"What is CYBER SECURITY?",

"CYBER SECURITY is the protection of your digital data, personal identification as well as your devices, such as phones and computers, against malicious access, alteration and denial of use. Would you like to hear about the major aspects of Cyber Security?",

"What are the major aspects CYBER SECURITY?",

"The major aspects of Cyber Security are Confidentiality, Integrity, and Availability. This is referred to as the C.I.A. Triad. Would you like to hear more?",

\*\*\*\*\*\* CIA TRIAD \*\*\*\*\*\*

"What is the C.I.A. Triad?",

"The C.I.A. TRIAD is a birds eye view on security. It addressed three broad categories: CONFIDENTIALITY, ensuring your data is private; INTEGRITY, ensuring your data is not altered; and AVAILABILITY, ensuring your data is available for authorized use. You can ask me about any of these. For a more in depth analyses of CYBER SECURITY, ask me about the X.8.0.5 FRAMEWORK.",

"Tell me more about Confidentiality.",

"CONFIDENTIALITY is the safeguard of your system against unauthorized access. Your system would include data, applications, the supporting services, devices and the identification of both users and as well as your infrastructure. Any attack in which an unauthorized user gains access to your information or systems would be a breach in CONFIDENTIALITY.",

\*\*\*encryption

"Tell me more about INTEGRITY.",

"INTEGRITY is the notion that the data you are sending and receiving has not been maliciously modified or altered in any way. Events that would effect INTEGRITY would be man in the middle attacks, where information is intercepted in transit and altered, or an attack against a database where customers' records such as invoices and balances, are altered. Breaches of INTEGRITY generally breach CONFIDENTIALITY as well.",

\*\*\*hashing

"Tell me more about AVAILABILITY.",

"AVAILABILITY is the idea that data and devices must be available to authorized users. Events that would effect AVAILABILITY include denial of service attacks.",

\*\*\*\*\*\* X.8.0.5. \*\*\*\*\*\*

"What is the X.8.0.5. FRAMEWORK?",

"The X.8.0.5. FRAMEWORK is an intricate method in which security can be managed. X.8.0.5. analyzes eight SECURITY DIMENSIONS across 3 SECURITY LAYERS and 3 SECURITY PLANES for a total of 72 points of analyses. 5 MAJOR THREATS are reviewed against each of the 72 points of analyses when applicable. You can ask me about any of these.",

"What are the SECURITY DIMENSIONS?",

"The eight SECURITY DIMESNIONS of the X.8.0.5. FRAMEWORK are: ACCESS CONTROL, AUTHENTICATION, NON-REPUDIATION, DATA CONFIDENTIALITY, COMMUNICATION SECURITY, DATA INTEGRITY, AVAILABILITY, and PRIVACY. You can ask me about any of these.",

\*\*\*\*\*\* LAYERS \*\*\*\*\*\*

"What are the SECURITY LAYERS?",

"The Security Layers are: INFRASTRUCTURE, SERVICES and APPLICATIONS. These represent the hierarchy of physical and digital systems. You can ask me about any of these.",

"What is the INFRASTRUCTURE layer?",

"The INFRASTRUCTURE LAYER consists of the physical hardware in which you information reside.

"What is the SERVICES LAYER?",

"The SERVICES LAYER include the software which provide the background support towards APPLICATIONS and the END USER.",

"What is the APPLICATIONS LAYER?",

"The APPLICATIONS LAYER is focused on the actual programs utilized by END USERS",

"What are the SECURITY PLANES?",

"The SECURITY PLANES are MANAGEMENT, CONTROL and END-USER. These address the different types and cases of users. You can ask me about any of these.",

"What is the MANAGEMENT PLANE?",

"The MANAGEMENT PLANE is the concerned with the administrative and operations of the system as a whole.",

"What is the CONTROL PLANE?",

"The CONTROL PLANE is concerned with communications between networks and devices, also called signaling information."

"What is the END-USER PLANE?",

"The END-USER PLANE is access and utilization of the system by customers, employees, family etc.",

\*\*\*\*\*\* SECURITY DIMENSIONS \*\*\*\*\*\*

"What is ACCESS CONTROL?",

"ACCESS CONTROL refers to the prevention of unauthorized access, management and use of network resources.",

"What is AUTHENTICATION?",

"AUTHENTICATION is the confirmation of all entities within the system including, users, devices, services and software."

"What is NON-REPUDIATION?",

"NON-REPUDIATION is the means in which changes and access are recorded to ensure the identity of the system, user or administrator who made the changes. This provides accountability for actions."

"What is Data Confidentiality?",

"Data Confidentiality is the protection from unauthorized access to information.",

"What is Communication Security?",

"Communication Security is the end to end protection of the movement of data.",

"What is DATA INTEGRITY?",

"DATA INTEGRITY measures the accuracy of data and protection against unauthorized modification.",

"What is AVAILABILITY?",

"AVAILABILITY is the assurance of access to authorized users.",

"What is PRIVACY?",

"Privacy refers to the safeguard of identifying information across INFRASTRUCTURE, SERVICES, and APPLICATIONS.",

\*\*\*\*\*\*\*MAJOR THREATS\*\*\*\*\*\*

"The MAJOR THREATS in CYBER SECURITY are Destruction of information or resources, Corruption or modification of information, Theft and removal or loss of information or other resources, Disclosure of private information and Interruption of services.",