Quiz - What are We Talking about when We Talk about Cybersecurity

1. Which is the National Institute of Standards' (NIST) definition of cybersecurity? 1 / 1 poi

- ○ The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.
- ○ The measures taken to protect governmental and military computer and weapons systems from unauthorized use, alteration, disruption or destruction.
- ◉ The protection of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

✓ **Correct**

Correct! This is the NIST definition of cyber or information security.

2. Which three (3) are components of the CIA Triad? 1 / 1 point

- [ ] Information
- [x] Availability

✓ **Correct**

Partially correct! Availability is the "A" in CIA.

- [x] Confidentiality

✓ **Correct**

Partially correct! Confidentiality is the "C" in CIA.

- [x] Integrity

✓ **Correct**

Partially correct! Integrity is the "I" in CIA.

- [ ] Access
- [ ] Cyber

Shafayet Bhuiyan

3. "A flaw, loophole, oversight, or error that can be exploited to violate system security policy." Is the definition of which key cybersecurity term?

1 / 1 point

- (•) Vulnerability
- ( ) Threat
- ( ) Exploit
- ( ) Risk

✓ **Correct**

Correct! This is the definition of a cybersecurity vulnerability.

3. "A flaw, loophole, oversight, or error that can be exploited to violate system security policy." Is the definition of which key cybersecurity term?

1 / 1 point

- (•) Vulnerability
- ( ) Threat
- ( ) Exploit
- ( ) Risk

✓ **Correct**

Correct! This is the definition of a cybersecurity vulnerability.

Shafayet Bhuiyan

4. "An event, natural or man-made, able to cause a negative impact to an organization." Is the definition of which key cybersecurity term? 1 / 1 point

- (●) Threat
- ( ) Vulnerability
- ( ) Exploit
- ( ) Risk

✓ Correct

Correct! This is the definition of a cybersecurity threat.

5. Most cyber attacks come from which one (1) of the following sources? 1 / 1 point

- ( ) Malicious events, such as an attack orchestrated by a foreign government.
- (●) Internal factors, such as current and former employees.
- ( ) Natural factors, such as hurricanes, lightning and tornados.
- ( ) External threats, such as hackers, malware and viruses.

✓ Correct

Correct! Most cyber attacks originate with inside actors.

Shafayet Bhuiyan

6. Vulnerabilities are weaknesses in a system that can be exploited. Which are the two (2) most common ways in which vulnerabilities are introduced to a system? 1 / 1 poi

- [ ] Many vulnerabilities are inherent in a systems operating system and cannot be patched, only monitored.
- [ ] Many vulnerabilities are introduced to a system by malware such as Trojan horses.
- [x] Many systems are shipped with known and unknown security holes, such as insecure default settings.

✓ **Correct**

Partially correct! Many systems are shipped with known and unknown vulnerabilities to worry about... right out of the box!

- [x] Many vulnerabilities occur as a result of misconfiguration by the system administrator.

✓ **Correct**

Partially correct! Many vulnerabilities are introduced by inexperienced administrators who leave security holes open to exploition.

7. Which security role would be responsible for conducting information security assessments for organizations, including analyzing events, alerts and alarms? 1 / 1 poi

- (•) Information Security Analyst
- ( ) Chief Information Security Officer
- ( ) Information Security Auditor
- ( ) Information Security Architect

✓ **Correct**

Correct! It is the Information Security Analyst who conducts security assessments and analyzes all security events.

Shafayet Bhuiyan