Security Concepts in Support of Organizational Risk Mitigation

Chapter 20

TOTAL Seminars

Episode 20.01

Business Impact Analysis

Objective: 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.

- Business impact analysis

Business Impact Analysis

- Study of what's important to a business and what critical functions must be sustained
- Considerations
  - Maximum tolerable downtime and disruption for activities
  - Operational disruption and productivity
  - Financial considerations
  - Regulatory responsibilities
  - Reputation

Business Impact Analysis Steps

- Select individuals to interview for data gathering
  - People from all levels
- Create data-gathering techniques
  - Surveys, questionnaires, and qualitative and quantitative approaches
- Identify the company's critical business functions
- Identify resources these functions depend on

Business Impact Analysis Steps

- Calculate how long critical functions can survive without these resources
- Identify vulnerabilities and threats to critical business functions
- Calculate the risk for each critical business function
- Document findings, report them to management, make recommendations

Episode 20.02

Risk Identification

Objective: 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.

- Risk identification process

Risk Identification

- Main goals
  - Identify vulnerabilities
  - Determine probability that a threat will exploit a vulnerability
  - Determine potential business impact of each threat
  - Provide economic balance between impact of the threat and cost of the countermeasure

Risk Identification

- Ask the right questions
  - What event could occur (threat event)?
  - What could be the potential impact (magnitude)?
  - How likely is it to happen (probability)?
  - What level of confidence do we have in the answers to the first three questions (certainty)?

Risk Identification Process

- Evaluate cyber threat intelligence
- Conduct vulnerability assessment
- Observe cybersecurity operations
- Organize brainstorming sessions

Risk Identification Process

- Risk register
  - Unique identifier
  - Short name
  - Description
  - Owner
  - Probability
  - Magnitude
  - Risk value (or rating)
  - Disposition

Episode 20.03

Risk Calculation and Communication

Objective: 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.

- Risk calculation
  - Probability
  - Magnitude
- Communication of risk factors

Risk Calculation

- Qualitative
- Quantitative
- Risks that must be mitigated first have:
  - Highest probability
  - Highest magnitude

TOTAL Seminars

Risk Calculation

- Delphi technique
  - Each person anonymously lists risks
  - Each person anonymously comments

Qualitative Risk Matrix

Probability	Magnitude				
	Negligible	Minor	Moderate	Major	Severe
Almost Certain	Moderate	High	High	Extreme	Extreme
Likely	Moderate	Moderate	High	High	Extreme
Possible	Low	Moderate	Moderate	High	Extreme
Unlikely	Low	Moderate	Moderate	Moderate	High
Rare	Low	Low	Moderate	Moderate	High

Source: Chapman, B., & Maymí, F. (2020). *CompTIA CySA+™ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002)*, 484.

Sample Impact Interpretation

Rating	Value	Interpretation
Severe	5	Organizational survival is at risk; damages exceed $1M
Major	4	Prolonged (4+ hrs.) disruption to key business functions; damages do not exceed $1M
Moderate	3	Brief (<4 hrs.) disruptions to key business functions; damages do not exceed $100K
Minor	2	Some disruption of nonessential functions; damages do not exceed $10K
Negligible	1	Individual, nonessential disruptions; damages do not exceed $1K

Source: Chapman, B., & Maymí, F. (2020). *CompTIA CySA+™ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002)*, 486.

Example Qualitative Risk Calculation

Risk: Data Breach	Probability of Risk Taking Place	Magnitude of Loss to the Company
Cybersecurity analyst	2	4
Database admin	4	4
Application programmer	3	3
System operator	4	3
Operational manager	4	4
Results	**3.4**	**3.6**

Source: Chapman, B., & Maymí, F. (2020). *CompTIA CySA+™ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002)*, 487.

Communication of Risk Factors

- Presentation to multiple audiences
- Must be tailored for each audience

Episode 20.04

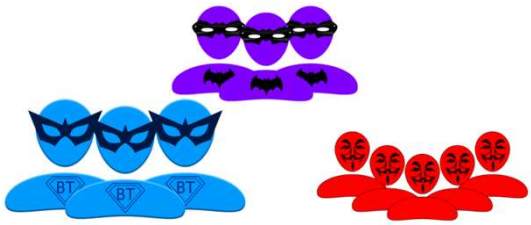
Training

Objective: 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.

- Training and exercises
  - Red team
  - Blue team
  - White team
  - Tabletop exercise

Teaming

- Red Team
  - Simulates threat actors (OPFOR); validates blue team assumptions
- Blue Team
  - The defenders; fixes red team discoveries
- White Team
  - Planners and moderators
- Purple Team
  - Dynamic hybrid of red and blue
  - Test blue team's processes, people, & technologies in a collaborative way



Training Programs & Resources

- Technical training
- Real life experience
- Active member of the community
  - Ex: presentations at security conferences
- Tabletop exercises (TTXs)
- Live-fire exercises
  - Cyber range
- Separate training teams

Episode 20.05

Supply Chain Assessment

Objective: 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.

- Supply chain assessment
  - Vendor due diligence
  - Hardware source authenticity

Vendor Due Diligence

- Review references and communicate with former and existing customers
- Review Better Business Bureau (BBB) reports
- Ensure that contracts/ agreements include requirements for adequate security controls
- Ensure that service level agreements (SLAs) are in place

Vendor Due Diligence

- Review vendor's security program
- Review internal and external audit reports and third-party reviews
- Conduct onsite inspection and interviews after signing the agreement
- Ensure the vendor has a business continuity plan (BCP)
- Implement a nondisclosure agreement (NDA)

Supply Chain Risk Assessment

- Hardware source authenticity
  - Trusted Foundry (DoD)