Security Principles and Foundations Summative Assessment

**Part 1:**

**Explain why applying each of the security principles discussed in this module, including Defense in Depth, Isolation, Simplicity of Design, Least Privilege, Fail-Safe Defaults, and Complete Mediation would contribute to minimizing the likelihood that a healthcare organization would be victimized by these kinds of attacks. Your answers should demonstrate of clear understanding of each of these principles and the impact of applying them in a healthcare setting.**

**Defense in Depth:**

**Defense-in-Depth is a concept that no single protection mechanism will provide complete protection. By layering protection mechanisms, the thought is that if an intruder gets beyond one level, they may be stopped at the next level.**

**Install a Firewall after the router, Scan all incoming and outgoing emails to detect and filter threats, such as phishing and spoofing emails, and executable files, Restrict user permissions for installing and running software applications. Make sure operating systems, antivirus and anti-malware software and signatures are up to date with the latest patches. Maintain offline, encrypted backups of data and to regularly test their backups. All of these precautions could have stop the Ransomware Hackers from succeeding.**

**Isolation:**

**Isolation compartmentalizes processes and isolates them from each other. This principle limits the interactions between processes and modules. For example, having a virtual machine running within a host operating system, isolates the virtual machine from the host system. A virtual machine allows you to run an operating system within an operating system on a single host computer. If malware were to infect the virtual machine, there should be little to no effect on the host system.**

**Simplicity of Design:**

**The Simplicity of Design principle allows network administrators to easily and quickly identify possible paths for intruders to access files from the system.**

**Most Healthcare networks I've worked with have their database offsite as the main hub, this site scans all incomming Data requests, incomming and outgoing of data transfers. only one way in.**

**All secondary sites and the network within have a specific IP range , this allows IT to pin point the compromised site and slow or stop the intrusion.**

**Least Privilege:**

**The Least Privilege principle involves only providing users with the privileges they need to perform their job. Restricting user permissions for installing and running software applications will cut down on unconsciously installing harmful and malicious programs.**

**Fail-Safe Defaults:**

**Principle of Fail-Safe Defaults denies access to any and all objects unless specific permissions have been enabled to provide a user access to the object. Meaning, by default, all permissions are set to the “deny” setting. Restricting all eMail attachments can stop harmful programs from entering the network.**

**Complete Mediation:**

**Complete Mediation restricts the caching of information. By implementing this principle, each time a user attempts to access an object within the network, the system has been configured to verify the user is authenticated to use that object. If user privileges have been cached, authentication would only take place initially, not every time. Putting a password protected rule on computers asking for Admin rights to open attachments or install a program will stop the spread of harmful software.**

**Part 2:**

**Describe what healthcare organizations should do at each stage of the Security Life Cycle to minimize the likelihood of being victimized by these kinds of attacks.**

**Identify:**

**Servers, routers, firewalls ( make sure firewall and their rules have been created to protect the site)**

**Operating systems ( update all OS to the lastest Patches )**

**Applications/Software ( update all firmware and back up all data for Applications/Softwares)**

**Assess:**

**perform a security assessment of equipment and employee knowledge of Cyber threats, educate the empolyees and secure comprromised equipments**

**Protect:**

**Here we attempt to mitigate the risks identified in the assessment phase. This is where we implement changes necessary to increase security for any identified issues.**

**if workers are unconsciously clicking on attachments in their eMails, Restrict or deny all incomming attachments.**

**Monitor:**

**The last phase of the cycle is to monitor the modifications made in the protection phase. Monitor all Work related devices, Sometimes work Phones are handed out in somecases workers can click on a link from a text message that can install harmful apps.**

**Part 3:**

**What is usually the weakest link in any healthcare organization’s security plan? Describe how education and continual training can be used to keep the initial stages of a ransomware attack from occurring.**

**People are the weakest link in the cybersecurity Chain. Policies and standards form the heart of the cycle and provide the structure required for the processes. If there are no Policies or Standards for Employees in reguards to Cyber Security than cybercriminals will exploit simple human error. Educating Healthcare Staff of Well-researched, targeted, legitimate-looking emails that are aimed at them attempting to solicit a reaction: a click of a link, an opening of an attachment, or persuading them to divulge credentials or other sensitive information. Send a Mock up test to employees eMails to help educate them on what to look for.**