Kae’ce Jackson

02/23/25

CYSE 200T

Prof Bowman

What is the CIA Triad?

The CIA Triad stands for Confidentiality, Integrity and Availability. Essentially, its a model that is specifically designed to help organizations enforce policies for information security. Each of these words have a different meaning in cybersecurity than their everyday uses, and it is used to find vulnerabilities and security risks and come up with solutions to these security risks. These are essential to keep organizations safe and serve as pillars to the IT world. These three core concepts intertwine with each other in order to keep organizations safe.

Confidentiality

The C in CIA stands for confidentiality, or privacy. More specifically to cybersecurity, confidentiality measures are implemented in order to limit access to sensitive information from unauthorized individuals. Information is categorized by the severity of the aftermath should this information fall into the wrong hands, and each level will have different protocols for preventing access and dealing with them. Some actions will be more severe than others due to the sensitivity of the information leaked.

Training is essential for higher authorized personnel dealing with this sensitive information, due to how high of a priority it is. Training should include the risks, proper protocols and information to help those dealing with sensitive information. They should be able

to identify risks before it is too late, and they should also know the proper steps to take. This can include password authentication, or two factor authentication which is becoming a more normalized procedure. Two factor authentications are a security process that requires users to provide two different authentication processes. For example, when logging into ODU sites, students have to input their usernames and passwords as well as confirm on their personal cellular devices to log in successfully. This makes it so that even if someone has your password, they will not be able to log in without your device and will have to do further work on their part to get in.

Integrity

Integrity is the process of maintaining consistency and trustworthiness of data. Data must not change, and shouldn't be altered or tampered with in any way by unauthorized personnel, or a breach of confidentiality. Integrity should include permission sets, user access, and other security protocols to protect information from being altered in any way, intentional or not, by individuals who are not authorized to do so. Backups and restoration programs are essential in cases of server crashes and should provide a way to restore files to their previous forms before they were altered.

Availability

Availability means that information should be always available for authorized users. This usually means that information and systems should always be kept up to date and readily accessible to authorized users aiming to access this information. Updates for systems should

always be installed to prevent delays in accessing information and to keep systems up and running with no issues. A backup plan should be implemented in case of issues.

Authentication vs Authorization

Authentications are security protocols to help verify the identity of an individual gaining access to information. Having users prove that they are authorized to access information limits the risk of unauthorized access to sensitive information and keeps data and organizations safe. Authorizations are a set of permissions that are given to a user that grants access to certain types of information. Authentication and authorizations intertwine together in order to provide a stable security environment. An unauthorized user will not be able to authenticate themselves and access information not meant for them, and authorized users will have to prove that they are in fact the correct user requesting access to data.