

Instructional Scenario

Network Security Audit: Securing the Small Business Backbone



Course/Duty Area: Cybersecurity Fundamentals/Examining Computer Networks as a Foundational Element of Cybersecurity

Scenario:

A local, family-owned architecture firm, ArchitekPro, recently expanded its operations into a new office space. They have a mix of wired and wireless devices, including servers, desktop workstations, and employees' bring-your-own-device (BYOD) laptops. However, they have not established a formal network design or security policy. The firm handles sensitive client blueprints, financial data, and personally identifiable information (PII) for their 15 employees. They have hired your team, the newly formed Cyber Defense Unit (CDU), to perform a foundational network security audit.

Your primary goal is to analyze their network needs, recommend a secure network structure (including a conceptual model like the OSI Model), and outline a policy to mitigate network-based vulnerabilities and threats. You must explain to the non-technical firm partners why a strong, well-understood network foundation is the absolute first step in cybersecurity.

Big Question:

How can a well-designed and secure computer network serve as the foundational element to protect a small business's sensitive data against common cyber threats and vulnerabilities?

Focused Questions:

- How do the basic components of a network (e.g., switches, routers, firewalls) work together, and what security role does each component play?
- How would you use the OSI model to explain the functions and potential vulnerabilities of common networking protocols (e.g., HTTP, FTP, TCP/IP) to the non-technical partners?
- Based on the firm's need for security and mobility, what are the primary advantages and disadvantages of using a wired network vs. a wireless network, and what is your final recommendation for their office?
- What are three specific cyber risks associated with allowing the employees' personal devices (BYOD) onto the corporate network, and what is one policy recommendation to mitigate each risk?

Student Project or Outcome:

Students will submit a formal cyber network audit report and presentation that includes

- a labeled network diagram illustrating the recommended physical and logical topology
- an explanation of the roles of key networking components and protocols in securing the network
- a section comparing wired and wireless networks and justifying the final network choice
- a draft BYOD security policy that outlines risks and acceptable usage rules.

Project-Based Assessment:

A grading rubric will be used to evaluate the clarity and technical accuracy of the audit report, particularly the correct identification of networking protocols and security measures related to the network foundation. The final presentation's ability to clearly communicate complex concepts (like the OSI model) to a non-technical audience will also be assessed.

Teacher Resources:

- [NIST Cybersecurity Framework](#)
- [NIST Small Business Cybersecurity Case Study Series](#)
- [Virginia Cyber Range](#)
- [Cisco Networking Academy](#) (Packet Tracer for network diagramming)
- [Cisco Small Business Network Security Checklist](#)

Scenario submitted by Lowell Mathis, Jr., Blacksburg High School, Montgomery County Public Schools