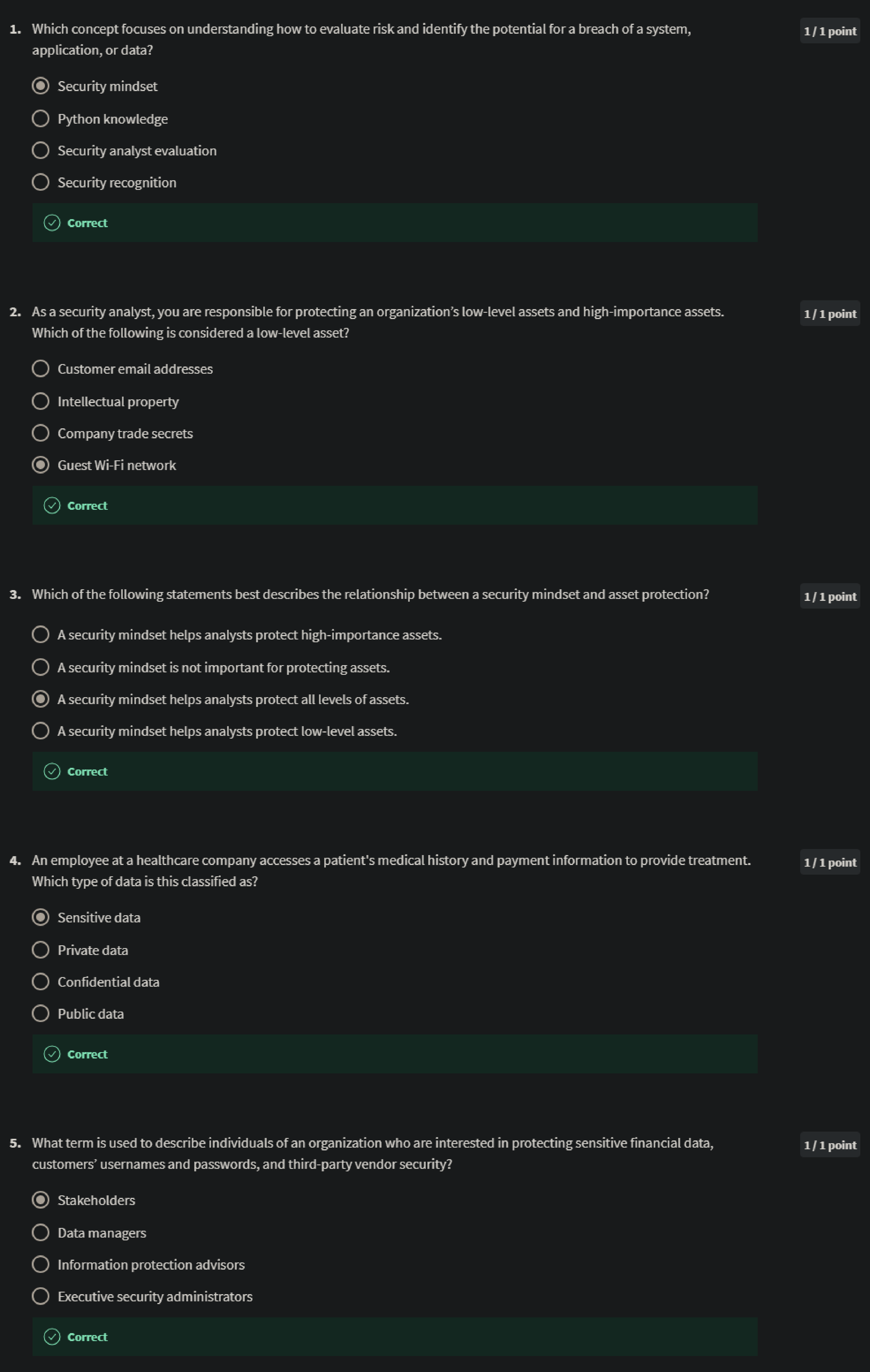


1. Which concept focuses on understanding how to evaluate risk and identify the potential for a breach of a system, application, or data?

1 / 1 point

● Security mindset

○ Python knowledge

○ Security analyst evaluation

○ Security recognition

✓ Correct

2. As a security analyst, you are responsible for protecting an organization's low-level assets and high-importance assets. Which of the following is considered a low-level asset?

1 / 1 point

○ Customer email addresses

○ Intellectual property

○ Company trade secrets

● Guest Wi-Fi network

✓ Correct

3. Which of the following statements best describes the relationship between a security mindset and asset protection?

1 / 1 point

○ A security mindset helps analysts protect high-importance assets.

○ A security mindset is not important for protecting assets.

● A security mindset helps analysts protect all levels of assets.

○ A security mindset helps analysts protect low-level assets.

✓ Correct

4. An employee at a healthcare company accesses a patient's medical history and payment information to provide treatment. Which type of data is this classified as?

1 / 1 point

● Sensitive data

○ Private data

○ Confidential data

○ Public data

✓ Correct

5. What term is used to describe individuals of an organization who are interested in protecting sensitive financial data, customers' usernames and passwords, and third-party vendor security?

1 / 1 point

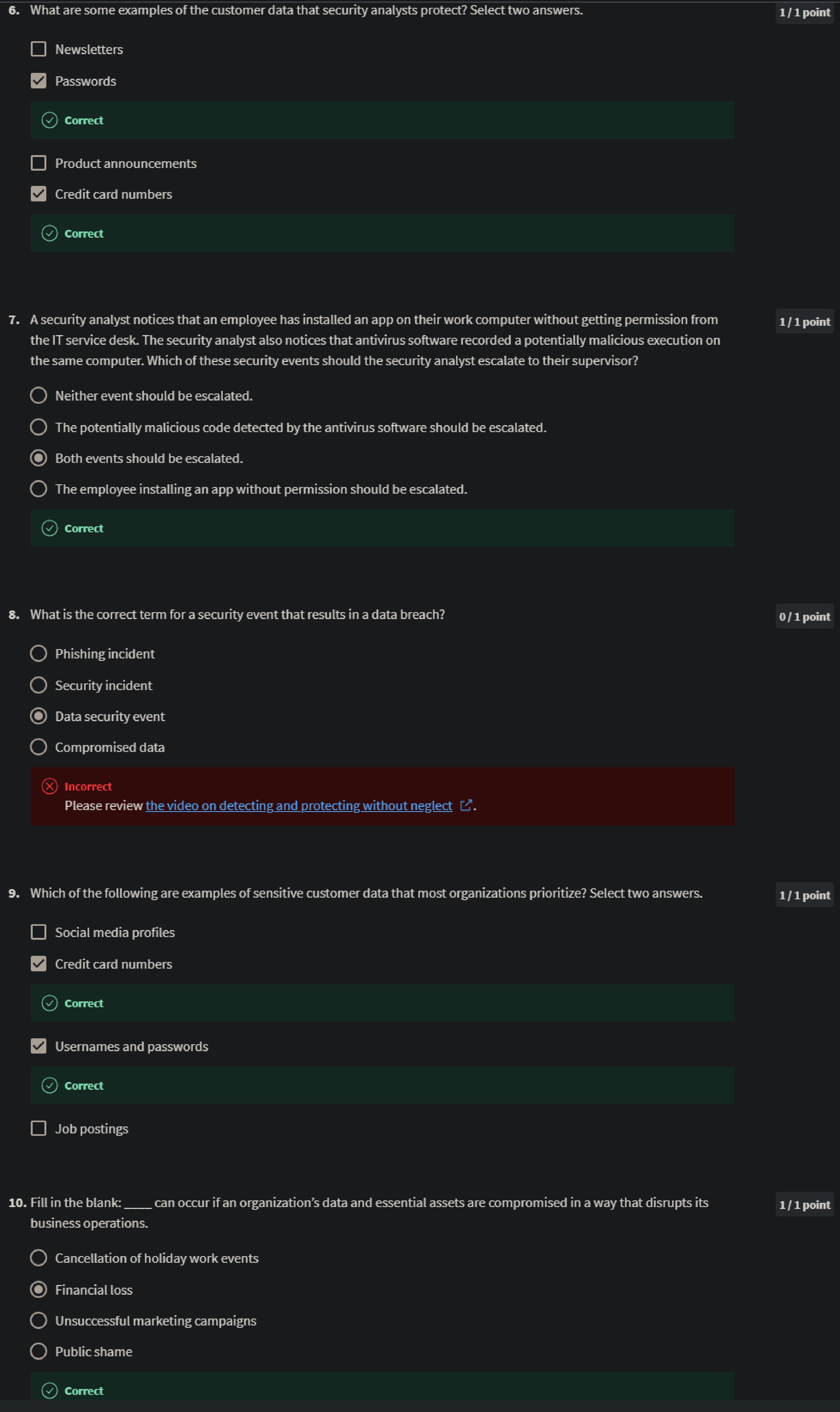
● Stakeholders

○ Data managers

○ Information protection advisors

○ Executive security administrators

✓ Correct



**6.** What are some examples of the customer data that security analysts protect? Select two answers.

**1 / 1 point**

□ Newsletters

☑ Passwords

Correct

□ Product announcements

☑ Credit card numbers

Correct

**7.** A security analyst notices that an employee has installed an app on their work computer without getting permission from the IT service desk. The security analyst also notices that antivirus software recorded a potentially malicious execution on the same computer. Which of these security events should the security analyst escalate to their supervisor?

**1 / 1 point**

○ Neither event should be escalated.

○ The potentially malicious code detected by the antivirus software should be escalated.

● Both events should be escalated.

○ The employee installing an app without permission should be escalated.

Correct

**8.** What is the correct term for a security event that results in a data breach?

**0 / 1 point**

○ Phishing incident

○ Security incident

● Data security event

○ Compromised data

Incorrect

Please review the video on detecting and protecting without neglect.

**9.** Which of the following are examples of sensitive customer data that most organizations prioritize? Select two answers.

**1 / 1 point**

□ Social media profiles

☑ Credit card numbers

Correct

☑ Usernames and passwords

Correct

□ Job postings

**10.** Fill in the blank: _____ can occur if an organization’s data and essential assets are compromised in a way that disrupts its business operations.

**1 / 1 point**

○ Cancellation of holiday work events

● Financial loss

○ Unsuccessful marketing campaigns

○ Public shame

Correct