Strategic Networking Infrastructure for Remote Workforce Enablement

Jayanti Saha

Westcliff University

MIS500/263-SMC-A: Santa Monica Combined - Spring 2026 - Session 3

Professor Thullen

January 19, 2026

Strategic Networking Infrastructure for Remote Workforce Enablement

The COVID-19 Pandemic has caused a paradigm shift in the way organizations view workforce mobilization, with the latter identifying networking infrastructure deficiencies that most organizations did not expect or plan for in their telecommunications networking infrastructure plans and solutions. In the case of a regional healthcare-related billing company that currently supports approximately 175 employees in its brick-and-mortar and three satellite offices, an abrupt shift to telework accessibility as caused network telecommunications-related deficiencies that currently haunt such SME organizations in determining which telecommunications solutions will best support their business in wiring their infrastructure or going wireless and which telecommunications solutions will best support their business in securing access to their sensitive patient billing information in these telecommunications and computer networking solutions and infrastructure plans and implementations in an ever-changing global economy that includes but is not limed to COVID-19 that has reshaped several ways in many organizations around the world today.

Physical Wiring Versus Wireless Infrastructure Focus

The hybrid approach by the healthcare billing company should emphasize wireless connectivity and the maintenance of strategic physical wiring for critical infrastructure components and high-security zones. This recommendation is a function of the fact that post-pandemic business operations will require flexibility for both on-premises and remote work arrangements, thereby necessitating the implementation of wireless infrastructure to facilitate employee mobility and adaptation. However, operating solely on wireless networks would introduce unnecessary security risks for an organization handling protected health information

under HIPAA regulations and performance bottlenecks in bandwidth-intensive operations such as video conferencing and transferring large files.

The wireless-first strategy should emphasize the deployment of enterprise-grade WIFI 6 access points across office locations to offer high-speed connectivity that supports multiple simultaneous connections from laptops, smartphones, and tablets without performance degradation. As explained by Cisco in their guidelines about wireless networking in 2023, new WIFI 6 grants much higher capacity with lower latency and better performance in interference-prone environments than its predecessor WIFI standards, thus making it suitable for business-critical applications. The billing company should implement zones of WIFI coverage to let employees move freely within the conference, collaborative work areas, and individual offices while having secure connections to billing systems and electronic health record platforms. This wireless infrastructure also provides the foundation that will support bringing your own device policies, where employees use personal smartphones and tablets for work purposes, thereby reducing hardware costs while accommodating diverse technology preferences.

However, physical wired networks are still required in scenarios where the use of wireless technology may create unacceptable levels of security and performance risks. The company should keep Ethernet links for server rooms where billing databases and application servers are located, as well as for networking closets where routers and switches are placed, as well as for billing specialists' working stations where a high volume of claims needs to be processed in a short time using a stable, always-connected network. Cables will help the company create a redundant connection in case of a wireless network failure to create a segmented network for secure systems that are isolated from the normal wireless networks used by ordinary employees. According to Tanenbaum and Wetherall (2021), wired Ethernet is the

superior networking technology in terms of reliability, security, and performance, at least for non-mobile equipment, because of the additional costs associated with wired networking compared to the available wireless alternatives.

Essential Telecommunications and Networking Components

For the healthcare billing firm to enable secure remote access to its business resources and protected health information, it must establish a full technology solution set that entails virtual private networking, next-generation firewalls, multi-factor authentication technologies, endpoint security software, and secure cloud infrastructure. The backbone for establishing secure remote access must begin with a full-featured VPN solution that enables the establishment of secure, encrypting tunnels from remote employee machines to the enterprise network, ensuring that confidential billing information sent over public internet infrastructures is safely insulated from interception. The use of SSL VPN technology must be preferred to traditional IPsec VPN technology for several compelling reasons, mainly because it is more compatible with a variety of home networking infrastructures, can function correctly under most configurations of firewalls without requiring cumbersome port-forwarding processes, and enables finely-tuned access controls to allow users to access solely the applications and associated data they require for the execution of their work roles.

The VPN network should be routed through a next-generation firewall that allows for deep packet inspection, intrusion prevention systems, application filtering at the application layer, and integration with threat Intelligence systems for detection and prevention of sophisticated cyber threats against the healthcare delivery sector. The solutions provided by manufacturers such as Palo Alto Networks, Fortinet, or Cisco provide next-generation threat management solutions that integrate standard firewall elements with advanced firewall solutions

such as malware protection, URL filtering, and data loss protection. These next-generation firewall solutions can inspect both the header and the payload of network traffic packets and make decisions beyond the standard network header reviews as done by the older firewall systems and can inspect for threats such as encrypted malicious payloads and command and control traffic from compromised endpoints (Stallings and Brown, 2018). The firewall should implement network segmentation that segments the billing database servers in a different VLAN from the office network to prevent the damage potential of individual system breaches.

Multi-factor authentication is yet another important element that the billing company must put in place before granting remote access for systems holding protected health information. In MFA, two or more factors must be provided for a user seeking access into systems or services. Such factors include something that the user knows (passwords or answers) or something the user possesses (smartphone authentication app/iPhone hardware token). This form of security is quite exemplary in preventing attacks targeting two-factor authenticated systems where attackers using breached passwords from data breaches or phishing discard security measures in place for systems of large corporations. Microsoft indicates that MFA prevents over 99.9% of account compromise attacks (Microsoft, 2023). The billing company should apply MFA in technology systems that need remote access through cloud services used by workers.

Lastly, the organization requires endpoint security tools such as antivirus software, endpoint response tools, and mobile device management solutions for safeguarding and managing the laptops and mobile devices personnel utilize to connect to business resources from home offices and distant sites. Such endpoint solutions should enable security policies such as disk encryption, automated security updates, screen lock timeout policies, and remote wipe

features which enable administrators of business information technology to wipe out business data on the lost or stolen devices. Cloud-enabled endpoint management solutions such as Microsoft Intune or VMware Workspace ONE will enable the billing company administration to monitor and manage company and employee-owned devices centrally and remotely and enforce security compliances without necessarily having devices brought to the office for configuration.

Security Challenges in Supporting Remote Access

The healthcare billing firm is faced with many interrelated security risks in providing remote connectivity to employees working with safeguarded health information from their home networks and personal computers. The most basic risk is in securing the devices used by employees to connect to corporate infrastructure because laptops, tablets, and smartphones being used to connect to corporate infrastructure are no longer in controlled office settings where in-house information technology personnel could monitor their current state of protections in real-time to address any incidents in a prompt manner. Employees using their home offices are accessing corporate infrastructure using consumer internet service providers whose routers are rarely upgraded in terms of security updates, have shared network segments with gaming consoles and smart home electronics owned by family relatives, and possibly lack direct office protection to safeguard computers from unauthorized users simply walking away momentarily.

Social engineering attacks and phishing campaigns represent an escalated threat in remote work environments where employees lack the informal security awareness reinforcement that occurs when colleagues can observe and question suspicious activities. Attackers specifically target remote workers with emails and phone calls impersonating IT help desk staff requesting passwords or tricking employees into installing malware disguised as legitimate software updates. The distributed nature of remote work makes these attacks more difficult to

detect and contain because compromised credentials or devices may go unnoticed for extended periods without the behavioral anomaly detection that occurs when coworkers notice unusual activities. As Hadnagy (2018) documents in his analysis of social engineering threats, remote work environments create psychological conditions that make employees more susceptible to manipulation, including isolation from colleagues who might challenge suspicious requests, time pressure to resolve technical issues without walking to an IT support desk, and reduced awareness of security risks when working in familiar home environments.

The risks of data exfiltration are further elevated when considering that staff is accessing identifiable billing information from their own personal devices and home networks where the company has little technical control over the storage, transmission, and exchange of this information. This could include staff unintentionally storing protected health information in personal cloud-based services such as Dropbox or Google Drive, emailing sensitive information to personal email services for convenience purposes, or having billing information exposed on shared computers in the home that are accessible by family members. The poor handling of data in this way can have serious implications for HIPAA compliance for the company when protected health information is mishandled and becomes unnecessarily exposed.

The firm is also required to mitigate insider threats, which become harder to mitigate with remote work conditions, as this setup eliminates the usual observation benefits inherent in shared office settings. Angry employees with financial problems might use their privileges to steal billing information to sell to identity thieves or to rivals and commit other types of billing fraud such as changing billing information to conceal past fraudulent activities or/system sabotage due to work-related grievances. The billing firm will require advanced data loss prevention capabilities, user behavior analysis, and data access analytics to help detect unusual patterns such as unusual database queries, out-of-hour access to secured systems, and large downloads of data, which might be indicators of insider threats warranting investigations.

References

1. Cisco. (2023). *WiFi 6 (802.11ax) solution overview*. https://www.cisco.com/c/en/us/solutions/enterprise-networks/802-11ax-solution/index.html
2. Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.
3. Microsoft. (2023). *Your Pa$$word doesn’t matter*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/
4. Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.
5. Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer networks* (6th ed.). Pearson.