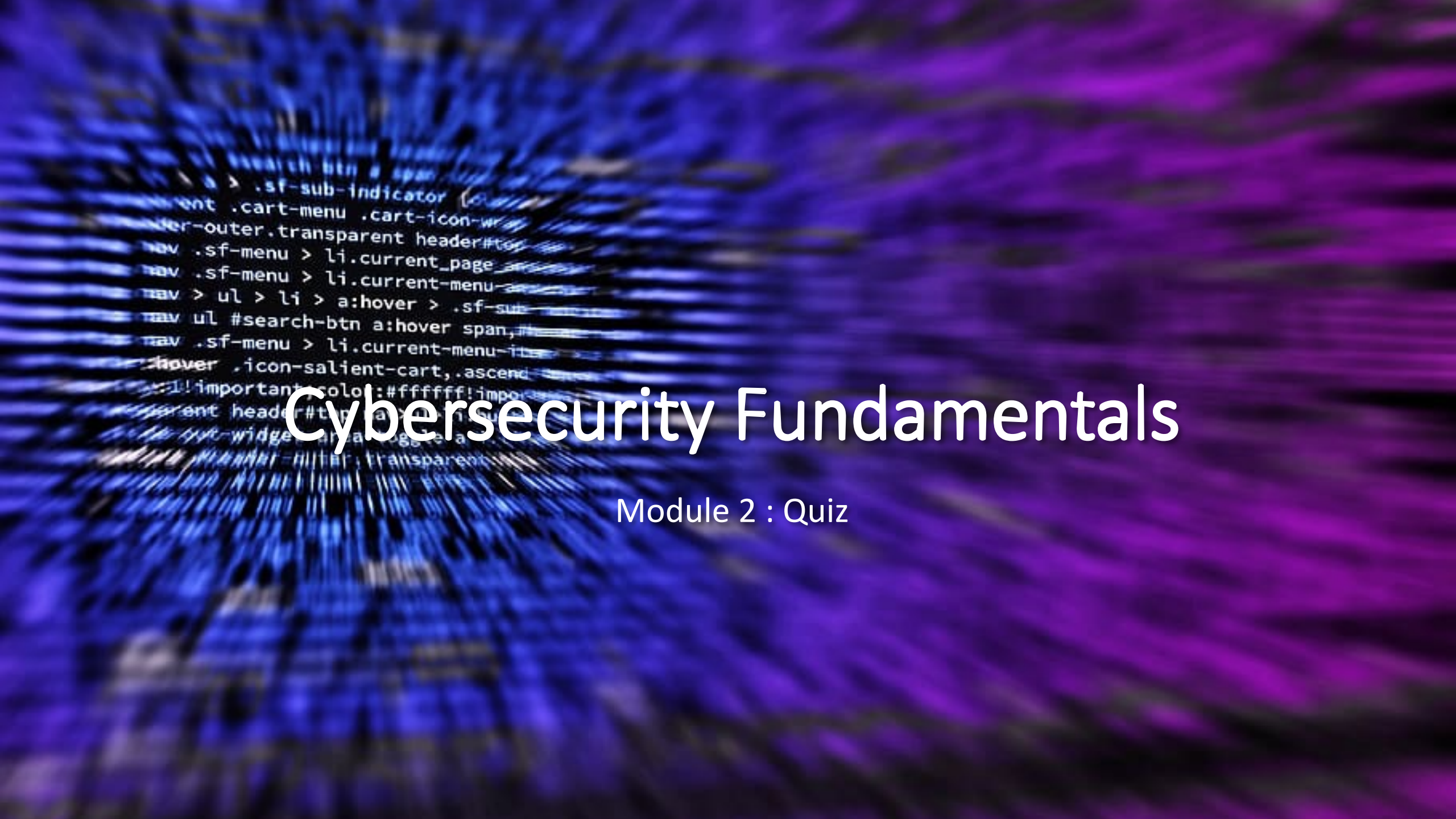


Cybersecurity Fundamentals

Module 2 : Quiz

Question 1

- You are working in your organization's security office. You receive a call from a user who has tried to log in to the network several times with the correct credentials, with no success. This is an example of a(n)_____.

  A) Emergency

  B) Event

  C) Policy

  D) Disaster

Question 2

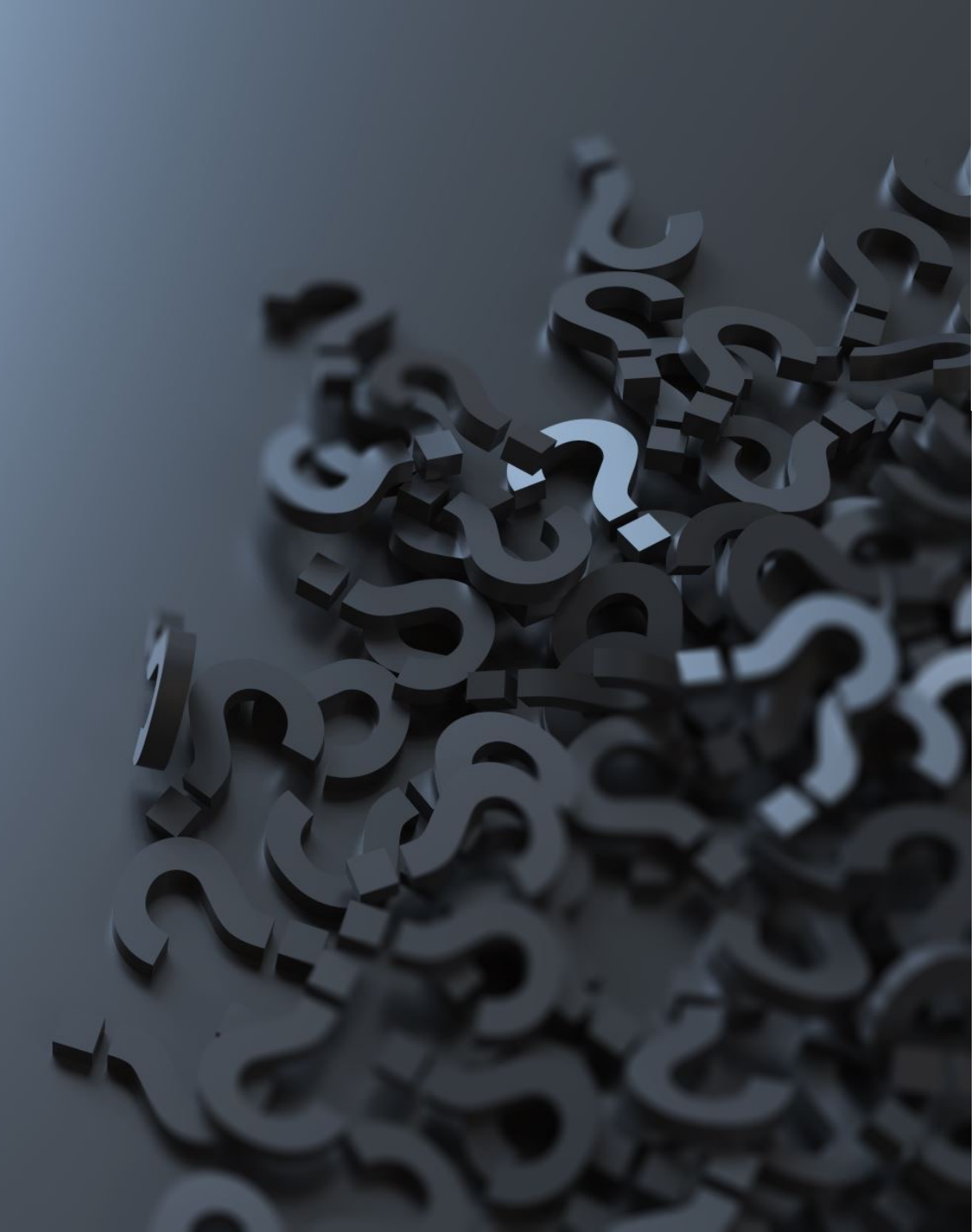
- You are working in your organization's security office. You receive a call from a user who has tried to log in to the network several times with the correct credentials, with no success. After a brief investigation, you determine that the user's account has been compromised. This is an example of a(n)_____.

  A) Risk management

  B) Incident detection

  C) Malware

  D) Disaster



Question 3

- An external entity has tried to gain access to your organization's IT environment without proper authorization. This is an example of a(n) _____.

  A) Exploit

  B) Intrusion

  C) Event

  D) Malware

Question 4

- When responding to a security incident, your team determines that the vulnerability that was exploited was not widely known to the security community, and that there are no currently known definitions/listings in common vulnerability databases or collections. This vulnerability and exploit might be called _____.

  A) Malware

  B) Critical

  C) Fractal

  D) Zero-day

Question 5

- True or False? The IT department is responsible for creating the organization's business continuity plan.

Question 6

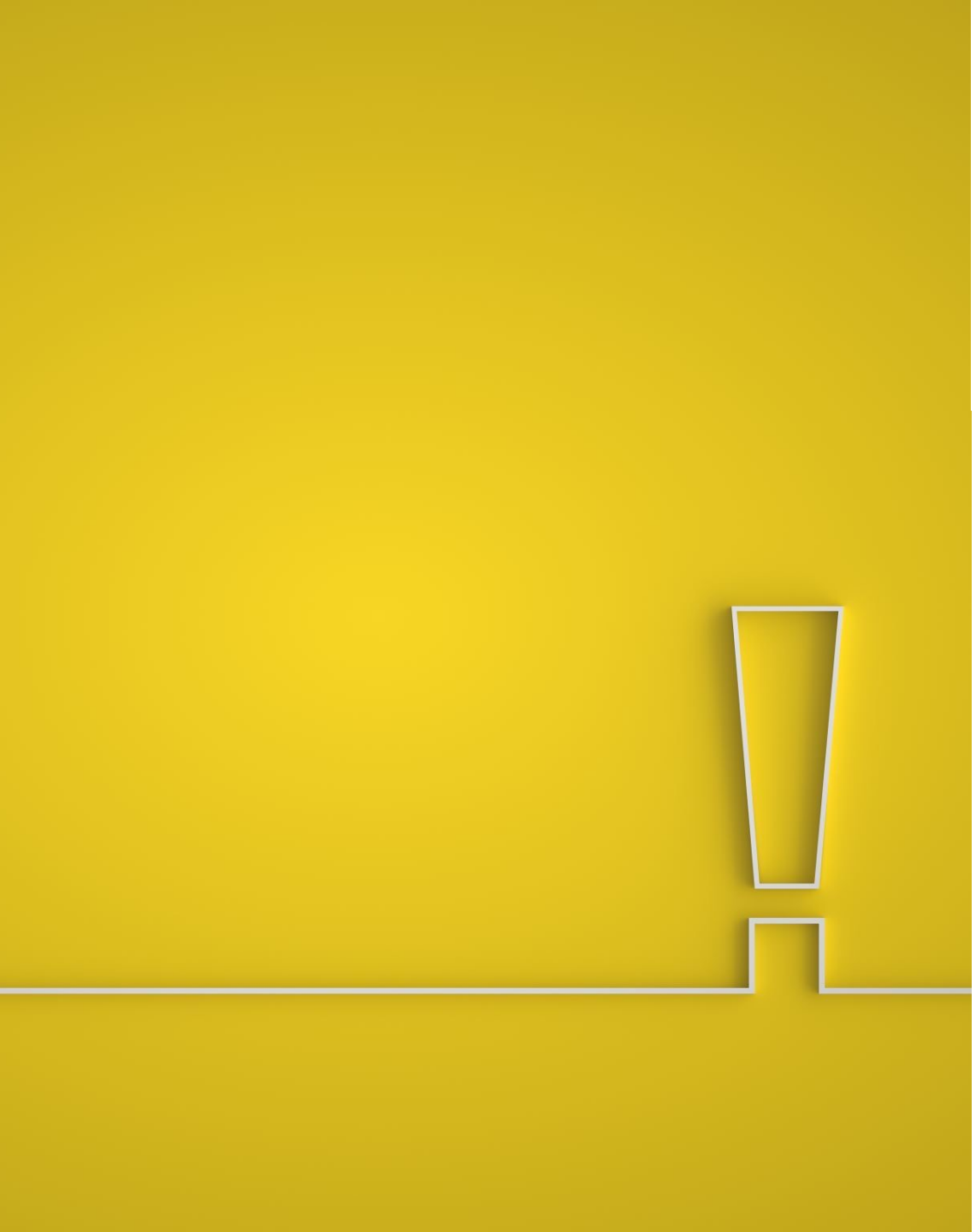
- The Business Continuity effort for an organization is a way to ensure critical _____ functions are maintained during a disaster, emergency, or interruption to the production environment.

  A) Business

  B) Technical

  C) IT

  D) Financial



Question 7

- Which of the following is very likely to be used in a disaster recovery (DR) effort?

  A) Guard dogs

  B) Data backups

  C) Contract personnel

  D) Anti-malware solutions

Question 8

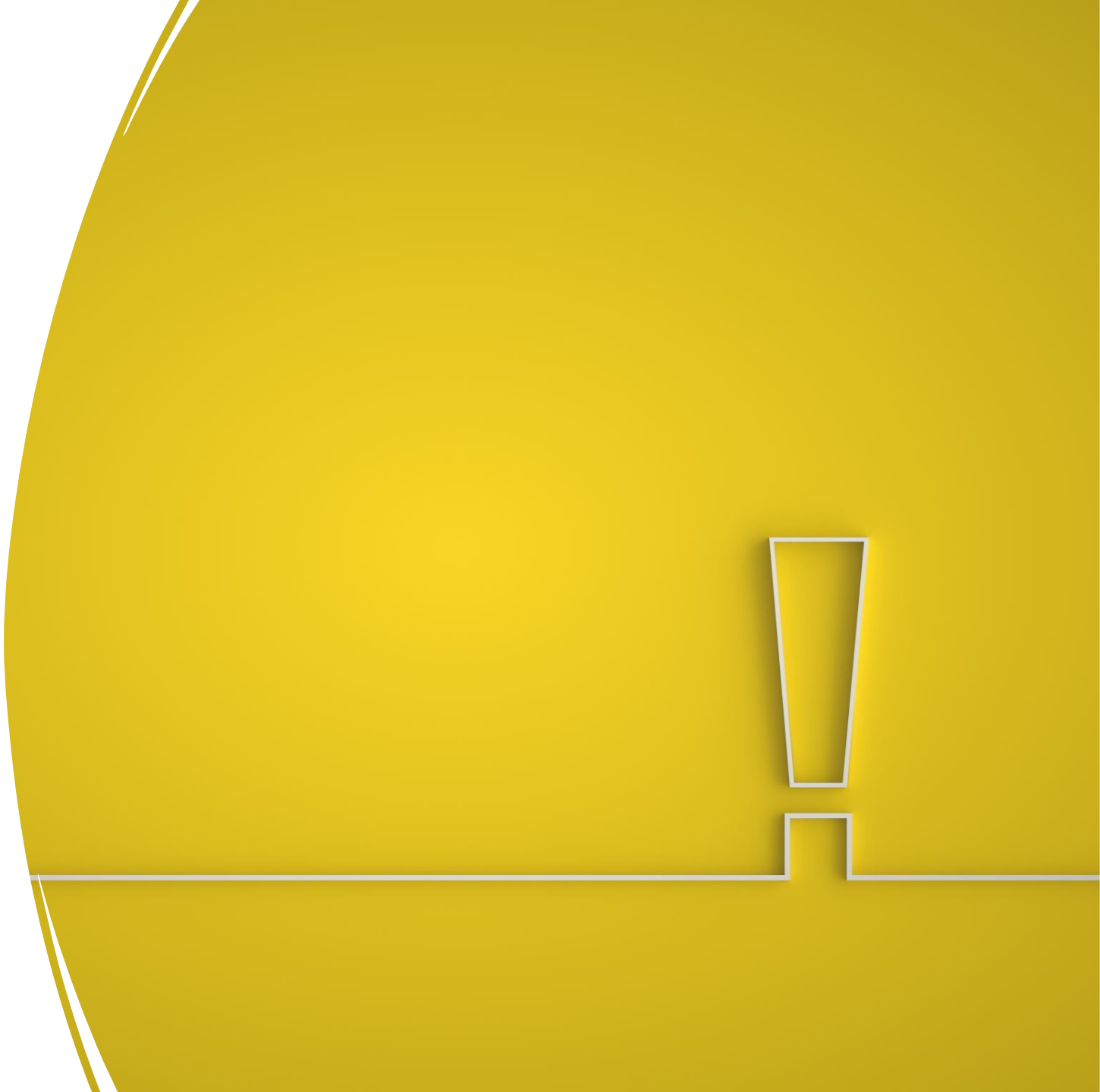
- Which of the following is often associated with DR planning?

  A) Checklists

  B) Firewalls

  C) Motion detectors

  D) Non-repudiation



Question 9

Which of these activities is often associated with DR efforts?

A) Employees returning to the primary production location

B) Running anti-malware solutions

C) Scanning the IT environment for vulnerabilities

D) Zero-day exploits

Question 10

- Which of these components is very likely to be instrumental to any disaster recovery (DR) effort?

  A) Routers

  B) Laptops

  C) Firewalls

  D) Backups