Module 1 Glossary

Estimated reading time: 4 minutes

Term	Definition
Academic pathways	The formal educational routes leading to a diploma or degree.
Attacker	An individual who identifies and exploits system vulnerabilities in an unethical manner.
CISO (Chief Information Security Officer)	The top-level executive responsible for establishing and maintaining an enterprise's security vision, strategy, and programs.
Compliance	The adherence to privacy regulations, enterprise security policies, and best practices in cybersecurity.
Cybersecurity	The practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from digital attacks.
Cybersecurity architects	They develop a comprehensive framework detailing how various security elements will interact and support each other.
Cybercrime analyst	They predict potential future attacks based on historical data and current trends and assist in developing robust defense strategies.
Cybersecurity consultant	They serve as an external expert, providing guidance and recommendations to organizations to improve their security framework and mitigate potential threats.
Cybersecurity design and implementation	The process of designing and setting up measures to protect an organization's digital assets.
Cybersecurity engineer	They design and create secure networks, systems, and application architectures.
Cybersecurity manager	They develop and implement security policies, manage a team of cybersecurity professionals, and liaise with senior management on all security-related issues.
Cybersecurity specialist	They monitor systems for potential threats, analyze and assess security breaches, and implement appropriate security measures to prevent future cyberattacks.
Encryption protocols	These are security measures implemented to protect sensitive information from unauthorized access, modification, or destruction.
Entry-level career	The starting point of a career often has lower pay and requires less experience or training.
Firewalls	The network security device monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Incident and intrusion analyst	The role is responsible for detecting and responding to cybersecurity breaches, pinpointing the source, and assessing the extent of the damage.
Incident response planning	The activities coordinated to respond to a security breach, including post-incident analysis and strategizing preventive measures.
Information assets	The data an organization uses to operate and make decisions.
IT auditor	They are responsible for critically examining and assessing an organization's IT systems, practices, and operations.
Intrusion detection systems	The advanced cybersecurity measures are implemented to detect potential threats to the organization's digital information and IT assets.
Lifelong learning	The ongoing, voluntary, and self-motivated pursuit of knowledge for either personal or professional reasons
Median	The middle number in a sorted list of numbers.
Networking	The process of interacting with others to exchange information and develop professional or social contacts.
Offensive security researcher	They identify and exploit system vulnerabilities ethically and controlled. They conduct comprehensive system analyses, document the testing process, and recommend security measures. They also educate staff on system best practices.
Penetration and vulnerability tester	They are responsible for identifying weaknesses and vulnerabilities in the system by deliberately probing and exploiting them, mimicking the actions of potential attackers.
Range	The difference between the lowest and highest values.
Security audits	The regular evaluations conducted to measure the effectiveness of the security architecture and compliance with regulations and best practices.
System analyses	The studies conducted to understand a system's function and design improvement strategies.
Vulnerabilities	The weak points in a system that malicious actors could potentially exploit.