Ydali Hernandez

C202406

Activity 4.

iSeeU Eyecare

1. **Using the 7 IT domains, select ALL the domains your company utilizes. Next, describe why you selected each of the domains (how does your company utilize them).**
    1.1. User domain: iSeeU eyecare employees, including optometrists, administrative staff, and IT personnel, authenticate to access patient records, scheduling systems, and other sensitive information. Each user has a unique credential and access level based on their role within the company

    1.2. Workstation domain: the company uses multiple computers and workstations for daily operations such as scheduling appointments, processing payments, and managing patient data. These systems need to be secure and efficient to ensure smooth business operations.

    1.3. LAN domain: Both Orlando and Tampa stores have a local area network (LAN) to connect their computers, printers, and other devices. The LAN supports internal communication and resources sharing within each store

    1.4. LAN-to-WAN domain: the Tampa store connects to the Orlando store's servers via a VPN, facilitating secure data transmission between locations. This connection is critical for accessing centralized patient records and other shared resources.

    1.5. WAN domain: iSeeU Eyecare utilizes the internet for various operations, such as accessing third-party insurance portals, cloud-based services, and external communications. Ensuring secure and reliable WAN connectivity is vital for business continuity.

    1.6. Remote Access domain: the VPN setup for the Tampa store falls under this domain, allowing secure remote access to the servers located in Orlando. This infrastructure supports remote work and ensures that staff can access necessary systems from different locations.

1.7. System/Application domain: the company uses various applications for patient management, electronic health records (EHR), and financial transactions. These systems must be secure and regularly updated to protect sensitive patient information and ensure regulatory compliance.

2. **Using the selected domains from item 1 above, select the two most important domains your company needs to address. Describe why each of the two domains you selected is the two most important.**

2.1. User Domain: the user domain is critical because it involves the primary interface between employees and the company's systems. Proper authentication and access control measures are essential to prevent unauthorized access to sensitive patient data and maintain the integrity of the information systems. Ensuring that users follow best practices in security can significantly reduce the risk of data breaches and other security incidents.

2.2. Lan-to-WAN domain: is crucial for maintaining secure and reliable communication between the Orlando and Tampa stores. This domain is pivotal for seamless data sharing and operational continuity between the two locations. Any vulnerabilities or failures in this domain could disrupt business operations, hinder access to critical data, and potentially expose sensitive information to external threats. Ensuring robust security measures and reliable connectivity in this domain is essential for the company's overall operational effectiveness and security posture. These two domains are fundamental because they directly impact the security and efficiency of daily operations and the protection of sensitive patient information, which is vital for maintaining compliance with healthcare regulations and ensuring patient trust.

3. **Using the 7 IT domains, what domains will NOT be as important for your company if Zero Trust was implemented? Describe why they will NOT be as important for your company.**

3.1. Workstation domain: in a Zero Trust model, the security emphasis shifts from the individual workstations to the overall security posture of the network and its resources. Each access request is verified regardless of the device's location or status, making the specific security measures on individual workstations less critical. Security policies, such as endpoint security and application whitelisting, would still be essential but not as central as the constant verification of user and device trust levels. The security focus is on continuous verification of user identity and device health, making the individual workstation's security less crucial. Zero

Trust ensures that even if a workstation is compromised, it cannot access critical resources without proper verification.

3.2. LAN domain: with Zero Trust, the traditional perimeter-based security model becomes less relevant. Instead, security controls focus on individual resources and data within the network. This means that the specific configuration and security of the local area network are less critical because every interaction within the network is authenticated and verified. The internal network's security boundaries are de-emphasized in favor of protecting individual resources and data access points. The LAN's traditional role of providing a secure internal network is diminished as Zero Trust assumes no inherent trust within the network. Every device and user action are subject to verification, reducing the need for strict internal network segmentation and controls.

3.3. WAN domain: similar to the LAN domain, the WAN domain's importance diminishes because Zero Trust principles treat internal and external traffic with the same level of scrutiny. The focus is on securing data and applications rather than the connections themselves. Every access attempt, whether from within the WAN or outside, undergoes the same rigorous verification process, making the WAN's specific security measures less significant. The WAN's importance is reduced because Zero Trust does not distinguish between internal and external network traffic. Security measures are applied uniformly, ensuring that all access requests are treated with equal scrutiny, regardless of their origin.

4. **Using the Compliance and Audit video, the slide entitled "Other Types of Supporting Documents," AND the Information Gathering and Reporting video slide entitled "Digital Forensics Reporting," what three documents listed or mentioned are the most important documents you would deliver for:**

4.1. **Ransomware case to a digital forensics investigator? Describe why each of the selected items is the most important document.**

4.1.1. Network Architecture Diagrams: are essential because they provide a visual representation of the network's structure, including all devices, connections, and pathways. In a ransomware investigation, these diagrams help forensic investigators understand how the ransomware spread through the network, identify vulnerable points, and determine how different systems were affected. This information is vital for implementing effective containment measures and for planning the recovery process.

4.1.2. System Log files: are crucial as they provide a detailed account of activities and events on the network and systems. For a ransomware case, these logs can help trace the point of entry, the actions performed by the ransomware, and any anomalous behavior that could indicate how the system was compromised. They also assist in understanding the timeline of the attack, which is critical for both containment and remediation efforts.

4.1.3. Vendor Documents and Agreements: are important because they contain details about the software, hardware, and services provided by third parties. These documents can include information about security measures, service level agreements, and responsibilities of the vendors. In a ransomware case, understanding the role and security practices of vendors can help identify if a third-party service was the attack vector and assess compliance with security policies and contractual obligations.

4.2. data breach case to a digital forensics investigator? Describe why each of the selected items is the most important document.

4.2.1. System Log Files: are essential because they provide a comprehensive record of all activities within the system, including user logins, access to sensitive data, and any suspicious or unauthorized actions. These logs help forensic investigators identify the point of breach, understand the methods used by attackers, and determine the extent of the compromised data. By analyzing these logs, investigators can trace the attackers' steps, establish a timeline of events, and assess the overall impact of the breach.

4.2.2. Network Architecture Diagrams: are critical because they offer a visual representation of the network's structure, including all connected devices, communication pathways, and data flows. In a data breach investigation, these diagrams help forensic investigators understand how the network is laid out, identify potential vulnerabilities, and determine how the attackers moved laterally through the network. This knowledge is vital for pinpointing entry points, understanding the attacker's path, and implementing effective containment and remediation strategies.

4.2.3. Security Plan: outlines the organization's cybersecurity policies, protocols, and procedures for protecting data and systems. It includes details on access controls, encryption methods, and incident response strategies. For a data breach investigation, the security plan helps forensic investigators assess the existing security measures, identify any gaps or weaknesses that were exploited, and evaluate the effectiveness of the organization’s response to the breach. Understanding the security plan provides insights into how well the organization was prepared for such incidents and what improvements are necessary to prevent future breaches.