Andree Salvo

Southern New Hampshire University

3-1 Journal: Audit and Assessment of Users, Workstations, and LANs

Instructor: Robert Chubbuck

Conducting audits on users, workstations, and LANs is essential as each presents distinct risks to an organization's security framework. For example, **Users** often represent the most vulnerable aspect of cybersecurity due to human mistakes, weak passwords, and a lack of security awareness, which can result in unauthorized access or data breaches inside the organization. Regular audits of user activities help detect unusual behavior, enforce the principle of least privilege, and ensure that accounts are promptly deactivated when employees leave. For workstations, audits are crucial to verify that devices are being securely patched, updated, and properly configured. Without proper oversight, endpoints may become susceptible to malware, outdated software, or misconfigurations that attackers could exploit. Adhering to security policies at both the user and workstation levels establishes a robust initial defense line.

However, auditing the LAN is equally important, as it links users and workstations and is frequently targeted by attackers seeking entry points. Observing LAN activity can reveal irregular traffic patterns, unauthorized devices, or improper protocol usage, which may indicate intrusions or insider threats. These audits also enable organizations to enhance network performance by pinpointing bottlenecks or inefficiencies, and by boosting both security and usability. In essence, conducting regular audits across all three environments, like users, workstations, and LANs, helps organizations demonstrate compliance with regulatory standards such as HIPAA, PCI-DSS, or NIST frameworks. When auditing at these levels, companies not

only reduce risks but also sustain a reliable and efficient computing environment for the organization.