

Assessing IT Risks: Strengthening Cybersecurity

Part 1: Office Roleplay Dialogue

Scenario: An IT Technician, Daniel, is working with his colleague, Lisa, to conduct an IT risk assessment for their company's network security.

Lisa: Hey Daniel, the security team asked us to conduct an IT risk assessment. Where should we start?

Daniel: We should begin with **threat modeling**. This helps us identify potential security threats by analyzing how attackers might try to exploit our systems.

Lisa: That makes sense. After identifying threats, how do we check for weaknesses?

Daniel: We perform **vulnerability scanning** to detect security gaps in our network. This helps us find outdated software, weak passwords, or misconfigured systems.

Lisa: What if we want to test how secure our system really is?

Daniel: Then we conduct **penetration testing**. This simulates a cyberattack to see if an attacker could exploit our vulnerabilities. It's a great way to evaluate our defenses.

Lisa: That sounds useful. But how do we prevent these vulnerabilities from becoming real problems?

Daniel: We follow **security patch management**, which involves regularly updating software to fix security flaws. Many attacks happen because companies fail to install patches in time.

Lisa: That's a good point. Is there anything else we should do to minimize risk?

Daniel: Yes, we apply **risk mitigation** strategies, such as implementing multi-factor authentication and restricting access to sensitive data. The goal is to reduce the impact of any security breaches.

Lisa: Got it. I'll document our findings and make recommendations for improvements.

Daniel: Sounds like a plan! Let's make sure our systems stay secure.

Part 2: Comprehension Questions

1. What is the purpose of threat modeling?

- (A) To analyze and identify potential security threats
- (B) To install new firewalls
- (C) To track employee internet usage
- (D) To improve the speed of company computers

2. What does vulnerability scanning help with?

- (A) Encrypting email communications
- (B) Managing employee login schedules
- (C) Updating printer drivers
- (D) Detecting weaknesses in a network

3. How does penetration testing improve cybersecurity?

- (A) By monitoring Wi-Fi signal strength
- (B) By simulating a cyberattack to test for weaknesses
- (C) By deleting unnecessary files from servers
- (D) By blocking all external network connections

4. What is the goal of risk mitigation?

- (A) To increase website loading speed
 - (B) To provide free software for employees
 - (C) To reduce the impact of security threats
 - (D) To prevent employees from using personal devices at work
-

Part 3: Key Vocabulary Definitions in Japanese

1. **Threat Modeling (脅威モデリング)** – サイバー攻撃の可能性を分析し、システムの脆弱性を特定する手法。
2. **Vulnerability Scanning (脆弱性スキャン)** – ネットワークやソフトウェアのセキュリティ上の弱点を自動で検出するプロセス。
3. **Penetration Testing (侵入テスト)** – 実際の攻撃をシミュレーションして、システムのセキュリティをテストする方法。
4. **Security Patch Management (セキュリティパッチ管理)** – ソフトウェアの脆弱性を修正するために、定期的にパッチを適用する管理プロセス。

5. Risk Mitigation (リスク軽減) – セキュリティ脅威の影響を最小限に抑えるための対策を講じること。

Part 4: Questions & Correct Answers

1. What is the purpose of threat modeling?

☒ (A) To analyze and identify potential security threats

2. What does vulnerability scanning help with?

☒ (D) Detecting weaknesses in a network

3. How does penetration testing improve cybersecurity?

☒ (B) By simulating a cyberattack to test for weaknesses

4. What is the goal of risk mitigation?

☒ (C) To reduce the impact of security threats