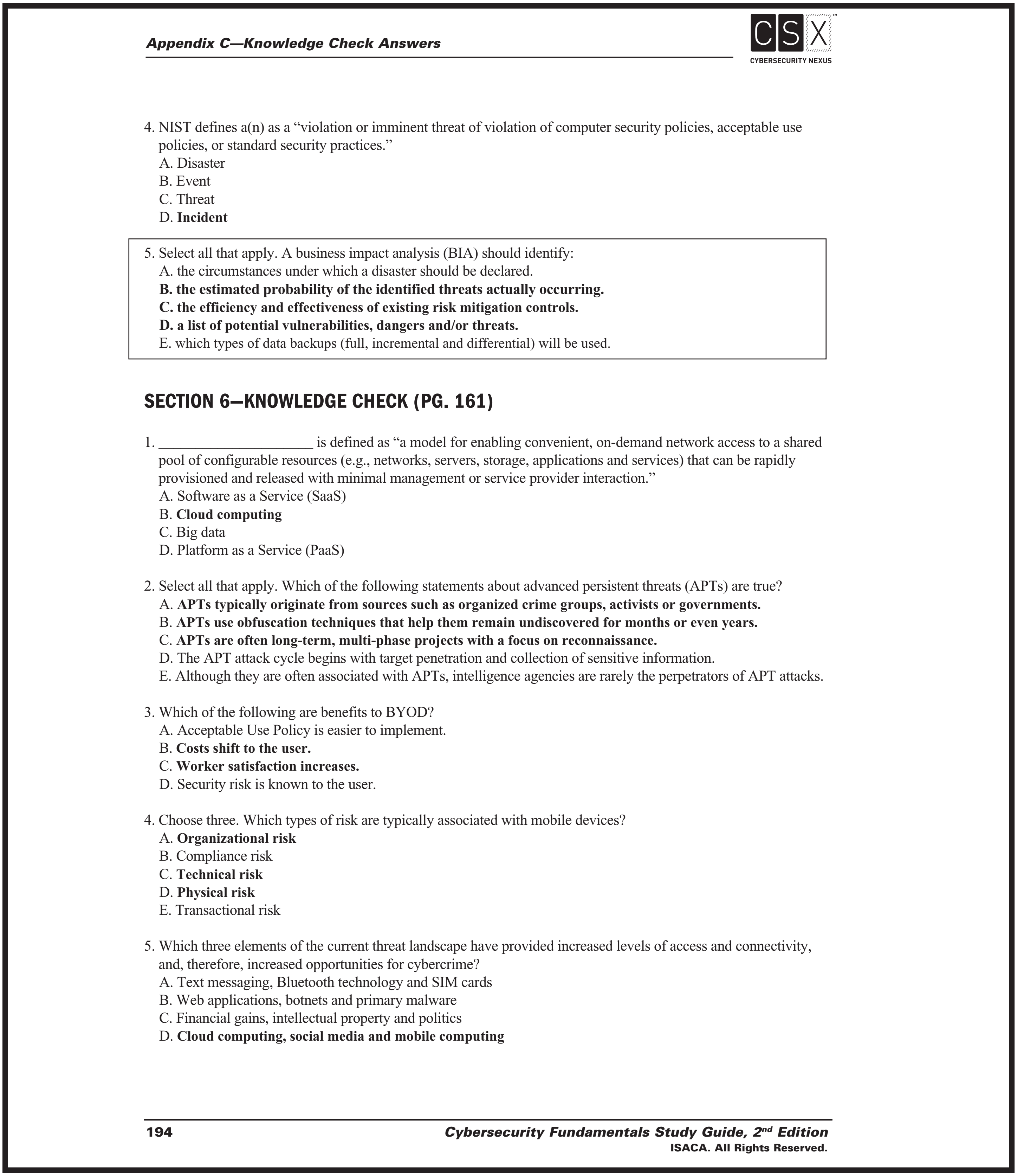
The following correction applies to page 194 of the *Cybersecurity Fundamentals Study Guide, 2nd Edition*. The justifications for question 5 have been corrected.



4. NIST defines a(n) as a "violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."
   A. Disaster
   B. Event
   C. Threat
   D. **Incident**

5. Select all that apply. A business impact analysis (BIA) should identify:
   A. the circumstances under which a disaster should be declared.
   B. the estimated probability of the identified threats actually occurring.
   C. the efficiency and effectiveness of existing risk mitigation controls.
   D. a list of potential vulnerabilities, dangers and/or threats.
   E. which types of data backups (full, incremental and differential) will be used.

SECTION 6—KNOWLEDGE CHECK (PG. 161)

1. _____________________ is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management or service provider interaction."
   A. Software as a Service (SaaS)
   B. **Cloud computing**
   C. Big data
   D. Platform as a Service (PaaS)

2. Select all that apply. Which of the following statements about advanced persistent threats (APTs) are true?
   A. **APTs typically originate from sources such as organized crime groups, activists or governments.**
   B. **APTs use obfuscation techniques that help them remain undiscovered for months or even years.**
   C. **APTs are often long-term, multi-phase projects with a focus on reconnaissance.**
   D. The APT attack cycle begins with target penetration and collection of sensitive information.
   E. Although they are often associated with APTs, intelligence agencies are rarely the perpetrators of APT attacks.

3. Which of the following are benefits to BYOD?
   A. Acceptable Use Policy is easier to implement.
   B. **Costs shift to the user.**
   C. **Worker satisfaction increases.**
   D. Security risk is known to the user.

4. Choose three. Which types of risk are typically associated with mobile devices?
   A. **Organizational risk**
   B. Compliance risk
   C. **Technical risk**
   D. **Physical risk**
   E. Transactional risk

5. Which three elements of the current threat landscape have provided increased levels of access and connectivity, and, therefore, increased opportunities for cybercrime?
   A. Text messaging, Bluetooth technology and SIM cards
   B. Web applications, botnets and primary malware
   C. Financial gains, intellectual property and politics
   D. **Cloud computing, social media and mobile computing**

ISACA®
Trust in, and value from, information systems