Narrator: It's important to have a comprehensive approach to maintaining the CIA Triad: confidentiality, integrity, and availability. These are the foundations of the cybersecurity domain.

Confidentiality means that no private information has been disclosed to unauthorized individuals. We need to ensure that personally identifiable information, also known as PII, is protected. If you are part of a security team, your goal is to protect the assets or the information of large corporations or multiple individuals. For example, if you work in banking, health care or insurance companies, you have multiple personal identifiers to protect.

Integrity ensures that this information is not being corrupted or changed without the information owner's permission. It confirms that the information being maintained is complete and accurate and consistent with the legitimate use of that information.

Interfering with the integrity of information can have serious ramifications. For example, someone without authority changes someone's medical information, and now a patient may be in jeopardy because someone changed that vital information.

Our job is to maintain the security of that information so that no one, unless authorized to do so, changes any part of the information we are protecting.

Availability is critical because it is essential that authorized users have access to important information in a timely manner. Cyberattacks that disrupt services often target the availability of data. A business cannot function if its employees and customers cannot access their information in a timely manner. A ransomware attack, for example, may lock up a system and block access to vital information and services. That access will not be restored until a payment is made.