CyberRookie CSX Fundamentals - Section 2: Cybersecurity Concepts

Core duty of cybersecurity	to identify, mitigate and manage cyberrisk to an organization's digital assets
Assessing risk	one of the most critical functions of a cybersecurity organization
Dependent on understanding the risk and threats an organization faces	Effective policies, security implementations, resource allocation and incident response preparedness
(3) three different approaches to implementing cybersecurity	Compliance-based, Risk-based, Ad hoc
Compliance-based	Also known as standards-based security, this approach relies on regulations or standards to determine security implementations. Controls are implemented regardless of their applicability or necessity, which often leads to a "checklist" attitude toward security.
Risk-based	relies on identifying the unique risk a particular organization faces and designing and implementing security controls to address that risk above and beyond the entity's risk tolerance and business needs.
Ad hoc	implements security with no particular rationale or criteria. Driven by vendor marketing, or they may reflect insufficient subject matter expertise, knowledge or training when designing and implementing safeguards.
Most organizations with mature security programs use a combination of these two (2) approaches.	risk-based and compliance-based
Require risk assessments to drive the particular implementation of the required controls.	Payment Card Industry Data Security Standard (PCIDSS) or the US Health Insurance Portability and Accountability Act (HIPAA).
Risk	The combination of the probability of an event and its consequence and mitigated through the use of controls or safeguards.
Threat	Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm. A potential cause of an unwanted incident
Threat source	as the actual process or agent attempting to cause harm
Threat event	as the result or outcome of a threat agent's malicious activity.
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation
Vulnerability	A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events
Residual risk	Even after safeguards are in place, there will always be this type of risk, defined as the remaining risk after management has implemented a risk response.
Inherent risk	The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)
In order to rank and prioritize threats among other existing threats	Cybersecurity professionals often analyze the threat's likelihood and impact
Qualitative rankings	most often used in cybersecurity risk assessment
Methodologies available to measure risk	Risk tolerance, Size and scope of the environment in question, Amount of data available

21. **Third-party Risk**	Cybersecurity can be more difficult to control, especially when different entities have different security cultures and risk tolerances
22. **Corporations**	have been known to breach security boundaries and perform malicious acts to gain a competitive advantage.
23. **Nation States**	often target government and private entities with a high level of sophistication to obtain intelligence or carry out other destructive activities.
24. **Hacktivists**	Although they often act independently, politically motivated hackers may target specific individuals or organizations to achieve various ideological ends.
25. **Cyberterrorists**	Characterized by their willingness to use violence to achieve their goals, frequently target critical infrastructures and government groups.
26. **Cybercriminals**	Motivated by the desire for profit, these individuals are involved in fraudulent financial transactions.
27. **Cyberwarriors**	also referred to as cyberfighters, are nationally motivated citizens who may act on behalf of a political party or against another political party that threatens them.
28. **Script Kiddies**	are young individuals who are learning to hack; they may work alone or with others and are primarily involved in code injections and distributed denial-of-service (DDoS) attacks.
29. **Online Social Hackers**	Skilled in social engineering, these attackers are frequently involved in cyberbullying, identity theft and collection of other confidential information or credentials.
30. **Employees**	Although they typically have fairly low-tech methods and tools, these dissatisfied individuals represent a clear cybersecurity risk. All of these attacks are adversarial, but some are not related to APT cyberattacks.
31. **Attack**	the actual occurrence of a threat or an activity by a threat agent (or adversary) against an asset
32. **Attack vector**	the path or route used to gain access to the target (asset)
33. **There are two types of attack vectors**	ingress and egress (also known as data exfiltration)
34. **Exploit**	takes advantage of a vulnerability
35. **Attack mechanism**	the method used to deliver the exploit
36. **Payload**	container, that delivers the exploit to the target
37. **Attack Attributes**	Attack Vector, Payload, Exploit, Vulnerability, Target (Asset)
38. **Adversarial threat event**	is made by a human threat agent (or adversary)
39. **Non-adversarial threat event**	is usually the result of an error, malfunction or mishap of some sort mishandling, wrong privileges, fire, flood, vulnerabilities in software, disk errors.
40. **Generalized Attack Process**	Perform reconnaissance, Create attack tools, Deliver malicious capabilities, Exploit and compromise, Conduct an attack, Achieve results, Maintain a presence or set of capabilities, Coordinate a campaign
41. **Perform reconnaissance**	The adversary gathers information using a variety of techniques
42. **Create attack tools**	The adversary crafts the tools needed to carry out a future attack
43. **Deliver malicious capabilities**	The adversary inserts or installs whatever is needed to carry out the attack
44. **Exploit and compromise**	The adversary takes advantage of information and systems in order to compromise them
45. **Conduct an attack**	The adversary coordinates attack tools or performs activities that interfere with organizational functions.
46. **Achieve results**	The adversary causes an adverse impact
47. **Maintain a presence or set of capabilities**	The adversary continues to exploit and compromise the system
48. **Coordinate a campaign**	The adversary coordinates a campaign against the organization
49. **Malware**	or malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations
50. **Stuxnet had three components**	a worm, link file and rootlet
51. **worm**	that carries out routines related to the payload
52. **link file**	that propagates copies of the worm

53. **rootkit**	that hides malicious processes to prevent detection
54. **Viruses**	A computer virus is a piece of code that can replicate itself and spread from one computer to another. It requires intervention or execution to replicate and/or cause damage.
55. **Network worm**	A variant of the computer virus, which is essentially a piece of self-replicating code designed to spread itself across computer networks. It does not require intervention or execution to replicate.
56. **Trojan horses**	A further category of malware is the Trojan horse, which is a piece of malware that gains access to a targeted system by hiding within a genuine application. Trojan horses are often broken down into categories reflecting their purposes.
57. **Botnets**	A botnet (a term derived from "robot network") is a large, automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as denial-of-service (DoS).
58. **More specific types of Malware**	Spyware, Adware, Ransonware, Keylogger, Rootkit
59. **Spyware**	A class of malware that gathers information about a person or organization without the knowledge of that person or organization
60. **Adware**	Designed to present advertisements (generally unwanted) to users
61. **Ransomware**	A class of extortive malware that locks or encrypts data or functions and demands a payment to unlock them.
62. **Keylogger**	A class of malware that secretly records user keystrokes and, in some cases, screen content.
63. **Rootkit**	A class of malware that hides the existence of other malware by modifying the underlying operating system.
64. **The MITRE Corporation publishes a catalogue of attack patterns known**	Common Attack Pattern Enumeration and Classification (CAPEC)
65. **Common Attack Pattern Enumeration and Classification (CAPEC)**	an abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed
66. **Advanced persistent threats**	Complex and coordinated attacks directed at a specific entity or organization. They require an enormous amount of research and time, often taking months or even years to fully execute.
67. **Backdoor**	A means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker-defined conditions.
68. **Brute force attack**	An attack made by trying all possible combinations of passwords or encryption keys until the correct one is found.
69. **Buffer overflow**	Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold
70. **Buffer overflow**	is an increasingly common type of security attack on data integrity
71. **Cross-site scripting (XSS)**	A type of injection in which malicious scripts are injected into otherwise benign and trusted web sites. An attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user
72. **Denial-of-service (DoS) attack**	An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.
73. **Man-in-the-middle attack**	An attack strategy in which the attacker intercepts the communication stream between two parts of the victim system and then replaces the traffic between the two components with the intruder's own, eventually assuming control of the communication
74. **Social engineering**	Any attempt to exploit social vulnerabilities to gain access to information and/or systems. It involves a "con game" that tricks others into divulging information or opening malicious software or programs.

75.	**Phishing**	A type of electronic mail (email) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering.
76.	**Spear phishing**	An attack where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim.
77.	**Spoofing**	Faking the sending address of a transmission in order to gain illegal entry into a secure system
78.	**Structure Query Language (SQL) injection**	According to MITRE, results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design.
79.	**Zero-day exploit**	A vulnerability that is exploited before the software creator/vendor is even aware of its existence.
80.	**Information security policies**	are a primary element of cybersecurity and governance
81.	**Information security policies**	They specify requirements and define the roles and responsibilities of everyone in the organization, along with expected behaviors in various situations.
82.	**Information security policies**	must be properly created, accepted and validated by the board and executive management before being communicated throughout the organization
83.	**Security policies**	should be an articulation of a well-defined information security strategy that captures the intent, expectations and direction of management
84.	**Security policies**	must be clear and easily understood by all affected parties
85.	**Security policies**	should be short and concise, written in plain language
86.	**Compliance documents**	such as policies, standards and procedures, outline the actions that are required or prohibited. Violations may be subject to disciplinary actions.
87.	**Policy framework**	the way that compliance documents relate to and support each other
88.	**Policy framework**	defines different types of documents and what is contained in each
89.	**Policies**	Communicate required and prohibited activities and behaviors
90.	**Standards**	Interpret policies in specific situations
91.	**Procedures**	Provide details on how to comply with policies and standards
92.	**Guidelines**	Provide general guidance on issues such as "what to do in particular circumstances." These are not requirements to be met, but are strongly recommended.
93.	**Scope of the information security policy involves**	enterprise's definition of information security, responsibilities associated with information security, vision, goals, metrics and rationale, how policy aligns with other high-level policies, Elaboration on specific information
94.	**Information security policy**	may potentially affect the security life cycle budget and cost management
95.	**Information security policy**	should be actively communicated to the entire enterprise and distributed to all employees, contractors, temporary employees and third-party vendors
96.	**Access Control Policy**	provides proper access to internal and external stakeholders to accomplish business goals.
97.	**Access Control Policy**	can be measured by Number of access violations that exceed the amount allowed, Amount of work disruption due to insufficient access rights, Number of segregation of duties incidents or audit findings
98.	**Access Control Policy**	should ensure that emergency access is appropriately permitted and revoked in a timely manner.
99.	**Access Control Policy Topics**	Physical and logical access provisioning life cycle, Least privilege/need to know, Segregation of duties, Emergency access
100.	**Access Control Policy and Personnel Information Security Policy**	meant for all corresponding business units, vendors and third parties.
101.	**Access Control Policy**	Updates and revalidation should involve HR, data and system owners, and information security.

102.	**Personnel Information Security Policy**	Execute regular background checks of all employees, Acquire information about key personnel in information security positions, Develop a succession plan for all key information security positions, Define and implement appropriate procedures for termination
103.	**Security Incident Response Policy**	definition of an information security incident, statement of how incidents will be handled, Requirements for the establishment of the incident response team,Requirements for the creation of a tested incident response plan, Incident documentation and closing
104.	**Security Incident Response Policy**	is meant for all corresponding business units and key employees.
105.	**Cybersecurity**	is a dynamic and ever-changing environment and therefore requires continuous monitoring, updating, testing, patching and changing as technology and business evolve.
106.	**Identity Management**	is comprised of many components that provide a collective and common infrastructure, including directory services, authentication services and authorization services and user-management capabilities, such as user provisioning and deprovisioning
107.	**Authorization**	process used for access control requires that the system be able to identify and differentiate among users. Access rules (authorizations) specify who can access what
108.	**Access restrictions at the file level generally include the following**	Read, inquiry or copy only, Write, create, update or delete only, Execute only, A combination of the above
109.	**Read-only access**	least dangerous type of access as long as the information being accessed is not sensitive or confidential
110.	**Access Control Lists11 (ACL)**	refer to a register of users (including groups, machines and processes) who have permission to use a particular system resource
111.	**Privileged User Management**	permits authorized users to maintain and protect systems and networks
112.	**Additional controls for privileged users**	limit by job function, background checks, additional logging, never sharing privileges, stronger passwords, reviewing accounts
113.	**Change Management**	ensure that changes to processes, systems, software, applications, platforms and configuration are introduced in an orderly, controlled manner and is not a standalone process
114.	**Configuration Management**	manage such changes and minimize their potential to disrupt operations, efficiency and profits. Also maintaining the security configurations of network devices, systems, applications and other IT resources is critically important to ensure security controls are properly installed and maintained
115.	**Benefits of a configuration management process**	verification of impact, assessment of a proposed change's risk, inspect different lines of defense, track items against baselines, insights into investigation, and version control.
116.	**Patch Management**	solutions to software programming errors.
117.	**Patching**	an important part of vulnerability management, and organizations must set up processes to identify patches that are relevant to their IT infrastructure