Cybersecurity Policy Discussion

---

1. Role-Play Dialogue (Approximately 10 minutes)

Context: The IT security team and management are discussing cybersecurity measures to prevent data breaches.

Participants:

- **James (CIO)** – Chief Information Officer
- **Sarah (IT Security Manager)** – Responsible for implementing cybersecurity policies
- **David (CEO)** – Concerned about business risks and compliance
- **Emma (Operations Manager)** – Represents the concerns of employees

Dialogue:

James: Thank you all for joining today's meeting. We need to strengthen our cybersecurity policies to prevent data breaches. If we strengthen our cybersecurity, then we could significantly reduce our risk exposure.

Sarah: That's correct. Currently, our firewall and encryption standards are outdated. If we update these measures, then our data will be much more secure.

David: I understand the need for security, but what about the budget? If we invest heavily in cybersecurity, then we might have to cut costs elsewhere.

Emma: Another concern is employee compliance. If we implement stricter policies, then employees might struggle with usability issues.

James: I see your points. However, if we don't act now, then a data breach could cost us far more than an initial investment.

Sarah: Exactly. We can also introduce employee training sessions. If employees receive proper training, then they will understand the importance of cybersecurity.

David: That makes sense. Let's draft a policy revision plan and determine the best way to balance security and usability.

Emma: Agreed. If we find an efficient solution, then this will benefit both the company and its employees.

---

2. Comprehension Questions & Sample Answers (Approximately 5 minutes)

1. **What is the main concern discussed in the meeting?**
    - The meeting focuses on strengthening cybersecurity policies to prevent data breaches.
2. **Why is David hesitant about investing in cybersecurity?**
    - He is concerned that investing in cybersecurity could require budget cuts in other areas.
3. **What potential issue does Emma bring up regarding stricter policies?**
    - She worries that stricter policies might make it difficult for employees to use company systems efficiently.
4. **What solution does Sarah propose to ensure employee compliance?**
    - She suggests providing cybersecurity training to employees so they understand the importance of compliance.

---

3. Teacher's Lesson Points (Concise Version)

Pre-Class Preparation:

- Review the dialogue and key vocabulary: cybersecurity, data breach, firewall, encryption, compliance.
- Prepare explanations on modal verbs (e.g., "could," "might") and conditional structures (e.g., "If we strengthen...").

Lesson Flow:

1. Introduction (2–3 minutes):

- Ask the student: “How does your company handle cybersecurity?”
- Introduce the lesson’s focus on cybersecurity discussions.

2. Reading & Analysis (10 minutes):

- Have the student read the dialogue aloud.
- Correct pronunciation and emphasize natural intonation.
- Highlight modal verbs and conditionals in context.

3. Comprehension Check (5 minutes):

- Ask comprehension questions and provide feedback.
- Encourage the student to use target vocabulary in responses.

4. Role-Play Practice (Remaining Time):

- The teacher plays the CIO or CEO, while the student plays the IT Security Manager or Operations Manager.
- Encourage the student to use key vocabulary and grammatical structures.

5. Wrap-Up (2–3 minutes):

- Summarize the key takeaways: importance of cybersecurity, modal verbs, and conditional statements.
- Assign a short homework task: Write a brief proposal outlining three cybersecurity improvements for a company, using at least three conditional sentences.