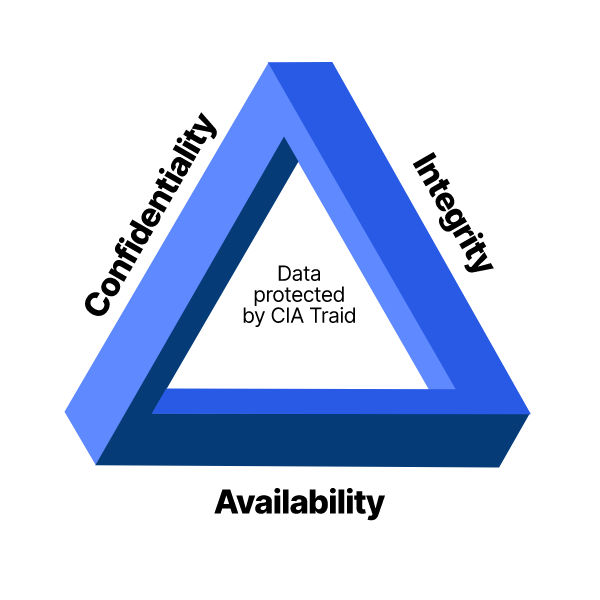
**Unit 3 Approaches to Cyber Security Design**

The CIA triad refers to an information security model made up of the three main components: confidentiality, integrity and availability. Each component represents a fundamental objective of information security



Network security refers to the various countermeasures put in place to protect the network and data stored on or passing through it. Network security works to keep the network safe from cyberattacks, hacking attempts, and employee negligence. There are three components of network security: hardware, software, and cloud services.

Hardware appliances are servers or devices that perform certain security functions within the networking environment. Hardware can be installed out of the path of network traffic, or “out-of-line,” but it’s more commonly installed in the path of traffic, or “in-line.” The advantage of this is that in-line security appliances are able to stop data packets that have been flagged as potential threats, whereas out-of-line appliances simply monitor traffic and send alerts when they detect something malicious. Network security software, which includes antivirus applications, can be installed on devices and nodes across the network to provide added detection and threat remediation.

Cloud services refer to offloading the infrastructure to a cloud provider. The set-up is generally similar to how network traffic passes through in-line hardware appliances, but incoming network traffic is redirected to the cloud service instead. The cloud service does the work of scanning and blocking potential threats for you before the traffic is allowed onto your network.

Every good network security system uses a combination of different types of network security tools to create a layered defense system. The theory behind this strategy is that if a threat manages to slip past one security countermeasure, the other layers will prevent it from gaining entry to the network. Each layer provides active monitoring, identification, and threat remediation capabilities in order to keep the network as secure as possible

What are the different types of network security devices and tools?

There are quite a few different networking security tools you can incorporate into your line-up of services. The following list is by no means exhaustive, but available security tools can include:

Access control. This refers to controlling which users have access to the network or especially sensitive sections of the network. Using security policies, you can restrict network access to only recognized users and devices or grant limited access to noncompliant devices or guest users.

Antivirus and anti-malware software. Malware, or “malicious software,” is a common form of cyberattack that comes in many different shapes and sizes. Some variations work quickly to delete files or corrupt data, while others can lie dormant for long periods of time and quietly allow hackers a back door into your systems. The best antivirus software will monitor network traffic in real time for malware, scan activity log files for signs of suspicious behavior or long-term patterns, and offer threat remediation capabilities.

Application security. Each device and software product used within your networking environment offers a potential way in for hackers. For this reason, it is important that all programs be kept up-to-date and patched to prevent cyberattackers from exploiting vulnerabilities to access sensitive data. Application security refers to the combination of hardware, software, and best practices you use to monitor issues and close gaps in your security coverage.

Behavioral analytics. In order to identify abnormal behavior, security support personnel need to establish a baseline of what constitutes normal behavior for a given customer’s users, applications, and network. Behavioral analytics software is designed to help identify common indicators of abnormal behavior, which can often be a sign that a security breach has occurred. By having a better sense of each customer’s baselines, MSPs can more quickly spot problems and isolate threats.

Data loss prevention. Data loss prevention (DLP) technologies are those that prevent an organization’s employees from sharing valuable company information or sensitive data—whether unwittingly or with ill intent—outside the network. DLP technologies can prevent actions that could potentially expose data to bad actors outside the networking environment, such as uploading and downloading files, forwarding messages, or printing.

Distributed denial of service prevention. Distributed denial of service (DDoS) attacks are becoming increasingly common. They function by overloading a network with one-sided connection requests that eventually cause the network to crash. A DDoS prevention tool scrubs incoming traffic to remove nonlegitimate traffic that could threaten your network, and may consist of a hardware appliance that works to filter out traffic before it reaches your firewalls.

Email security. Email is an especially important factor to consider when implementing networking security tools. Numerous threat vectors, like scams, phishing, malware, and suspicious links, can be attached to or incorporated into emails. Because so many of these threats will often use elements of personal information in order to appear more convincing, it is important to ensure an organization’s employees undergo sufficient security awareness training to detect when an email is suspicious. Email security software works to filter out incoming threats and can also be configured to prevent outgoing messages from sharing certain forms of data.

Firewalls. Firewalls are another common element of a network security model. They essentially function as a gatekeeper between a network and the wider internet. Firewalls filter incoming and, in some cases, outgoing traffic by comparing data packets against predefined rules and policies, thereby preventing threats from accessing the network.

Mobile device security. The vast majority of us have mobile devices that carry some form of personal or sensitive data we would like to keep protected. This is a fact that hackers are aware of and can easily take advantage of. Implementing mobile device security measures can limit device access to a network, which is a necessary step to ensuring network traffic stays private and doesn’t leak out through vulnerable mobile connections.

Network segmentation. Dividing and sorting network traffic based on certain classifications streamlines the job for security support personnel when it comes to applying policies. Segmented networks also make it easier to assign or deny authorization credentials for employees, ensuring no one is accessing information they should not be. Segmentation also helps to sequester potentially compromised devices or intrusions.

Security information and event management. These security systems (called SIEMs) combine host-based and network-based intrusion detection systems that combine real-time network traffic monitoring with historical data log file scanning to provide administrators with a comprehensive picture of all activity across the network. SIEMs are similar to intrusion prevention systems (IPS), which scan network traffic for suspicious activity, policy violations, unauthorized access, and other signs of potentially malicious behavior in order to actively block the attempted intrusions. An IPS can also log security events and send notifications to the necessary players in the interest of keeping network administrators informed.

Web security. Web security software serves a few purposes. First, it limits internet access for employees, with the intention of preventing them from accessing sites that could contain malware. It also blocks other web-based threats and works to protect a customer’s web gateway.