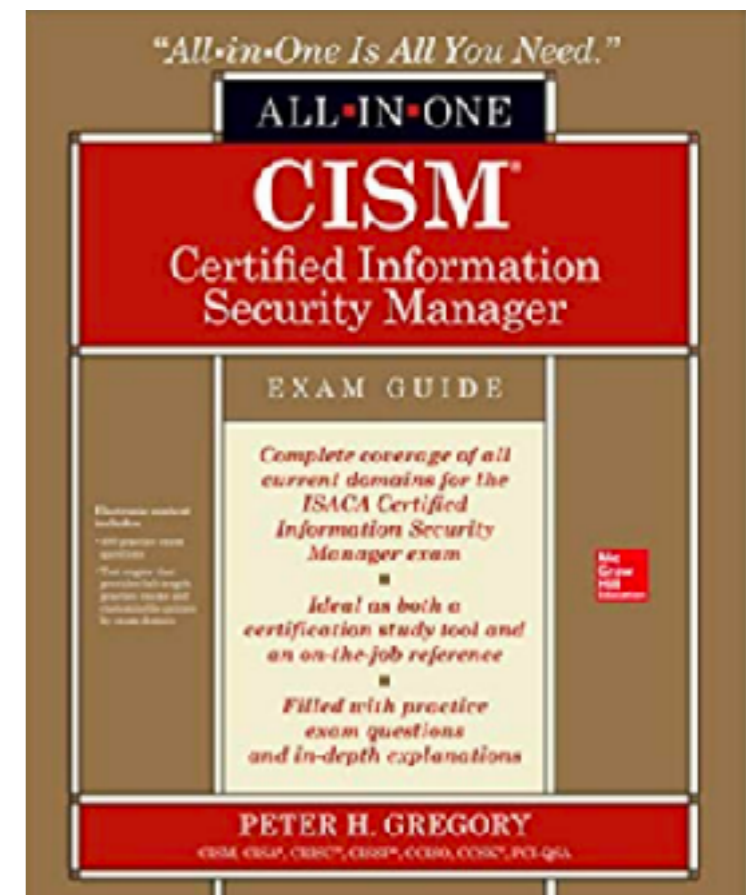


# CNIT 160: Cybersecurity Responsibilities

## 3. Information Risk Management Part 3

Pages 125 - 158



# Topics

- **Part 1 (p. 102 - 115)**
  - **Risk Management Concepts**
  - **Implementing a Risk Management Program**
- **Part 2 (p. 114 - 125)**
  - **The Risk Management Life Cycle**
- **Part 3 (p. 125 - 158)**
  - **The Risk Management Life Cycle**
- **Part 4 (p. 158 - 182)**
  - **Operational Risk Management**

# **Asset Identification and Valuation**

# Assets

- **Hardware assets**
  - **Servers, network hardware, workstations, printers, etc.**
  - **May include assets in storage and replacement components, depending on scope**
  - **Often poorly inventoried and maintained**
  - **Often omits applications**

# Asset Tracking Software

- **Security scan, patch management, and asset inventory systems may help**
  - **But they are often poorly maintained**

# Asset Characteristics

- **Identification (model, serial number)**
- **Value (consider depreciation)**
- **Location**
- **Security classification**
- **Asset group**
- **Owner**
- **Custodian**

# Physical Inventory

- **Verify the information in the asset inventory**
- **Assets may be moved or retired**
- **Missing assets may have been moved without authorization or stolen**

# Subsystem and Software Assets

- **Information Assets**
  - **Customer information**
  - **Intellectual property**
  - **Business operations**
- **Virtual assets**
  - **Leased, not owned**
  - **But they have a replacement cost**



# Cloud-Based Information Assets

- **Company information assets held by another company**
- **Often overlooked**
- **Unless you use a cloud access security broker**

# Virtual Assets

- **Can be deployed without involving other stakeholders**
  - **Such as purchasing**
- **Subject to *virtual sprawl***
- **Sometimes automatically generated via *elasticity***
- **Software-Defined Networking (SDN)**
  - **Facilitates creation of virtual networking devices**

# **Asset Classification**

# Asset Classification

- **Assigns assets to categories**
  - **Representing usage or risk**
- **Determines *criticality***
- **Criticality includes:**
  - **Information sensitivity (such as customer information)**
  - **Operational dependency**

# Resources

- **Criticality forms the basis for**
  - **Information Protection**
  - **Redundancy**
  - **Business continuity planning**
  - **Access management**

# Best Approach

- **First identify and classify *information assets***
  - **Then classify systems**
- **Often overlooked:**
  - **Unstructured data**
  - **Data residing outside organization's approved systems**

# Information Classification

- **Analyzed for value, criticality, integrity, and sensitivity**
- **Examples:**
  - **Monetary value**
  - **Operational criticality**
  - **Accuracy or integrity**
    - **Data that must be highly accurate**
    - **Such as price lists**
  - **Sensitivity (like PII)**

# Classification Levels

- **Secret** Merger and acquisition plans, user and system account password, and encryption keys
  - **Restricted** Credit card numbers, bank account numbers, Social Security numbers, detailed financial records, detailed system configuration, and vulnerability scan reports
  - **Confidential** System documentation, end-user documentation, internal memos, and network diagrams
  - **Public** Marketing collateral, published financial reports, and press releases
-



# Information Handling

	<b>Secret</b>	<b>Restricted</b>	<b>Confidential</b>	<b>Public</b>
<b>Example Information Types</b>	Passwords; merger and acquisition plans and terms	Credit card numbers; bank account numbers; Social Security numbers; detailed financial records; detailed system configuration; vulnerability scan reports	System documentation; end-user documentation; internal memos; network diagrams	Brochures; press releases
<b>Storage on Server</b>	Must be encrypted; store only on servers labeled sensitive	Must be encrypted	Access controls required	Access controls required for update
<b>Storage on Mobile Device</b>	Must never be stored on mobile device	Must be encrypted	Access controls required	No restrictions
<b>Storage in the Cloud</b>	Must never be stored in the cloud	Must be encrypted	Access controls required	Access controls required for update
<b>E-mail</b>	Must never be e-mailed	Must be encrypted	Authorized recipients only	No restrictions

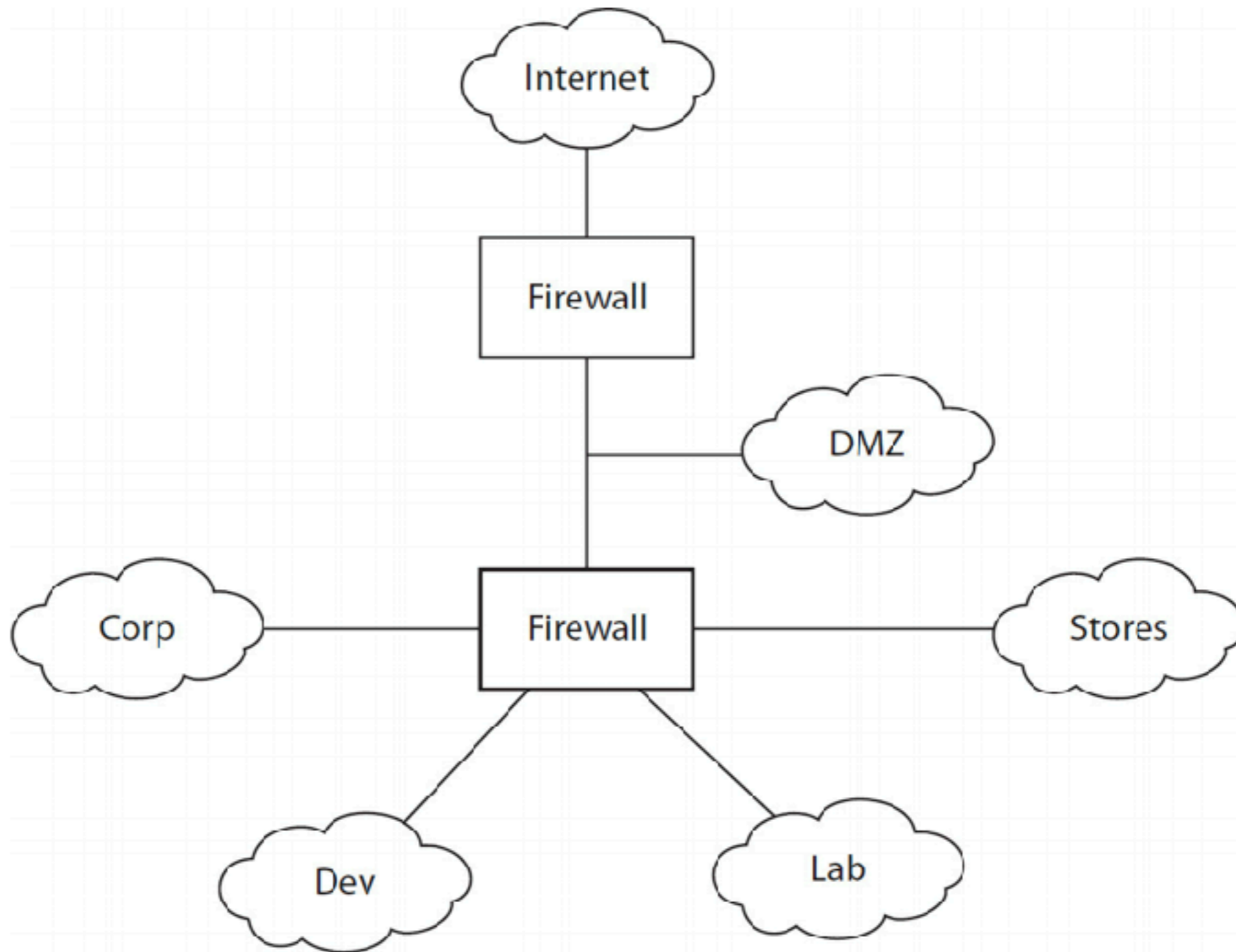
# Information Handling

<b>Website</b>	Must never be stored on any web server	Must be encrypted	Access controls required	No restrictions
<b>Fax</b>	Encrypted, manned fax only	Manned fax only; no e-mail-based fax	Manned fax only	No restrictions
<b>Courier and Shipment</b>	Double wrapped; signature and secure storage required	Signature and secure storage required	Signature required	No restrictions
<b>Hard-Copy Storage</b>	Double locked in authorized locations only	Double locked	Locked	No restrictions
<b>Hard-Copy Distribution</b>	Only with owner permission; must be registered	To authorized parties only; only with owner permission	To authorized parties only	No restrictions
<b>Hard-Copy Destruction</b>	Cross-cut shred; make specific record of destruction	Cross-cut shred	Cross-cut shred or secure waste bin	No restrictions
<b>Soft-Copy Destruction</b>	Erase with DoD 5220.22-M spec tool	Erase with DoD 5220.22-M spec tool	Delete and empty recycle bin	No restriction

# System Classification

- **Database management server**
- **Demilitarized zone firewall**
- **Internet time server**
  
- **Facilities can also be classified**

# Network Segmentation



# **Asset Valuation**

# Qualitative Asset Valuation

- **Rate from 1 to 10**
- **Determines which assets are more valuable than others**

# Quantitative Asset Valuation

- **Replacement cost**
- **Book value**
- **Net present value (revenue generation)**
- **Redeployment cost (virtual machines)**
- **Creation or reacquisition cost**
- **Consequent financial cost**
  - **Cost of a breach**

# Kahoot!

**Ch 3c-1**



# Threat Identification

# Threat Identification

- **Internal**
- **External**
- **Advanced Persistent Threats (APTs)**
- **Emerging Threats**

# Sources of Threat Intelligence

- **ISO/IEC 27005's Appendix C, "Examples of Typical Threats"**
  - **NIST Special Publication 800-30's Appendix E, "Threat Events"**
-

# Internal Threats

- **Well-meaning personnel making errors in judgment**
- **Well-meaning personnel making errors in haste**
- **Well-meaning personnel making errors because of insufficient knowledge or training**
- **Well-meaning personnel being tricked into doing something harmful**
- **Disgruntled personnel being purposefully negligent**
- **Disgruntled personnel deliberately bringing harm to an asset**
- **A trusted individual in a trusted third-party organization doing any of these**

# Rogue Employees


- **A network manager in San Francisco who locked all other network personnel out of the network on the claim that no others were competent enough to manage it**
- **A securities trader at a UK-based brokerage firm who bankrupted the firm through a series of large unauthorized trades**
- **A systems administrator at an intelligence agency who acquired and leaked thousands of classified documents to the media**

# Man-Made Threats

- **Leaked data by email, USB, etc.**
- **Eavesdropping**
- **DoS attack**
- **Fire**

The Washington Post  
*Democracy Dies in Darkness*

## The butt-dial heard round the world



Rudy, no! (Getty Images) (Elsa/Photographer./Getty Images)

By **Alexandra Petri**  
Columnist

Oct. 25, 2019 at 3:55 p.m. PDT

Home  
Share  
945

# Natural Threats

- **Earthquake**
- **Forest fire**
- **Solar flares**

# External Threats

---

## External Threat Actors

Former employees

Current and former consultants

Current and former contractors

Competitors

Hacktivists

Personnel in current and former third-party service organizations, vendors, and suppliers

Government intelligence agencies (foreign and domestic)

Criminal organizations (including individuals)

Terrorist groups (including individuals)

Activist groups (including individuals)

Armed forces (including individuals)

---



# Motivations

---

## **Threat Actor Motivations**

Competitive advantage

Economic espionage

Monetary gain

Political gain

Intelligence

Revenge

Ego

Curiosity

Unintentional errors

---

# APT's

- **Nation-state espionage**
- **Work slowly and carefully**
- **Establish persistent concealed foothold**
- **Exfiltrate data over a long period of time**

# Emerging Threats

- **New techniques**

Phenomenon	Response
Emerging technologies, including bring your own device (BYOD), cloud computing, virtualization, and Internet of Things (IoT)	New targets of opportunity, many of which are poorly guarded when first implemented
Improved technologies (faster processing time)	More rapid compromise of cryptosystems
Improved technologies (faster network speeds)	More rapid exfiltration of larger data sets; easier transport of rainbow tables used to crack hash tables
Improved anti-malware controls	Attack innovation—techniques evaded anti-malware controls

# Vulnerability Identification

- **Configuration fault**
- **Design fault**
- **Known unpatched weakness**
- **Undisclosed unpatched weakness**
- **Undiscovered weakness**
- **Third-party vulnerabilities**
  - **In cloud services**

# Risk Identification

- **Threats**
- **Threat actors**
- **Vulnerabilities**
- **Asset value**
- **Impact**

# Risk, Likelihood, and Impact

*Risk = threats × vulnerabilities*

*Risk = threats × vulnerabilities × asset value*

*Risk = threats × vulnerabilities × probabilities*

---

# Likelihood

- **Hygiene**
- **Visibility**
- **Velocity (warning or foreknowledge)**
- **Motivation**
- **Skill**

# Impact

- **Direct cash losses**
- **Reputation damage**
- **Loss of business—decrease in sales**
- **Drop in share price—less access to capital**
- **Reduction in market share**
- **Diminished operational efficiency (higher internal costs)**
- **Civil liability**
- **Legal liability**
- **Compliance liability (fines, censures, etc.)**
- **Interruption of business operations**



# Qualitative Risk Analysis

<b>Probability</b>	<b>Likely</b>	Medium Risk	High Risk	Extreme Risk
	<b>Unlikely</b>	Low Risk	Medium Risk	High Risk
	<b>Highly Unlikely</b>	Insignificant Risk	Low Risk	Medium Risk
		<b>Slightly Harmful</b>	<b>Harmful</b>	<b>Extremely Harmful</b>
		<b>Consequences</b>		

# **Risk Analysis Techniques and Considerations**

# Dimensions of an Asset

- **Asset value**
- **Threat scenarios**
- **Threat probabilities**
- **Relevant vulnerabilities**
- **Existing controls and their effectiveness**
- **Impact**

# Gathering Information

- **Interviews with process owners**
  - **Interviews with application developers**
  - **Interviews with security personnel**
  - **Interviews with external security experts**
  - **Security incident records**
  - **Analysis of incidents that occur in other organizations**
  - **Prior risk assessments (caution is advised, however, to stop the propagation of errors from one assessment to the next)**
-

# Risk Analysis Types

- **Qualitative**
  - **Higher v. lower**
- **Semiquantitative**
  - **Scale 1 to 5**
- **Quantitative**
  - **Actual costs**
  - **Difficult to measure event probability and costs**

# Quantitative Risk Analysis

- **Asset Value (AV)**
- **Exposure Factor (EF)**
- **Single Loss Expectancy (SLE)**
- **Annualized Rate of Occurrence (ARO)**
- **Annualized Loss Expectancy (ALE)**

# OCTAVE

- **Operationally Critical Threat Asset and Vulnerability Evaluation**
- **Risk analysis approach developed at Carnegie Mellon University**

# OCTAVE

- **Step 1: Establish risk measurement criteria**
- **Step 2: Develop an information asset profile**
- **Step 3: Identify information asset containers**
- **Step 4: Identify areas of concern**



# OCTAVE

- **Step 5: Identify threat scenarios**
- **Step 6: Identify risks**
- **Step 7: Analyze risks**
- **Step 8: Select mitigation approach**

# Other Risk Analysis Methodologies

- **Delphi method**
  - **Questionnaires given to experts**
- **Event Tree Analysis (ETA)**
  - **Derived from FTA, models a threat scenario**
- **Fault Tree Analysis (FTA)**
  - **Diagram of consequences for an event scenario**
- **Monte Carlo Analysis**
  - **Simulates a system using minimum, likely, and maximum values**

# Risk Evaluation and Ranking

- **Looking at all risks by business unit or service line**
  - **Looking at all risks by asset type**
  - **Looking at all risks by activity type**
  - **Looking at all risks by type of consequence**
-

# Risk Ownership

- **Assign individual risks to individual people**
- **Middle- or upper-management leaders**
- **Owners also own controls and resources**
- **Make risk treatment decisions**
- **Accountable**

# Risk Treatment

- **Risk acceptance**
- **Risk mitigation**
- **Risk avoidance**
- **Risk transfer**

# Framework for Risk Acceptance

- **The cost of risk mitigation is greater than the value of the asset being protected.**
- **The impact of compromise is low, or the value or classification of the asset is low.**

---

<b>Risk Level</b>	<b>Level Required to Accept</b>
Low	Chief information officer (CIO) or manager of information security
Medium	CISO or director of information security
High	CEO, COO, or president
Severe	Board of directors

# Revisiting an Accepted Risk

- **The value of the asset may have changed during the year.**
  - **The value of the business activity related to the asset may have changed during the year.**
  - **The potency of threats may have changed during the year, potentially leading to a higher risk rating.**
  - **The cost of mitigation may have changed during the year, potentially leading to greater feasibility for risk mitigation or transfer.**
-

# Controls

- **Common outcome of risk treatment**
- **Procedures or technical controls**



# Legal and Regulatory Considerations

- **Mandatory protective measures**
  - **PCI-DSS has these**
- **Optional protective measures**
  - **HIPAA has these**
- **Mandatory risk assessments**
  - **PCI-DSS requires them**

# Compliance Risk

- **Consequences of non-compliance**
  - **With a law, regulation, or legal obligation**
- **Two forms**
  - **Actual security incident**
  - **Fines and sanctions for mere noncompliance**
- **Business may pay fines rather than comply**

# Costs and Benefits

- **Change in threat probability**
- **Change in threat impact**
- **Change in operational efficiency**
- **Total Cost of Ownership (TCO)**

# TCO

- **Acquisition**
  - **Deployment and implementation**
  - **Recurring maintenance**
  - **Testing and assessment**
  - **Compliance monitoring and enforcement**
  - **Reduced throughput of controlled processes**
  - **Training**
  - **End-of-life decommissioning**
-

# Kahoot!

**Ch 3c-2**