

16. A state's National Guard base is documenting cybersecurity risks from physical vulnerabilities. Which of the following would be classified as a moderate risk?
- (A) An unlocked trailer containing non-networked office equipment that cannot be used to access sensitive systems
  - (B) A locked warehouse with noncritical computers that could be a foothold to access other network resources
  - (C) A publicly accessible touchscreen directory for visitors that contains no sensitive data and is unlikely to be exploited
  - (D) A main server room that contains sensitive systems and information and does not have sufficiently restricted or controlled access

**Questions 17 through 20 refer to the following.**

Consider the following article.

*Small Town Bank Disrupts Attempted Cyber Attack on Customer Database*

Fairgrove Community Bank, a local financial institution serving residents of central Kentucky, reported that it successfully stopped a cyber intrusion attempt earlier this week aimed at its customer database.

The attack was detected on Tuesday afternoon when automated security systems flagged unusual database queries originating from the bank's online loan application form. Investigators determined that the form was being used to input malicious code.

"One of the strings the adversary submitted included ' OR '1'='1';--', " said James Holloway, a network administrator at Fairgrove Community Bank. "That's a common trick pulled from online tutorials."

Holloway said the attacker did not succeed in accessing any customer data, but the attempt revealed a flaw in the bank's web application.

Fairgrove Community Bank's security team has since patched the vulnerability. No data was compromised, and banking operations continued without interruption.

"This wasn't some advanced adversary," Holloway added. "They were copying code from the internet and testing to see if anything would work. But even simple attacks like this can work if we don't implement best practices."

Fairgrove Community Bank says it is conducting a full audit of its customer-facing applications to ensure proper protections are in place.