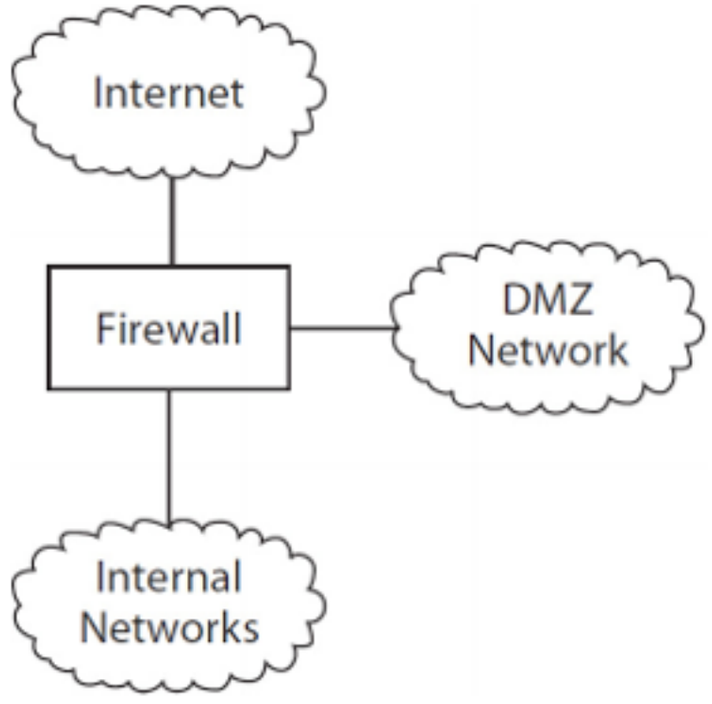
Network Protection Topics (continued)

- **Wireless network protection**
- **Web content filters**
- **Cloud access security broker**
- **DNS filter**
- **E-mail protection**
- **Network access control'**

Firewalls

Firewalls

- **Protect a network from harmful traffic**
- **A DMZ (demilitarized zone) is a semi-trusted network**
- **For public servers**
- **Like Web and E-mail servers**



Firewall Rules

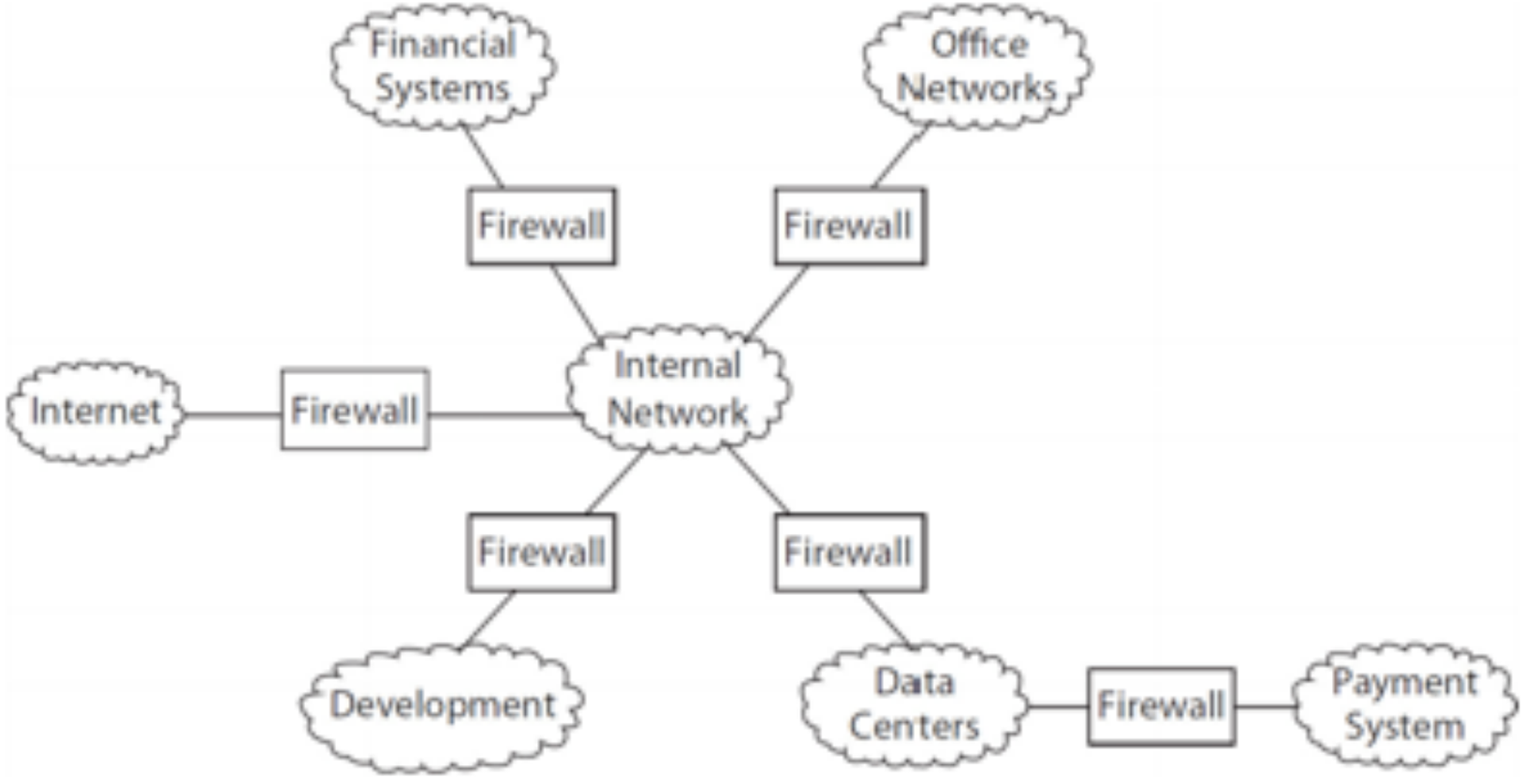
Source IP Address	Source Port	Destination IP Address	Destination Port	Permit or Deny
0.0.0.0 to 255.255.255.255	25	141.204.10.22	25	Permit
0.0.0.0 to 255.255.255.255	53	141.204.10.24	53	Permit
141.204.10.24	53	0.0.0.0 to 255.255.255.255	53	Permit
0.0.0.0 to 255.255.255.255	119	141.204.10.22	119	Permit
141.204.12.1 to 141.204.12.255	80, 443	0.0.0.0 to 255.255.255.255	80, 443	
0.0.0.0 to 255.255.255.255	0 to 65535	141.204.10.1 to 141.204.10.255 + 141.204.12.1 to 141.204.12.255	0–65535	Deny

Application firewalls

- **Control traffic to an application server**
  - **Usually a web server**
  - **Block attacks like SQL injection**

Segmentation

- **Partitioning a network into zones**
- **Layers of security: defense in depth**

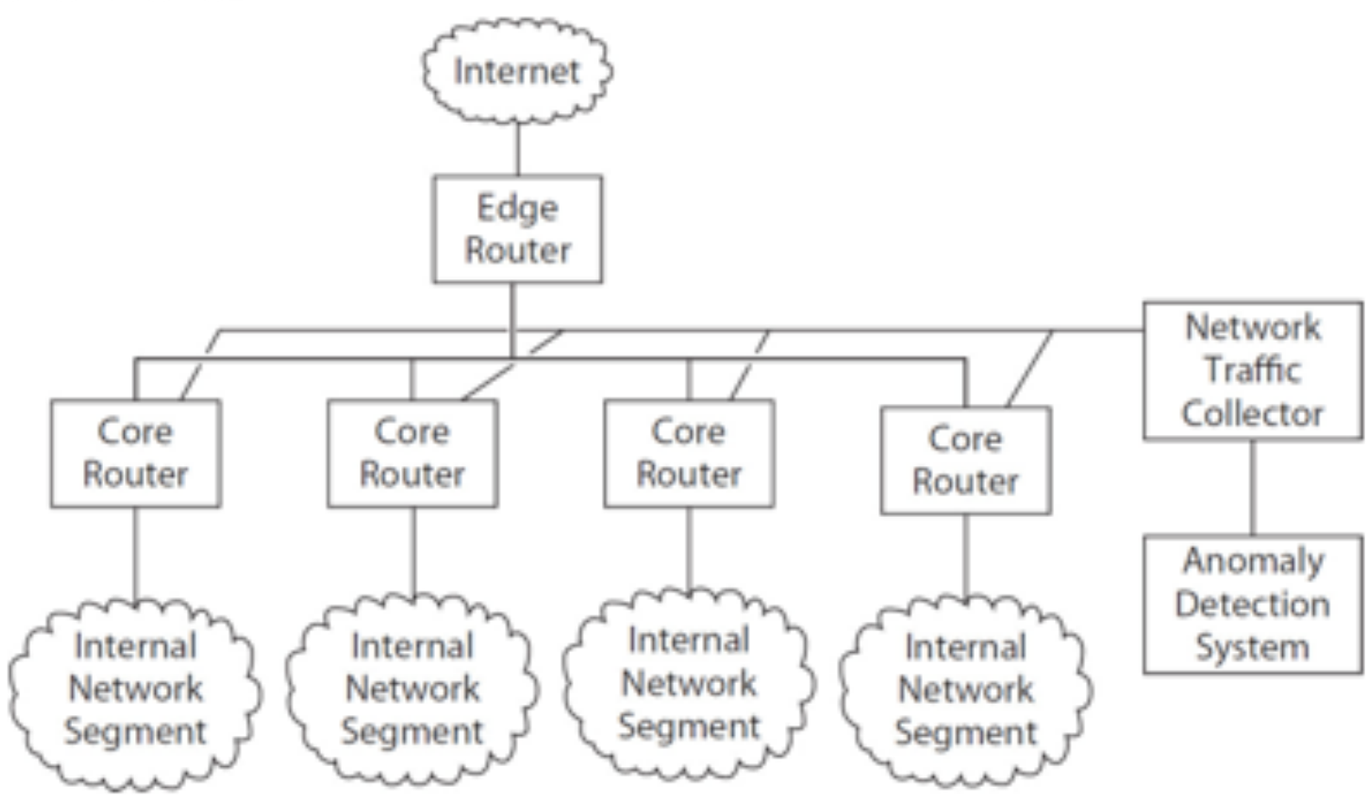


Intrusion Prevention Systems

- **Block malicious traffic**
- **By recognizing packet contents, or**
  - **Known malicious IP addresses and domains**
  - **Include feeds of malicious data**
  - ***Threat intel feed***
- **Require vigilance**
  - **May block useful traffic**

Network Anomaly Detection

- **Learns what normal traffic is like**
- **Alerts when unusual patterns of traffic flow are detected**



Network Anomaly Standards

- **Netflow from Cisco**
- **sFlow**
- **Remote Monitoring (RMON)**
  - **An earlier protocol**

Network Taps and Span Ports

- Devices that send a copy of all packets
  - to a monitoring system

Packet Sniffers

- **Allow an analyst to see all traffic at a point**
- **Helpful filtering and packet dissection features**
- **Wireshark is the leading tool**

Wireless Network Protection

- **WEP is old and vulnerable**
- **WPA and WPA2 are much better**
- **Rogue access points**
  - **Often set up by employees**
  - **Not secure enough to satisfy security policy**
- **A common attack point**

Web Content Filters

- **Block malicious sites**
  - **Preventing employees from using them**
- **Block categories**
  - **Games, porn, social networks, etc.**
- **Inline device only works on company network**
- **Software agent on endpoint works in every location**

Cloud Access Security Broker (CASB)

- **Monitors and controls access to Internet sites**
  - **Example: your company uses Box, so it blocks Dropbox**
- **Resembles web content filter**

DNS Filter

- **Block content by manipulating DNS queries and responses**
- **Prevents access to known malicious sites and other unwanted content**
- **Works on all DNS-based traffic, not just web browsing**

E-mail Protection

- **Over 90% of successful network intrusions**
  - **Begin with phishing messages**
- **CEO fraud targets executives**
- **May carry ransomware**

Spam and Phishing Filters

- **Use *rules***
- ***Quarantine* blocked e-mails**
  - **User can view and release them**
- ***White lists* and *black lists***

Types of Phishing

- **Clone phishing**
  - **Copying a legitimate email and modifying it**
- **Phishing**
- **Smishing (over SMS)**
- **Spear phishing**
  - **Specially crafted to target**
- **Spim (via instant messaging)**
- **Whaling**
  - **Targeting CEO or other key executive**

Phishing Testing

- **Sending fake phishing messages to test employee's awareness**
  - **Useful measure of vulnerability**

Network Access Control

- **Only allow certain devices to connect**
    - **Only company-issued devices**
    - **Only devices with up-to-date security patches**
    - **Only devices with up-to-date anti-malware software**
    - **Only devices with specific security settings**
    - **Only devices associated with authorized users**

Ch 4b

Endpoint Protection and Management

Endpoint

- **Smartphone**
- **Tablet**
- **Laptop**
- **Desktop computer**

Reasons Attackers Target Endpoints

- **Often contain sensitive information**
- **Easily lost or stolen**
- **Often lack up-to-date anti-malware protection**
- **Permitted to access internal company networks**

Reasons Attackers Target Endpoints (continued)

- **Users often open phishing attachments**
- **May lack current security patches**
- **Users may have local administrator privileges**
- **May be powerful devices on fast networks**
  - **Useful for sending spam or DDoS attacks**

Configuration Management

- **Image management**
  - **Binary representation of a fully installed and configured endpoint computer**
- **Configuration management**
  - **Automated tools to deploy patches, change configuration settings, and install and remove software**

Configuration Management (continued)

- **Remote control**
  - **For assistance, troubleshooting, and more**
- **Remote destruction (wipe)**
- **Data encryption**
  - **Full-disk encryption**
  - **Protects data stored on a mobile device from a thief**

Configuration Standards

- **Documents that detail the operational and security configuration for endpoints**
- **May also have a *hardening document***

Malware Prevention

Types of Malware

- **Virus**
  - **Attaches to EXE files (old, not common now)**
- **Trojan**
  - **Deceives the user, pretending to be something harmless like a game**
- **Macro**
  - **Program within an document**
  - **Usually MS Office (Excel, Word, etc.)**

Types of Malware (continued)

- **Rootkit**
  - **Hidden within the operating system**
  - **Difficult to detect and remove**
- **Fileless**
  - **Memory-resident**
  - **Difficult for antivirus to detect**
- **Ransomware**
  - **Encrypts files and demands payment**

Types of Malware (continued)

- **Destructware**
  - **Wipes or encrypts files to destroy them**
- **Remote Access Trojan (RAT)**
- **Keylogger**

Anti-Malware Techniques

- **Signatures**
  - **Matches known byte patterns**
- **Process observation**
  - **Detects suspicious behavior**
- **Sandbox**
  - **Runs files in a virtual system to detect malicious behevior**

Deception

- **Scrambles the memory map to block malware attacks**

ACALVIO

PARTNERS COMPANY SCHEDULE A DEMO

Introducing Acalvio ShadowPlex Ransomware Protection

Acalvio ShadowPlex offers an innovative anti-ransomware solution that leverages deception technology and AI to **detect and respond to any ransomware variant, including all the known strains, as well as unknown or zero-day ransomware variants**. ShadowPlex can consistently and reliably detect every ransomware strain, including **Maze**, **WastedLocker**, **REVil**, **Ryuk**, **NetWalker**, **Ragnar Locker**, and **Netfilm** within seconds.

If you're concerned about the ransomware threat to your organization, visit us here for more information or see it for yourself and schedule a demo to see ShadowPlex work every time against these threats

The Death ot AV

- **Traditional antivirus software using signatures is much less effective now**
- **Malware can use *packing* to change the signatures**

Virtual Desktop Infrastructure (VDI)

- **Users connect to a desktop operating system in the cloud**
  - **Such as Azure**
- **All processing and data reside in the cloud**
- **Far smaller *attack surface***

Enterprise Anti-Malware

- **Centralized console**
  - **Allows engineers to observe and manage anti-malware running on thousands of endpoints**
  - **Can run scans, reinstall anti-malware, change configurations**
- **Can send alerts to SIEM systems or SOC personnel when malware is detected**

End-User Administrator Rights

- **Most users ran Windows XP as Administrator all the time**
- **Microsoft's User Account Control is a safer system**
  - **User has limited privileges**
  - **Only escalates briefly to administrator when installing software**

Security Program Operations

Identity and Access Management

Credentials

- **In the past, when organizations had few business applications**
  - **Users had separate credentials for each app**
- **But as more apps were used, like cloud services**
  - **Users had to remember too many passwords**
  - **So they'd re-use passwords, or store them insecurely**
  - **And there were many password resets to manage**

Central Identity and Access Management

- ***Reduced sign on* or *single sign-on***
  - **Employees only need one password**
  - **Easily locked out when an employee leaves**
- **But that makes the password a high-value theft target**
- **Solution: Multifactor authentication**

Access Operations

- **Provisioning access to new workers**
- **Adjusting access rights to workers being transferred**
- **Assisting workers with access issues such as forgotten passwords**
- **Assisting workers whose accounts have been locked out for various reasons**
- **Removing access from departing workers**

Less Routine Events

- **Integrating a new business application with a centralized authentication service**
- **Resetting a user's credentials in response to the loss of a laptop computer or mobile device**

Access Governance

- **Ensuring that user accounts conform to policy**
  - **Access Reviews**
  - **Segregation of Duties**
  - **Priviliged Account Audits**
  - **Activity Reviews**
  - **Access Recertification**
  - **User Behavior Analytics**

Access Reviews

- **Comfirm that all workers who need access have it**
  - **And that others do not**
- **Required by some regulations**

Accumulation of Privileges

- **Long-term employees move from one position to another**
  - **And may keep access from old role**
- **Difficult to prevent**
  - **User may still be working with the previous department**

Segregation of Duties

- **A single individual cannot perform a high-risk action**
  - **A second person must also take action**
- **Example: create a vendor, request payment, approve payment**
  - **Must be handled by different people**

Segregation of Duties Access Review

- **Examine user rights to high-risk and high-value roles**
- **Make sure no one person has two roles in the same function**
- **If there are not enough personnel for true segregation of duties**
  - **Make reviews more frequent to compensate**

Priviliged Account Audits

- **Audit the personnel approved for high privileges**
  - **Like Administrator or Domain Admin**
- **Limit the roles to the smallest number of people possible**

Activity Reviews

- **Which users are active?**
- **Identify accounts that have been inactive for a long time (such as 90 days)**
- **Remove or lock them**
- **This helps to reduce *accumulation of privilege***

Access Recertification

- **List users and roles**
- **Determine whether access is still required**
- **This helps to reduce *accumulation of privilege***

User Behavior Analytics

- **User activities are baselines**
- **Anomalous activity triggers events or alarms**
- **May indicate unauthorized activity by users**
- **Or compromised accounts**

Ch 4b