CyberRookie CSX Fundamentals - Section 1: Cybersecurity Introduction and Overview

Quizlet

Study online at quizlet.com/_7r6ggy

1. **Cybersecurity**	The protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems
2. **Numerous factors, both internal and external, can directly impact an organization and its security needs, including:**	business plans and business environment & Available information technology, security process or systems in particular
3. **Many factors that can impact security, such as:**	Platforms and tools used, Network connectivity (internal, third-party, public), Level of IT complexity, Operational support for security, User community and capabilities, New or emerging security tools
4. **When evaluating business plans and the general business environment, consider drivers such as:**	Nature of business, Risk tolerance, Security profile, Industry trends for security, Mergers, acquisitions and partnerships, Consider type, frequency and resulting level of integration, Outsourcing services or providers
5. **Confidentiality**	protection from unauthorized access or disclosure
6. **Integrity**	protection from unauthorized modification
7. **Availability**	protection from disruptions in access
8. **In order to successfully protect their systems and information, cybersecurity professionals must**	demonstrate a high degree of situational awareness.
9. **Cybersecurity**	is a field that demands skilled professionals who possess the foundational knowledge, education and thought leadership necessary to confront the difficulties that accompany constant technological change.
10. **Cybersecurity addresses**	both internal and external threats to an organization's digital information assets by focusing on critical electronic data processes, signal processing, risk analytics and information system security engineering.
11. **Information security**	deals with information, regardless of its format—it encompasses paper documents, digital and intellectual property in people's minds, and verbal or visual communications.
12. **Cybersecurity**	is concerned with protecting digital assets—everything from networks to hardware and information that is processed, stored or transported by internetworked information systems
13. **In their cybersecurity frameworks, both the National Institute of Standards and Technology (NIST) and the European Union Agency for Network and Information Security (ENISA) have identified five key functions necessary for the protection of digital assets.**	Identify, Protect, Detect, Respond, Recover
14. **(3) three key concepts that are used to guide security policies**	Confidentiality, Integrity, Availability
15. **Loss of confidentiality can result in the following consequences:**	Disclosure of information protected by privacy laws, Loss of public confidence, Loss of competitive advantage, Legal action against the enterprise, Interference with national security
16. **Confidentiality can be preserved using the following methods:**	Access Controls, File Permissions, Encryption
17. **Loss of integrity can result in the following consequences:**	Inaccuracy, Erroneous decisions, Fraud
18. **Integrity can be preserved using the following methods:**	Access controls, Logging, Digital Signatures, Hashes, Encryptions

19.	**Loss of availability can result in the following consequences:**	Loss of functionality and operational effectiveness, Loss of productive time, Interference with enterprise's objectives
20.	**Availability can be preserved using the following methods:**	Redundancy, Backups, Access Controls
21.	**Nonrepudiation**	is when the message or info is genuine, integrity has been protected, party sending or receiving it cannot deny or repudiate that they sent or received it. Transactions that require trust, such as financial transactions and legal matters, implemented through transactional logs and digital signatures.
22.	**(Protecting Digital Assets): Identify**	is one of the five key functions necessary for the protection of digital assets when using organizational understanding to minimize risk to systems, assets, data and capabilities.
23.	**(Protecting Digital Assets): Protect**	is one of the five key functions necessary for the protection of digital assets when designing safeguards to limit the impact of potential events on critical services and infrastructure.
24.	**(Protecting Digital Assets): Detect**	is one of the five key functions necessary for the protection of digital assets when implementing activities to identify the occurrence of a cybersecurity event.
25.	**(Protecting Digital Assets): Respond**	is one of the five key functions necessary for the protection of digital assets when taking appropriate action after learning of a security event.
26.	**(Protecting Digital Assets): Recover**	is one of the five key functions necessary for the protection of digital assets when planning for resilience and the timely repair of compromised capabilities and services.
27.	**Governance**	is the responsibility of the board of directors and senior management of the organization to Provide strategic direction, Ensure that objectives are achieved, Ascertain whether risk is being managed appropriately, Verify that the organization's resources are being used responsibly
28.	**Risk management**	process by which an organization manages risk to acceptable levels. Requires the development and implementation of internal controls to manage and mitigate risk throughout the organization, including financial and investment risk, physical risk and cyberrisk
29.	**Compliance**	the act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations. It also includes voluntary requirements resulting from contractual obligations and internal policies.
30.	**Cybersecurity professional's duties**	analysis of policy, trends and intelligence. Using problem-solving and detection skills, better understand how an adversary may think or behave and possess advanced analytical capabilities. Include practitioners or part of senior management.
31.	**Cybersecurity governance**	depends on commitment, resources and responsibility for cybersecurity management, and it requires a means for the board to determine whether its intent has been met. Can be accomplished only by senior management involvement in approving policy and by appropriate monitoring and metrics coupled with reporting and trend analysis.
32.	**Board of Directors**	Members need to be aware of the organization's information assets and their criticality to ongoing business operations. Provided with the high-level results of comprehensive risk assessments and business impact analyses (BIAs), Tone at the top must be conducive to effective security governance.
33.	**Executive management**	organizational functions, resources, and supporting infrastructure are available and properly utilized to fulfill the directives of the board, regulatory compliance and other demands. Looks to the CISO or other senior cybersecurity manager to define the program. Provides education and guidance to the executive management team. Acts as an advisor.
34.	**Chief Information Security officer (CISO) or Chief Security Officer (CSO)**	the individual who oversees information security and cybersecurity varies from organization to organization

35.	**Cybersecurity manager will be responsible for**	Developing the security strategy, Overseeing the security program and initiatives, Coordinating with business process owners for ongoing alignment, Ensuring that risk and business impact assessments are conducted, Developing risk mitigation strategies, Enforcing policy and regulatory compliance.
36.	**Cybersecurity Practitioners**	security architects, administrators, digital forensics and network security specialists. Design, implement and manage processes and technical controls and respond to events and incidents. Direction, policies, guidelines, mandates and regulations set by the board of directors, executives and cybersecurity management
37.	**Cybersecurity Roles**	Board of Directors, Executive Committee, Senior Management, Cybersecurity Practitioners