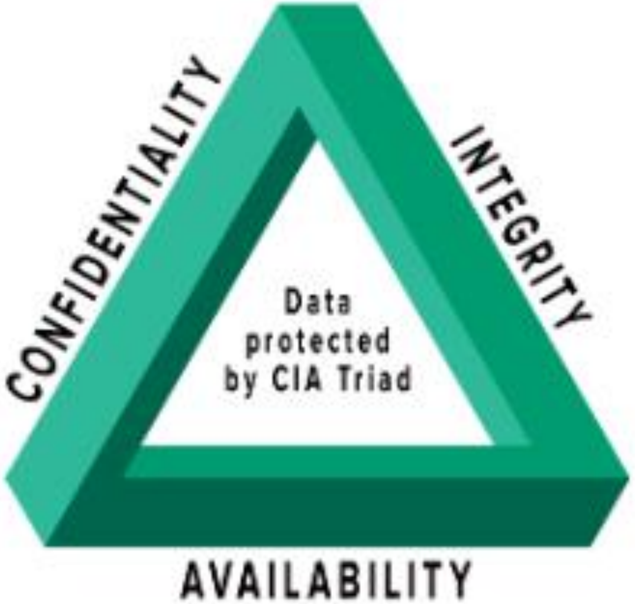
Information Security Policies and Standards

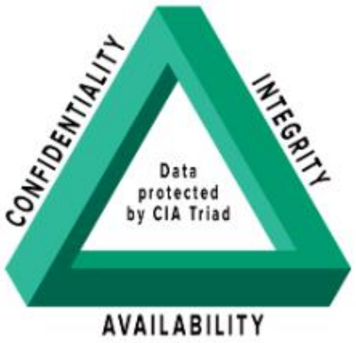
- Security Policies: Development and Implementation
- Security Standards and Frameworks (e.g., ISO/IEC 27001, NIST)
- Compliance and Regulatory Requirements

REVIEW

protection
data
privacy
safe
code
secrecy
security
password

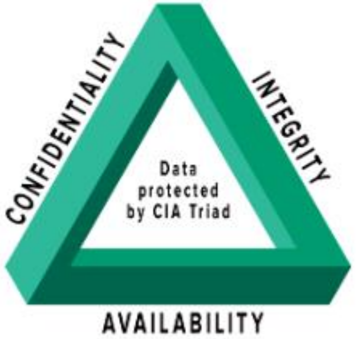
The CIA Triad





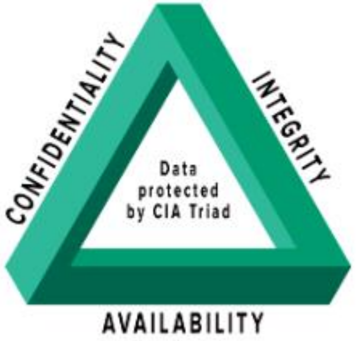
Confidentiality

Protecting information from unauthorized access.



Integrity

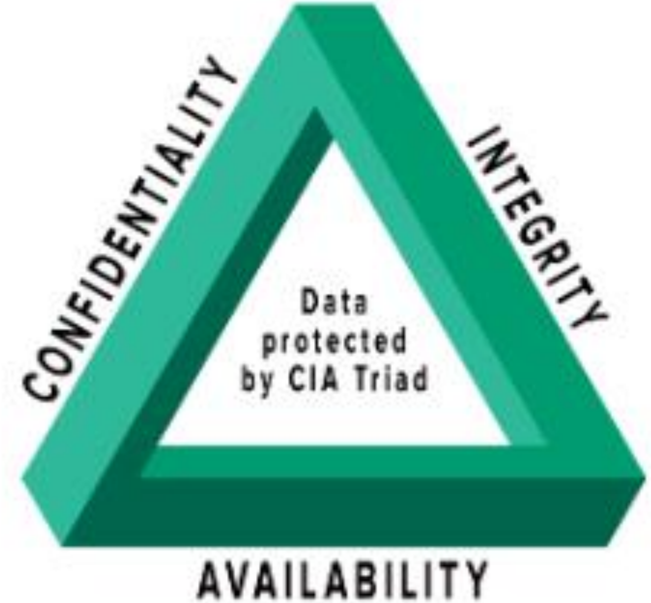
Ensuring that information remains accurate and unaltered.



Availability

Making sure that information is accessible to authorized users when they need it.

The CIA Triad



Types of Threats

- **Malware**
- **Phishing**
- **Insider Threats**

Real-World Examples

1. Comelec Data Breach (2016)
2. Wendy's Philippines (2017)
3. Cebuana Lhuillier Marketing Server Branch (2019)
4. UCPB Independence Day Cyber Attacks (2020)
5. PhilHealth Medusa Attack (2023)

Information Assurance vs. Information Security: Understanding the Differences

- **Information Security**: Focuses on protecting data and systems from threats.
- **Information Assurance:** Encompasses a broader scope, including risk management, compliance, and ensuring the reliability of information systems.

Key Takeaways

1. The CIA Triad is fundamental to understanding information security.
2. Different types of threats require different defensive strategies.
3. Real-world examples teach us the importance of having clear security goals.
4. Information Assurance offers a holistic approach to managing risks and protecting information.

Information Security Policies and Standards

- Security Policies: Development and Implementation
- Security Standards and Frameworks (e.g., ISO/IEC 27001, NIST)
- Compliance and Regulatory Requirements

Objective:

Understand the importance of information security policies and standards, and how they are implemented within organizations to protect information assets.

What are Information Security Policies?

These are formal documents that outline how an organization plans to protect its information assets.

Example:

- Password Policy
- Acceptable Use Policy (AUP)
- Data Classification Policy
- Incident Response Policy
- Remote Access Policy

What are Information Security Standards?

- benchmarks that those rules are measured against.
- provide a way to evaluate the effectiveness of security policies and ensure that they meet industry best practices.

Some well-known international standards

- ISO/IEC 27001
- NIST
    - National Institute of Standards and Technology

Difference

- Policies are specific to an organization and its needs.
- Standards are universally recognized frameworks that help organizations align their security practices with industry norms.

The Role of Policies and Standards in Organizations

- help mitigate security risks by providing a clear plan of action for protecting information assets.
- reduces the likelihood of breaches and ensures that everyone in the organization knows their role in maintaining security

Information assets

- databases,
- data files,
- contracts and agreements,
- system documentation,
- user manuals,
- training materials,
- operational/support procedure,
- business continuity plans,
- back up plans,
- audit trails,
- archived information.

Process

- identifying risks,
- setting goals,
- regularly reviewing and updating the policies

Case Study

Case Study 1:
Organization with
Strong Security Policies

Case Study 2:
Organization with Weak
or Outdated Security
Policies

Case Study 1: Organization with Strong Security Policies

Scenario:

A financial institution receives an influx of phishing emails targeting its employees.

Response:

Robust Incident Response Policy

Comprehensive Employee Security Awareness Training

Case Study 2: Organization with Weak or Outdated Security Policies

Scenario:
A retail company has not updated its security policies in several years.

The company's Password Management Policy is outdated, requiring only 8-character passwords without enforcing periodic changes.

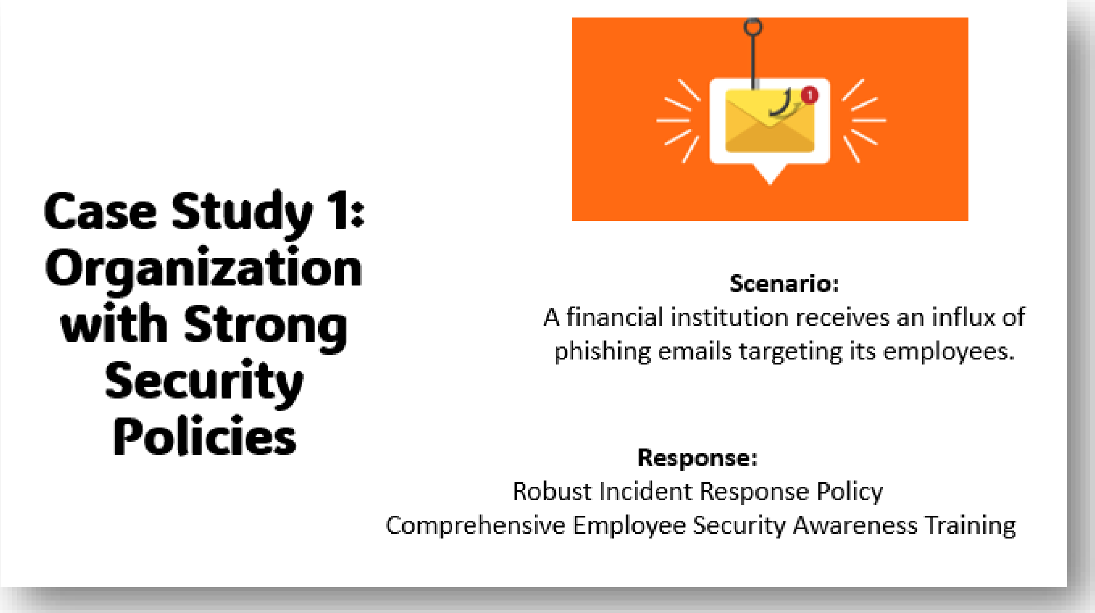
There is no mandatory Two-Factor Authentication (2FA) for critical systems.

Case Study 2: Organization with Weak or Outdated Security Policies

Response:

Because the company’s Incident Response Plan is outdated and employees are not regularly trained on security threats, the phishing attack goes unnoticed for several days.

During this time, the attacker gains unauthorized access to the company's customer database, exfiltrating sensitive customer information including credit card details and personal data.

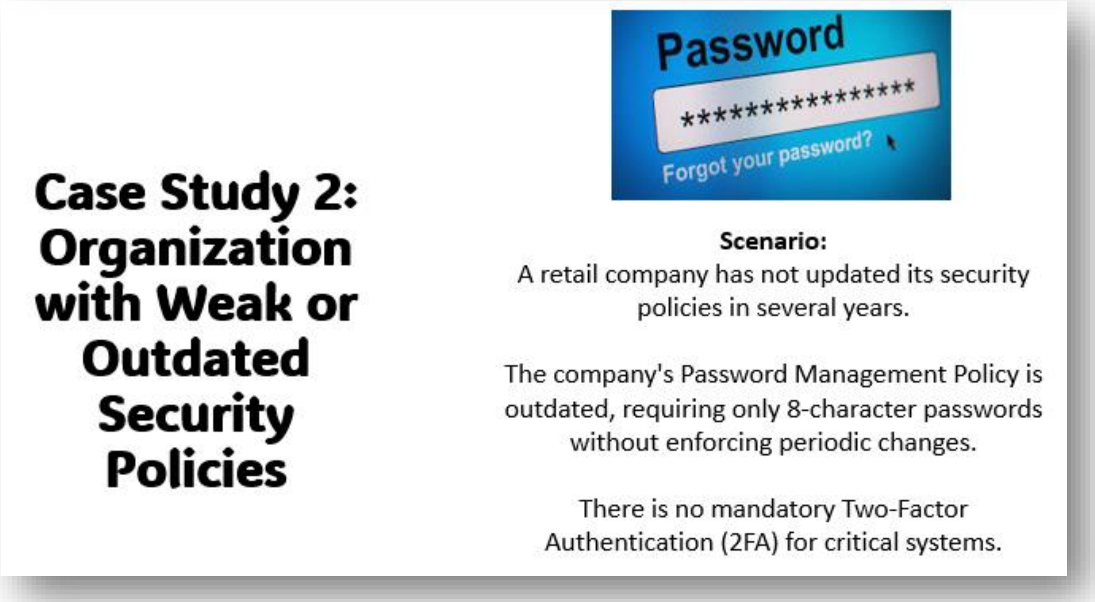


Case Study 1: Organization with Strong Security Policies

Scenario:
A financial institution receives an influx of phishing emails targeting its employees.

Response:
Robust Incident Response Policy
Comprehensive Employee Security Awareness Training

organization’s preparedness and adherence to security standards allowed it to thwart a phishing attack with minimal impact.



Case Study 2: Organization with Weak or Outdated Security Policies

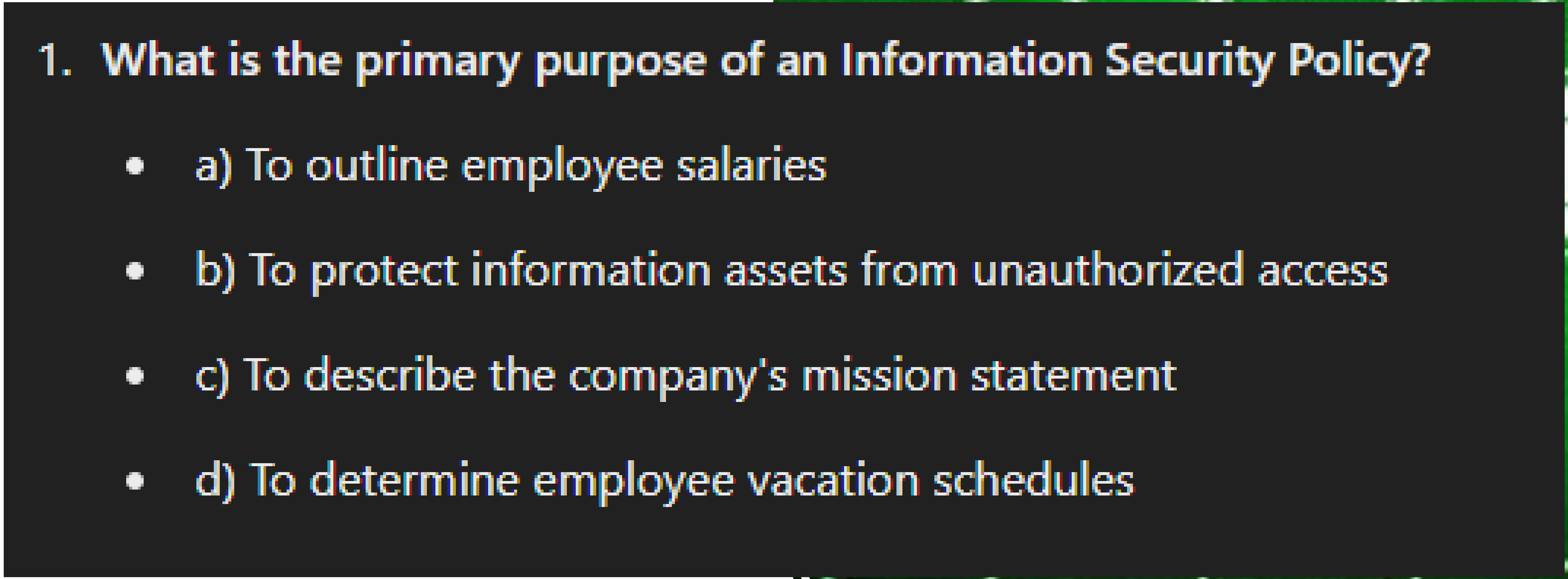
Scenario:
A retail company has not updated its security policies in several years.

The company's Password Management Policy is outdated, requiring only 8-character passwords without enforcing periodic changes.

There is no mandatory Two-Factor Authentication (2FA) for critical systems.

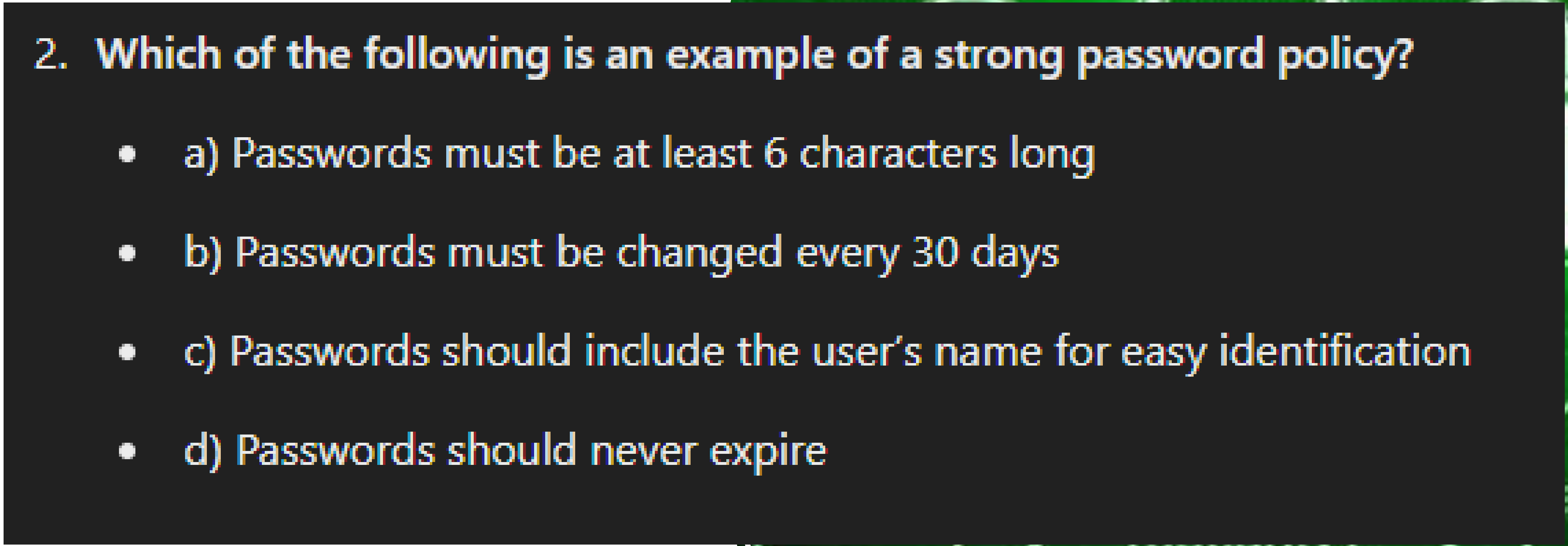
the lack of robust security measures led to a significant data breach with severe consequences.

Quiz - Multiple Choice



1. **What is the primary purpose of an Information Security Policy?**
    - a) To outline employee salaries
    - b) To protect information assets from unauthorized access
    - c) To describe the company's mission statement
    - d) To determine employee vacation schedules

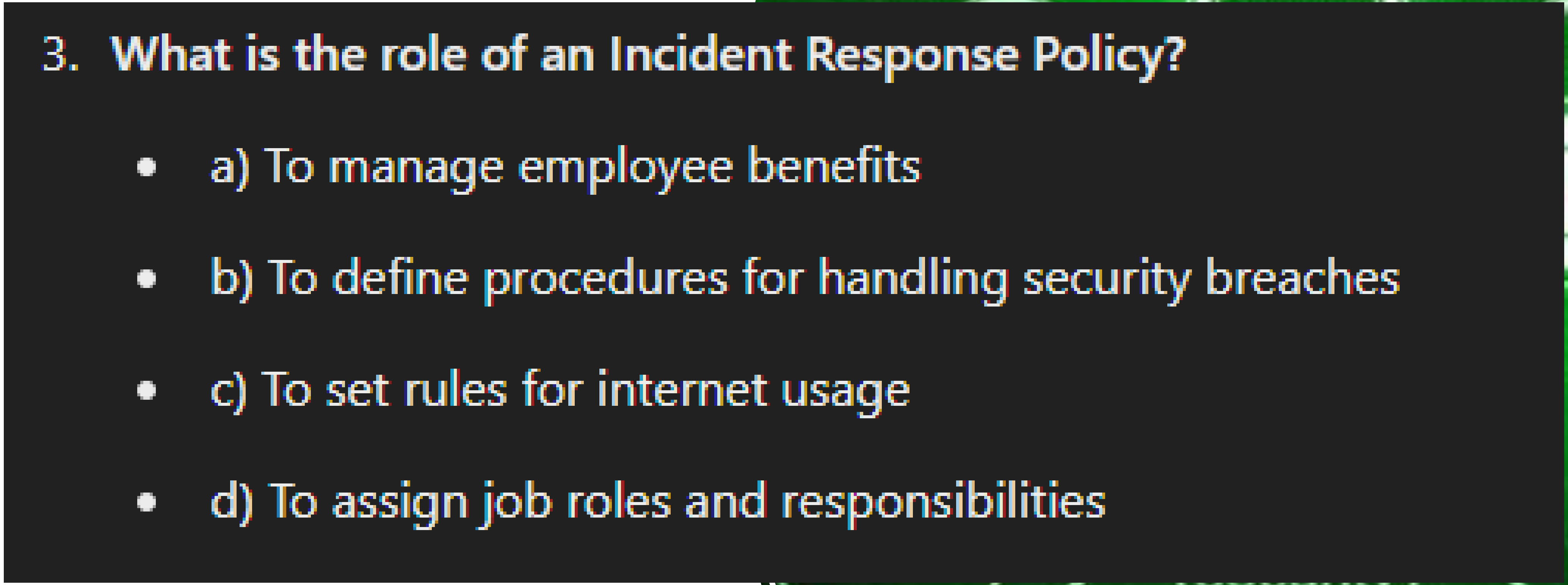
Quiz - Multiple Choice



2. Which of the following is an example of a strong password policy?

- a) Passwords must be at least 6 characters long
- b) Passwords must be changed every 30 days
- c) Passwords should include the user's name for easy identification
- d) Passwords should never expire

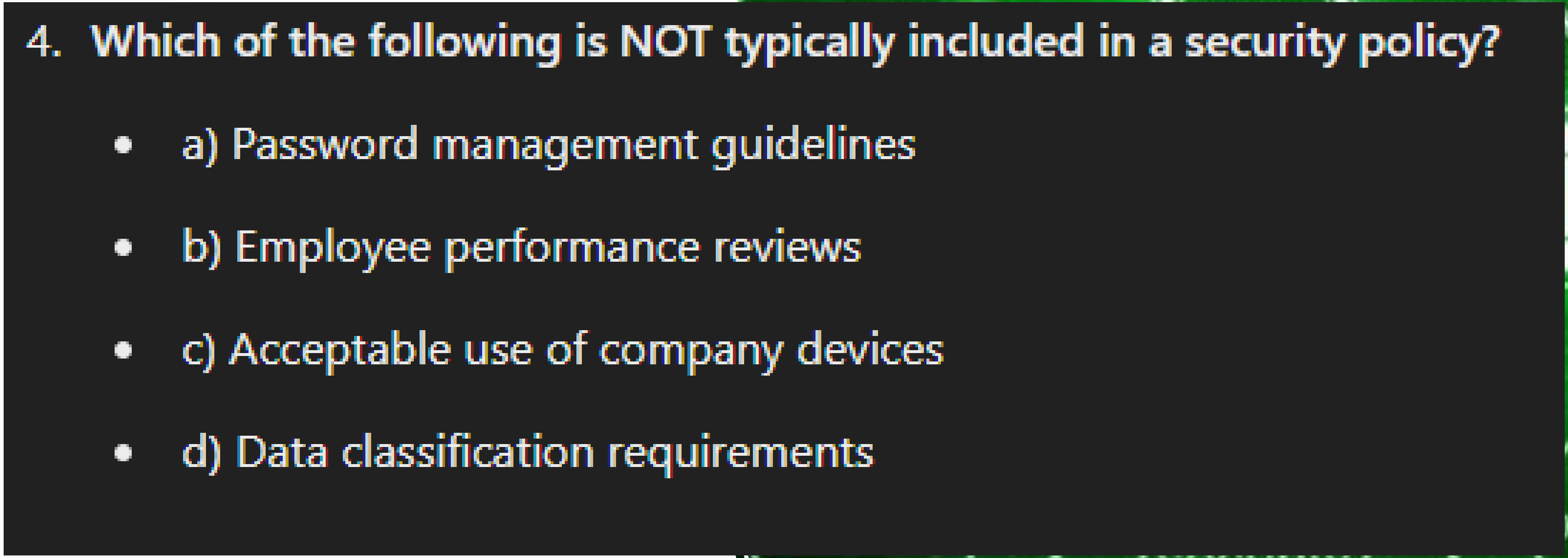
Quiz - Multiple Choice



3. What is the role of an Incident Response Policy?

- a) To manage employee benefits
- b) To define procedures for handling security breaches
- c) To set rules for internet usage
- d) To assign job roles and responsibilities

Quiz - Multiple Choice



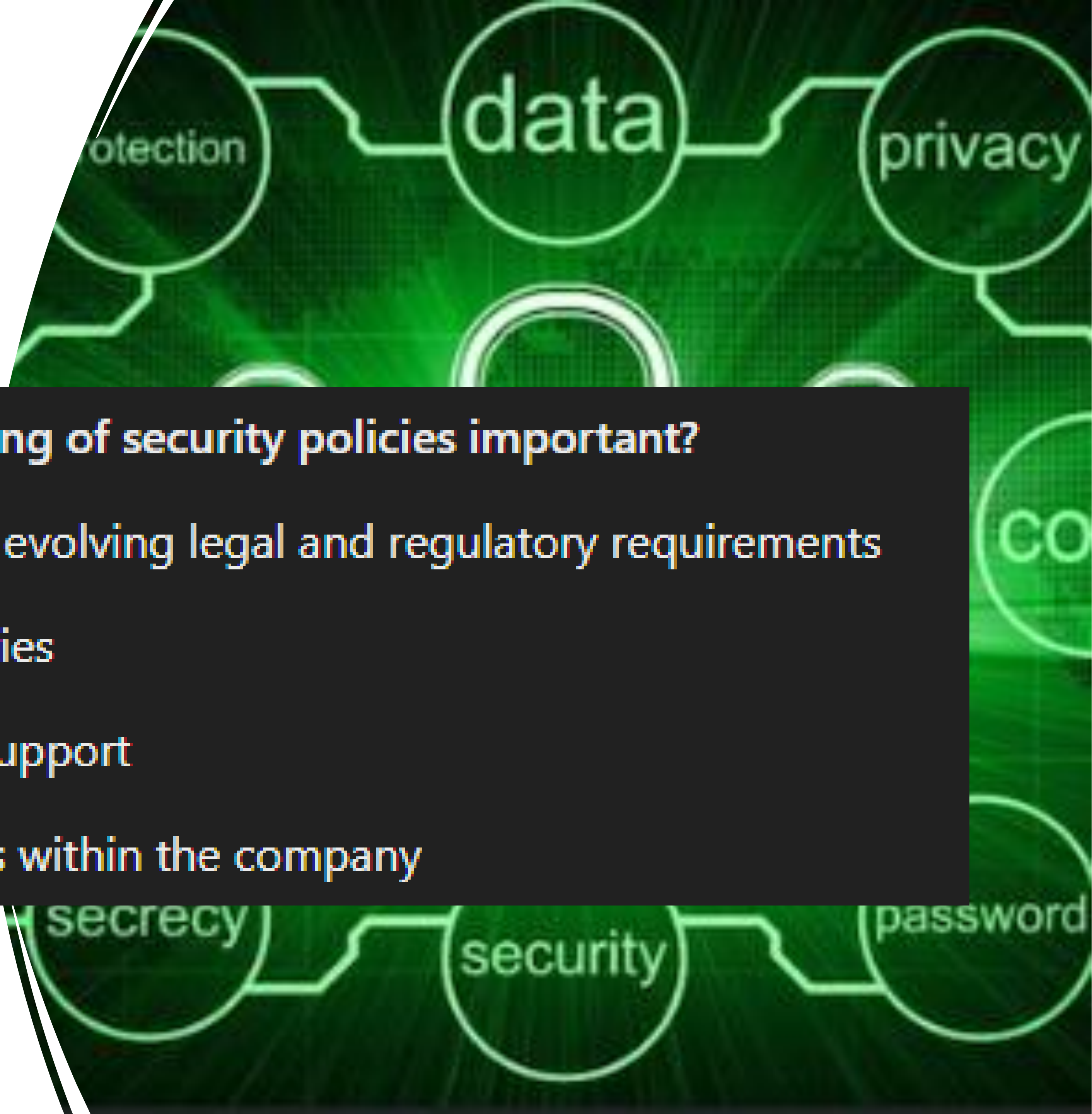
4. Which of the following is NOT typically included in a security policy?

- a) Password management guidelines
- b) Employee performance reviews
- c) Acceptable use of company devices
- d) Data classification requirements

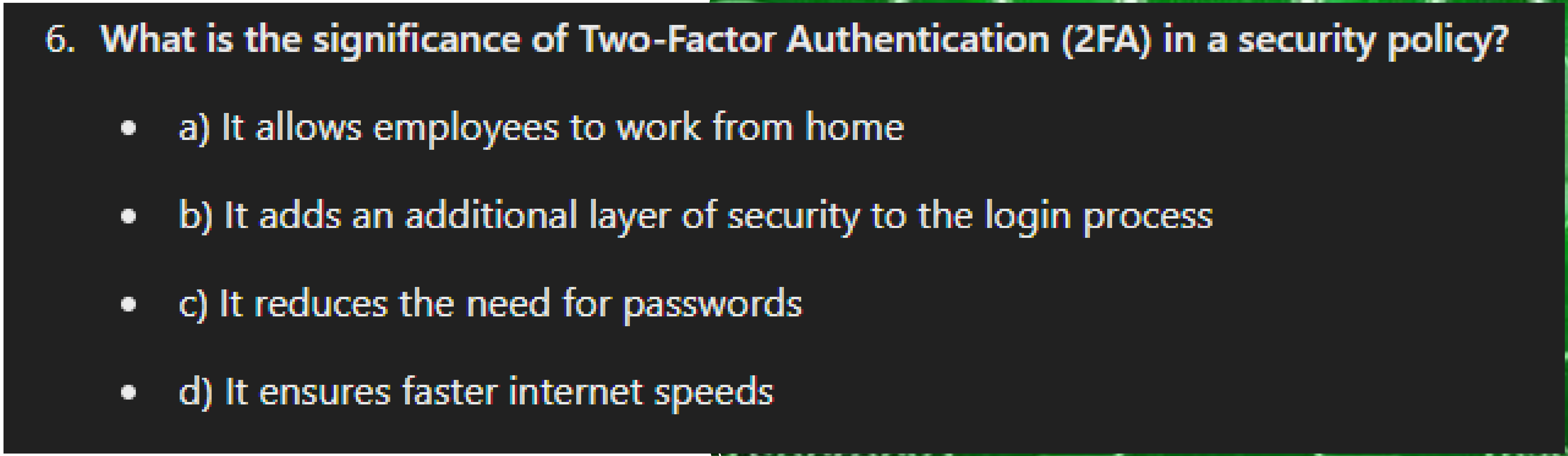
Quiz - Multiple Choice

5. **Why is regular review and updating of security policies important?**

- a) To ensure compliance with evolving legal and regulatory requirements
- b) To increase employee salaries
- c) To reduce the need for IT support
- d) To promote social activities within the company



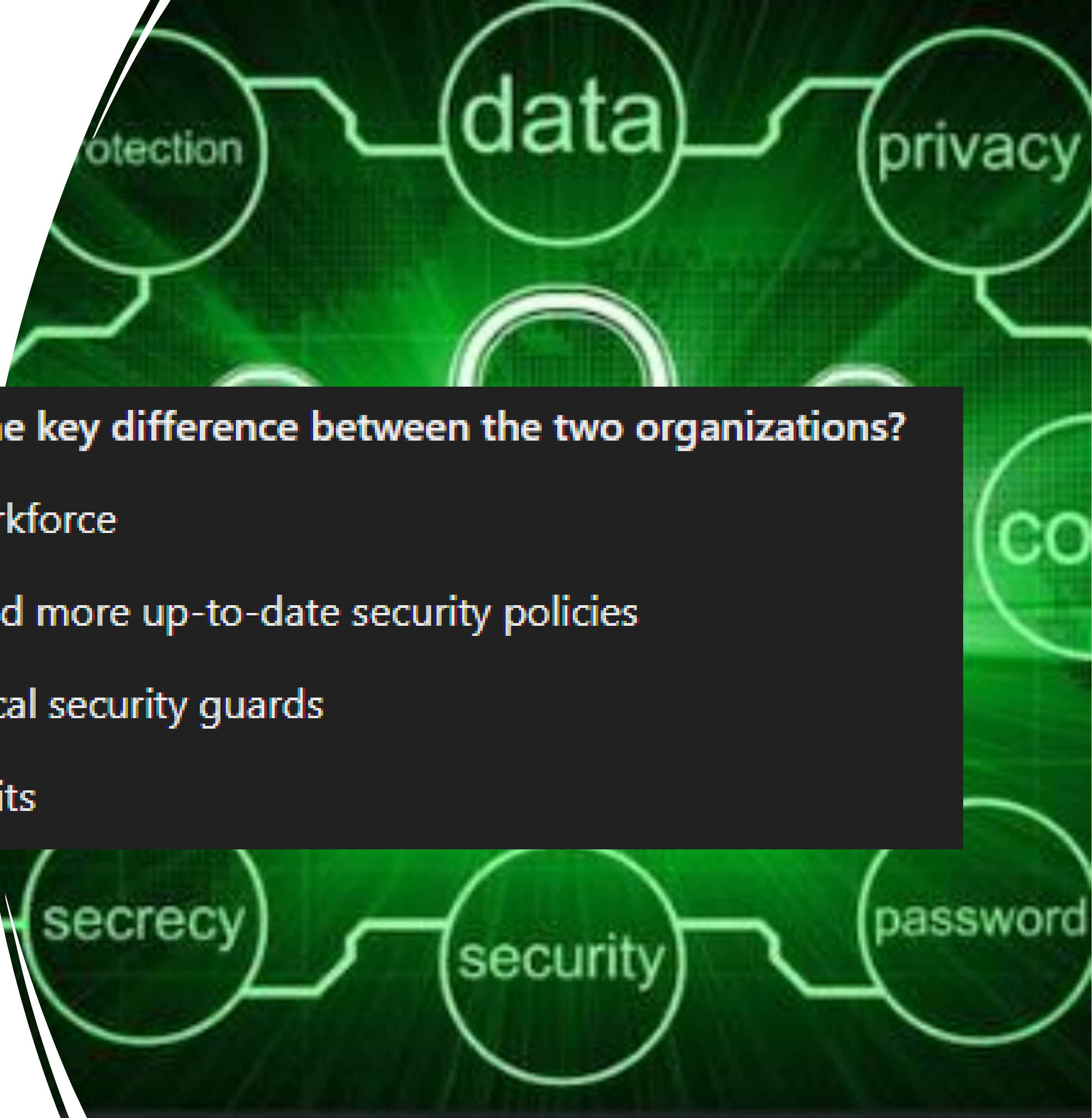
Quiz - Multiple Choice



6. **What is the significance of Two-Factor Authentication (2FA) in a security policy?**

- a) It allows employees to work from home
- b) It adds an additional layer of security to the login process
- c) It reduces the need for passwords
- d) It ensures faster internet speeds

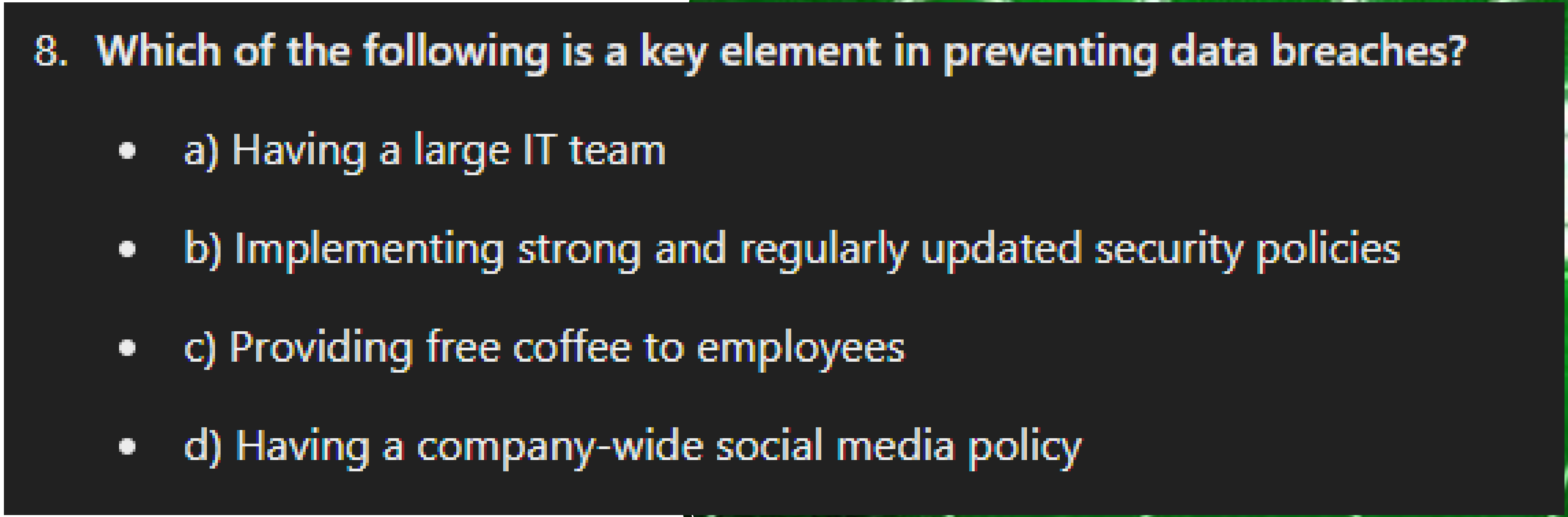
Quiz - Multiple Choice



7. In the case study discussed, what was the key difference between the two organizations?

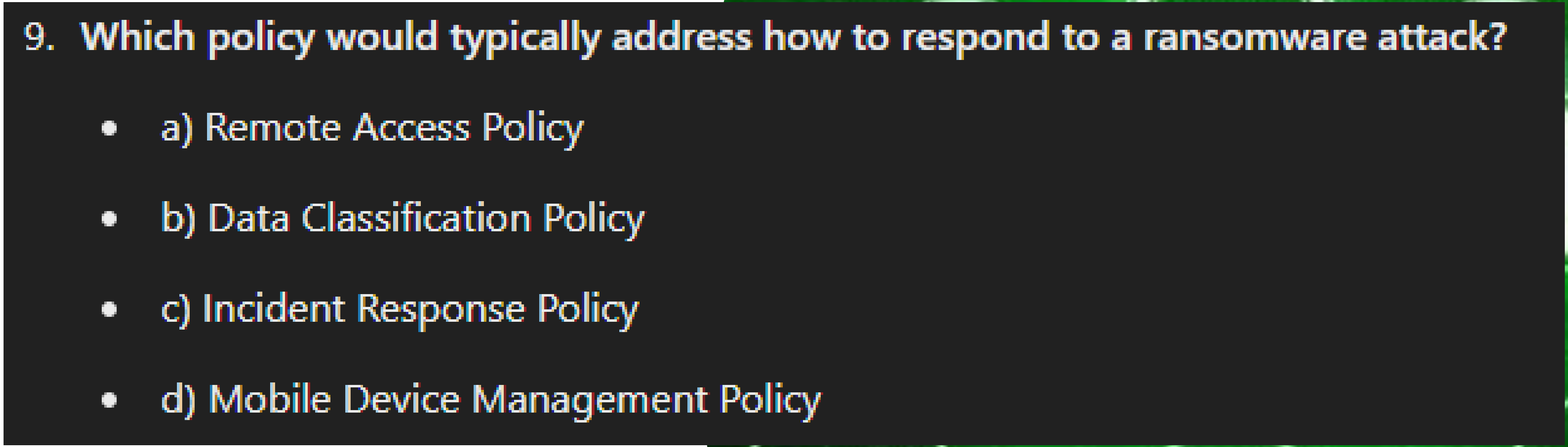
- a) One organization had a larger workforce
- b) One organization had stronger and more up-to-date security policies
- c) One organization had more physical security guards
- d) One organization had higher profits

Quiz - Multiple Choice



8. Which of the following is a key element in preventing data breaches?
    - a) Having a large IT team
    - b) Implementing strong and regularly updated security policies
    - c) Providing free coffee to employees
    - d) Having a company-wide social media policy

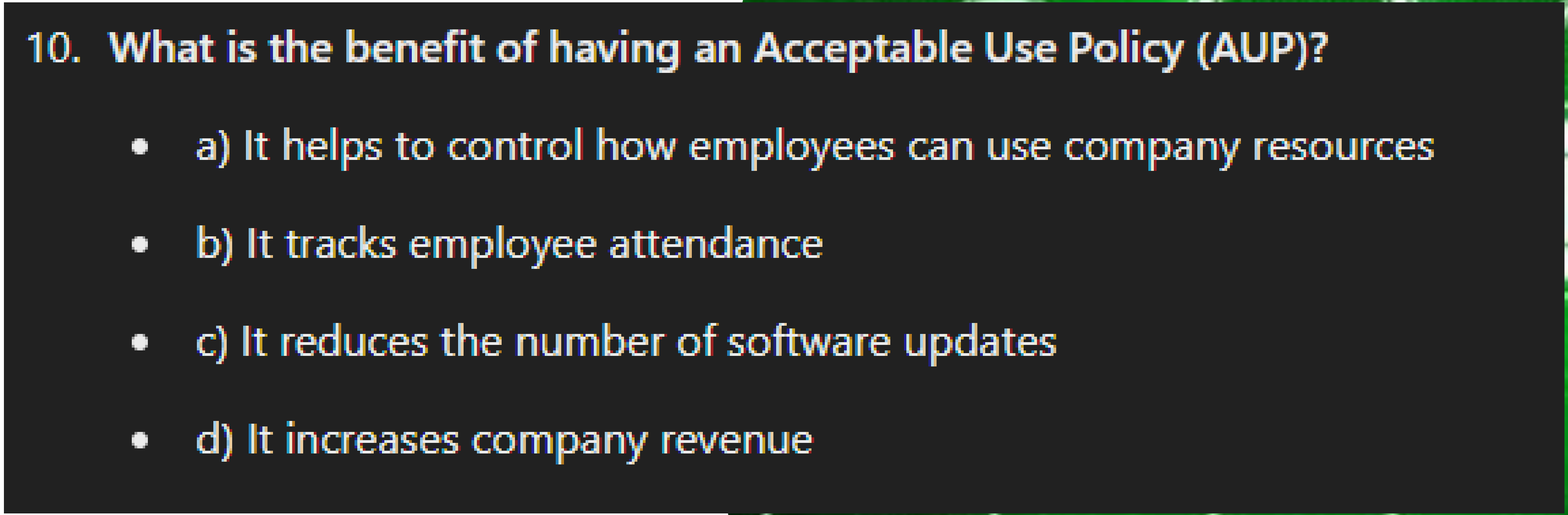
Quiz - Multiple Choice



9. Which policy would typically address how to respond to a ransomware attack?

- a) Remote Access Policy
- b) Data Classification Policy
- c) Incident Response Policy
- d) Mobile Device Management Policy

Quiz - Multiple Choice



10. **What is the benefit of having an Acceptable Use Policy (AUP)?**

- a) It helps to control how employees can use company resources
- b) It tracks employee attendance
- c) It reduces the number of software updates
- d) It increases company revenue

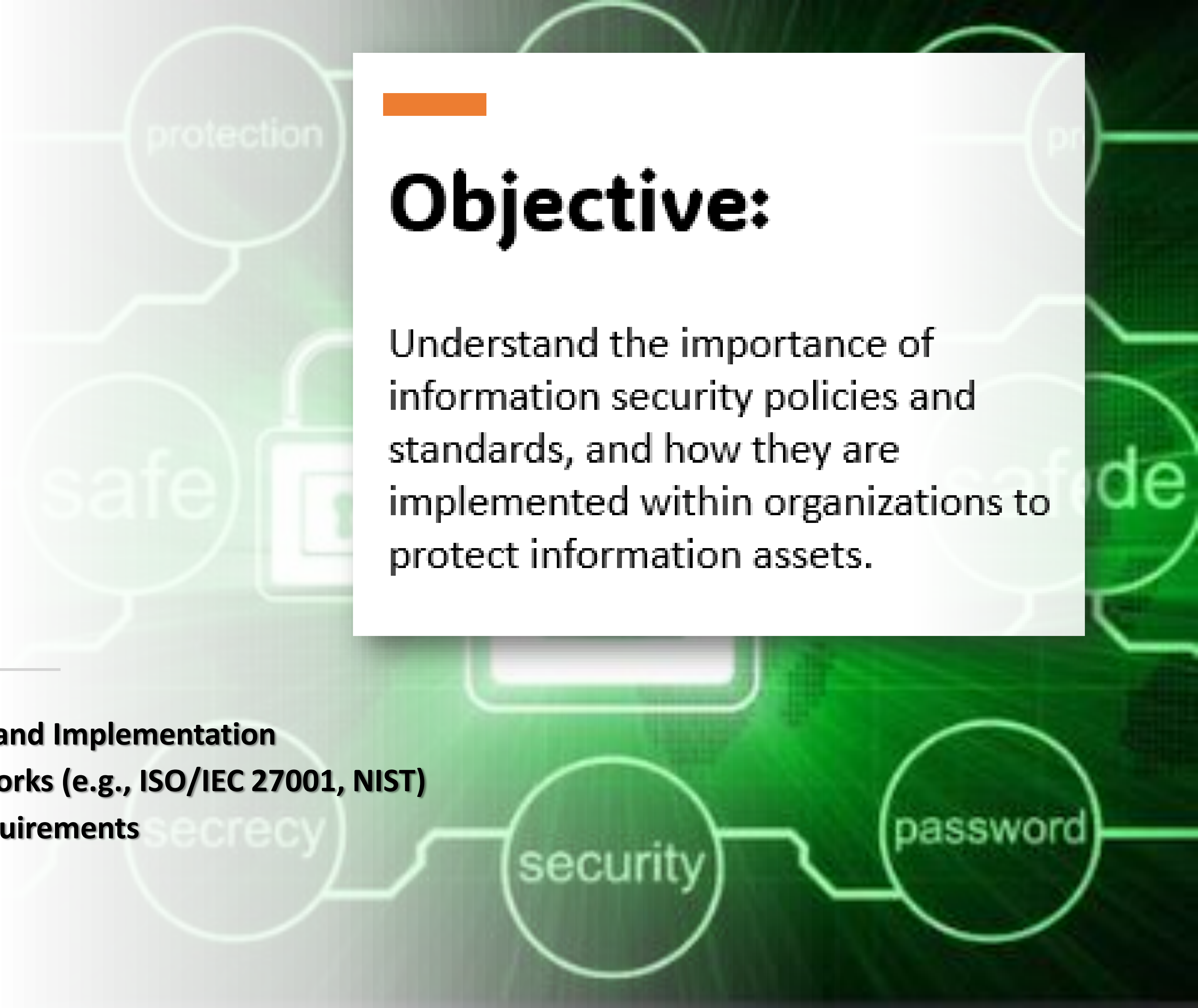
Assignment:

Case Study Analysis:

- Research a real-world example of a data breach that occurred due to inadequate or outdated information security policies.
- Write a 2-3 page analysis covering the following:
  - ❖ The background of the organization and the breach.
  - ❖ The specific weaknesses in the security policies that led to the breach.
  - ❖ The impact of the breach on the organization and its stakeholders.
  - ❖ Recommendations on how the breach could have been prevented through stronger or updated policies.

Information Security Policies and Standards

- Security Policies: Development and Implementation
- Security Standards and Frameworks (e.g., ISO/IEC 27001, NIST)
- Compliance and Regulatory Requirements



Objective:

Understand the importance of information security policies and standards, and how they are implemented within organizations to protect information assets.

Thank You.

protection
data
privacy
safe
code
secrecy
security
password