Cybersecurity & Risk Management Strategies

Part 1: Dialogue

Characters:

- **Naoki (CIO)** – Chief Information Officer, responsible for overseeing cybersecurity policies.
- **Elena (Security Analyst)** – Security Analyst, assisting in risk management planning.

Elena: Naoki, with increasing cyber threats, how are we strengthening our cybersecurity framework?

Naoki: Our focus is on risk management—identifying vulnerabilities and ensuring compliance with industry standards.

Elena: That's essential. Are we updating our data protection policies as well?

Naoki: Yes, we're refining access controls and encryption protocols to enhance data security.

Elena: What about incident response? Do we have a structured plan in case of a breach?

Naoki: Absolutely. We've implemented a step-by-step process to contain, analyze, and mitigate security incidents.

Elena: That's great. Are employees trained on cybersecurity awareness?

Naoki: Yes, regular training ensures that everyone understands potential threats and best practices.

Elena: Sounds solid. I'll review our compliance documentation to ensure we meet all requirements.

Naoki: Perfect. Let's schedule a security audit next month to assess our improvements.

Elena: Good idea! I'll coordinate with the team and set up the details.

Part 2: Comprehension Questions

1. What is the company's main focus in improving cybersecurity?
   - (A) Reducing employee salaries
   - (B) Strengthening risk management
   - (C) Increasing IT spending randomly
   - (D) Removing all security controls
2. How is the company improving data protection?
   - (A) By deleting old data
   - (B) By enhancing encryption and access controls
   - (C) By allowing unrestricted data access
   - (D) By avoiding security updates
3. What is included in the company's incident response plan?
   - (A) Ignoring cyber threats
   - (B) Hiring external consultants only
   - (C) Containing, analyzing, and mitigating security incidents
   - (D) Waiting until legal action is taken

4. What step will the company take next to ensure compliance?
    - (A) Conducting a security audit
    - (B) Disabling security policies
    - (C) Removing all firewalls
    - (D) Ignoring cybersecurity threats

Part 3: Key Vocabulary & Definitions in Japanese

- **Cybersecurity** – サイバーセキュリティ
- **Risk management** – リスク管理 (リスクかんり)
- **Compliance** – コンプライアンス
- **Data protection** – データ保護 (データほご)
- **Incident response** – インシデント対応 (インシデントたいおう)

Part 4: Answer Key

1. What is the company's main focus in improving cybersecurity?
    - (B) Strengthening risk management ✅
2. How is the company improving data protection?
    - (B) By enhancing encryption and access controls ✅
3. What is included in the company's incident response plan?

   - (C) Containing, analyzing, and mitigating security incidents ✅

4. What step will the company take next to ensure compliance?
   - (A) Conducting a security audit ✅