Healthcare Cyber In A Box - Definitions

Term	Definition	External Links
Access Control	The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Account Compromise	The malicious takeover of a computer or login account. This is often a result of a password compromise.	
Account Deprovisioning	The act of removing user access to applications, systems and or a network.	
Account Provisioning	The act of granting user access to applications, systems and or a network.	
Alerting Mechanism	A notification that a specific attack has been detected or directed at an organization's information systems.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Allowlist	A list of entities that are considered trustworthy and are granted access or privileges.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Anti-Virus and malware	A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents. Sometimes by removing or neutralizing the malicious code.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Asset	A person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Backup	A copy of files and programs made to facilitate recovery if necessary.	https://csrc.nist.gov/glossary
Blocklist	A list of entities that are blocked or denied privileges or access.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Command and Control	A method of compromise in which an attacker or cybercriminal sends commands to systems compromised by malware to move through a network or receive stolen data.	
Cybersecurity	Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Data Classification	The process of organizing data into broad categories in order to more easily locate and protect sensitive data.	
Data Flows	Diagrammatic representation of data movement to illustrate the pathways which data may move throughout networks and systems.	
Data Loss	he result of unintentionally or accidentally deleting data, forgetting where it is stored, or exposure to an unauthorized party.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Data Loss Prevention	A set of procedures and mechanisms to stop sensitive data from leaving a security boundary.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Data Loss Prevention	Detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in use (endpoint actions), in motion (network traffic), and at rest (data storage).	https://en.wikipedia.org/wiki/Data_loss_prevention_software
Decommisioning	The act of making something (laptop, server, system, etc…) inoperable	
Digital Signatures	A value computed with a cryptographic process using a private key and then appended to a data object, thereby digitally signing the data.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Email Protection Systems	Hardware or software systems put in place to protect email	
Encryption	The process of transforming plaintext into ciphertext.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Endpoint	Devices such as laptops, tablets, mobile phones, Internet-of-things devices	

Endpoint Protection Systems	Hardware or software systems put in place to protect endpoints	
Firewall	A capability to limit network traffic between networks and/or information systems.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Governance	Security governance is a process for overseeing the cybersecurity teams who are responsible for mitigating business risks. Security governance leaders make the decisions that allow risks to be prioritized so that security efforts are focused on business priorities rather than their own. They also govern the interplay of mitigating identified business risks, addressing internal and external threats, and dealing with compliance.	Definition of Security Governance - Gartner Information Technology Glossary
Identity and Access Management	The methods and processes used to manage subjects and their authentication and authorizations to access specific objects.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Incident	An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Incident Response	he activities that address the short-term, direct effects of an incident and may also support short-term recovery.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Incident Resposne Plan	A set of predetermined and documented procedures to detect and respond to a cyber incident.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Information Security Policy	An aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Intrusion Detection System	The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Intrusion Prevention Systems	The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents.	https://csrc.nist.gov/glossary
Managed Security Service	Network security services that have been outsourced to a service provider. A company providing such a service is a managed security service provider (MSSP)	https://en.wikipedia.org/wiki/Managed_security_service
Medical Device	An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is: recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. The term "device" does not include software functions excluded pursuant to section 520(o).	Per Section 201(h) of the Food, Drug, and Cosmetic Act
Mitigating Controls	Controls built to discover, reduce, or prevent risk.	

Mobile Device Management	The administration of mobile devices, such as smartphones, tablet computers and laptops. MDM is usually implemented with the use of a third-party product that has management features for particular vendors of mobile devices.	https://en.wikipedia.org/wiki/Mobile_device_management
Multifactor Authentication	A characteristic of an authentication system or an authenticator that requires more than one distinct authentication factor for successful authentication. MFA can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are	https://csrc.nist.gov/glossary
Network Access Control	A feature provided by some firewalls that allows access based on a user’s credentials and the results of health checks performed on the telework client device.	https://csrc.nist.gov/glossary
Network Monitoring	Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages or other trouble.	https://en.wikipedia.org/wiki/Network_monitoring
Network Segementation	The act or practice of splitting a computer network into subnetworks	https://en.wikipedia.org/wiki/Network_segmentation
Patching	A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it.	https://en.wikipedia.org/wiki/Patch_(computing)
Penetration Testing	An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Phishing	A digital form of social engineering to deceive individuals into providing sensitive information.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Physical Security	Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks).	https://en.wikipedia.org/wiki/Physical_security
Playbooks	A predefined guide or process which is enacted during an incident. The guide walks the reader through the predefined steps to resolve a specific incident type (e.g. a phishing playbook).	
Ransomware	Type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid.	https://en.wikipedia.org/wiki/Ransomware
Security Automation	The use of information technology in place of manual processes for cyber incident response and management.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Security Controls	Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.	https://en.wikipedia.org/wiki/Security_controls
Security Operations Center	A centralized unit that deals with security issues on an organizational and technical level.	https://en.wikipedia.org/wiki/Security_operations_center
Single Sign On	An authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.	https://en.wikipedia.org/wiki/Single_sign-on
Social Engineering	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.	https://csrc.nist.gov/glossary
Tabletop Exercise	A discussion-based exercise where personnel meet in a classroom setting or breakout groups and are presented with a scenario to validate the content of plans, procedures, policies, cooperative agreements or other information for managing an incident.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

Threat Assessment Program	he product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Vulnerability management	In the NICE Framework, cybersecurity work where a person: Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.	https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
Web Application Scanning	Using software to scan a website or application for vulnerabilities	