Kern Grant
IT331_M6 – Network Security Design
Heith Hennel
October 6th, 2026

ASSESSMENT PART 1

Differences between external and internal threats in Network Security

A threat to network security refers to an action to access data or a system without authorization. These threats can be classified as internal or external. Internal threats can come from users such as employees with data access. The user's action can be intentional, like leaking sensitive data. It can also be unintentional, like mishandling a company device or opening a phishing email. External threats are people or systems without authorization or connection to the company. These bad actors, like hackers, attempt to breach the network or systems to access sensitive data, interfere with operation, or gain control. Internal threats are harder to protect against because they come from trusted authorized users. To reduce the risk, companies can use access controls, which limit permissions based on job role, and an activity monitoring software to detect uncommon activities. Cybersecurity training also helps employees recognize social engineering threats like phishing emails. In addition, a written security policy is important because it gives employees clear instructions on protecting company data and systems. To protect against external threats, companies rely on security programs like firewalls, intrusion detection, and prevention systems to monitor and stop suspicious traffic. Lastly, data encryption is used to protect data in transit, and multi-factor authentication is used to verify user identity. (Types of Cyberthreats, IBM).

Pretty Good Privacy" (PGP)

Pretty Good Privacy is an encryption program used to protect data by keeping it private and authentic. It works by combining symmetric encryption with public key encryption. Symmetric encryptions use the same key for the sender and receiver to lock and unlock the information. Public key encryption has two different keys, a public and a private. The public key encrypts the data, and the private key unlocks it. It is like giving everyone a locked mailbox to drop letters, and I, the receiver, have the private key to open it. According to TechTarget, PGP became one of the first widely used public key cryptography tools (TechTarget). PGP has stood the test of time because it is proven to be reliable and secure. According to TechTarget, PGP strength comes from combining the two forms of encryption, symmetric for speed and public key for security. It is also known as OpenPGP, meaning anyone can use or improve it. PGP is still trusted today because of its flexibility, end-to-end encryption, and open source. (What is Pretty Good Privacy, TechTarget). PGP will most likely remain useful today but may not in the long term. As technology advances, hackers develop power tools that target older encryption systems. According to TechTarget, PGP strength depends on how it is implemented and the encryption algorithms it uses. While PGP is a framework that uses two encryption methods, inside, it relies on a specific encryption algorithm to lock and unlock data. That means the quality of algorithms, key length, and the setup choices all affect how secure it is. To remain effective, PGP would need ongoing updates and new algorithms to stand up against emerging threats.

The Kerberos system identifies users trying to access a network or service(TechTarget). It works like a digital ID checker. Kerberos gives a special ticket proving my identity, removing the need to type my password each time. It is like getting a wristband at a concert, I can walk out of the venue and back in without showing a ticket again. PGP and Kerberos both protect data in different ways. PGP focuses on data encryption between the sender and receiver. Kerberos focuses on proving who the user is before accessing network or system data. It uses a ticket instead of a key like PGP. Advanced Encryption Security (AES) algorithm can be used for both Kerberos, which applies it to authentication, and PGP, which uses it to encrypt data. A better key encryption than PGP is GNU Privacy Guard (GnuPG). GnuPG follows the Open PGP standard and updates to PGP. It offers the same features as PGP but is open source, free, and easier to integrate with modern systems. Because of the improvements, GnuPG is considered the replacement for PGP(What is Pretty Good Privacy, TechTarget).

Techniques to Secure Wireless Communications

Two techniques to secure wireless communications are Virtual Private Network (VPN) and Secure Sockets Layer / Transport Layer Security (SSL/TLS). Both methods encrypt data as it travels over networks to prevent unauthorized access. A VPN is a protected tunnel between the user device and the endpoint network. It protects all traffic from being intercepted on public Wi-Fi or cellular connections. SSL/TLS encrypts data at the application level, like using HTTPS to browse a website or send an online form. VPNs protect all network traffic from the device, and SSL/TLS protects applications. Together, they make sure data transmitted wirelessly remains private and protected.

Data communication on a public wireless hotspot is not safe without encryption. Public Wi-Fi. Networks are open, which means anyone within range can connect and monitor the unprotected traffic. According to TechTarget, data in motion must be encrypted to prevent attackers from seeing it. Without protection like VPNs or SSL/TLS, hackers can intercept data like logins, emails, or financial details as they travel through the network. Users should only send sensitive data on open networks through HTTPS or a VPN tunnel to stay safe. (How to secure Data at Rest, In Use, and In Motion, TechTarget).

Kern Grant
IT331_M6 – Network Security Design
Heith Hennel
October 6th, 2026

ASSESSMENT PART 2

Network Assessment

Gift of Fortune Enterprises (GoFE) current network consists of a small peer-to-peer LAN using an older 8-port switch connected to the internet service provider router. All computers share the same network for file and printer access. There are no network segments, a central server, or security management. The current network setup supports basic communication but creates congestion and security risk as the business grows.

Network Media

I assume the media used for Gifts of Fortune Enterprise was Category 5 or 5e Ethernet cabling. The company's computers run Windows 7 Pro, which was released in 2009. That information helps me establish a timeframe for this network. In addition, the business has been using an older 8-port switch since 1999. I would assume the cabling was installed during that time or updated with cables that reflect the standards of the early 2000s. Based on this key information, the office media was Cat 5 or 5e (Cat 5 Enhanced) Ethernet cabling. Cat 5 cabling was a standard in the late 1990s, and Cat 5e was introduced in the early 2000s (Enable-IT, 2025).

Network Noise or Signal Integrity

Two noise or signal integrity issues that may impact Gifts of Fortune Enterprise network are electromagnetic interference (EMI) and crosstalk. Because the company operates in a warehouse setting, it's likely exposed to noise or other signal integrity issues that impact the network. A warehouse would likely have electrical equipment like compressors and motors that create electromagnetic interference (EMI). According to GeeksforGeeks, EMI is an unwanted interference in an electrical circuit caused by an outside source (EMI, GeeksforGeeks). In this scenario, the copper Ethernet cables carry data using electrical signals at a specified frequency. The nearby electrical equipment also produces electromagnetic energy that can overlap with the cable frequency. This interference can disrupt network communication and result in data errors, reduced speed, or cause unstable internal and external connections. The company could use Cat 5 or 5e, shielded twisted pair cabling (STP) to reduce the EMI. According to GeeksforGeeks, STP cables include an extra shielding layer to reduce EMI (Difference between Unshielded Twisted Pair and Shielded Twisted Pair Cables, GeeksforGeeks).

The second possible signal integrity issue is crosstalk. Crosstalk is signal interference caused by the electric or magnetic energy between network cables (Crosstalk, TechTarget). In the company's case, the Ethernet cables may have multiple cables bundled or wire pairs running close together inside the same cable. This can cause signals from one wire to overlap with another. It can result in signal interference, data errors, and reduced network speed. Use shielded twisted pair (STP) cabling to prevent or minimize crosstalk. STP provides a conductive layer around the wires that blocks interfering electromagnetic fields (Difference between Unshielded Twisted Pair and Shielded Twisted Pair Cables, GeeksforGeeks).

Network Devices

Router

- The router provided by Nation Online connects the company's internal network to an external network, like the Internet. It assigns IP addresses, manages network traffic, and may have a built-in firewall for protection.

Switch

- The switch connects multiple devices within the company's local network and directs data between them. It allows the computers in the warehouse to share files and communicate internally.

Desktop Computers

- Employees use the desktop computers in the main offices to access files, send emails, and perform daily business activities. Each desktop connects to the network through the switch for data sharing.

Laptop

- The laptop in the warehouse is used to perform business activities. It is similar to a desktop computer, but it is mobile. The user can work from the laptop on the go, so it's convenient.

Dot Matrix printer

- The printer in the warehouse is used to print invoices, shipping labels, or order forms. It connects the warehouse computer through the network and allows employees to print documents for business operations.

Laser Printer

- The laser printer is connected to Kyle's office assistant. It is used to print documents like reports. The other employees send print jobs to the assistant through the network.

Identify all items being shared by users on the network

Laser printer

- Employees can email or send print jobs to Kyle's assistant for printing.

Dot Matrix Printer

- Shared throughout the warehouse computer.

Files and Data

- Files are stored on individual computers and shared in the company's peer-to-peer network. Employees in the main office and warehouse access files or the specific device data through the switch. The switch connects all computers on the same local network.

Email communication

- Used by the staff to exchange files and send print requests to the assistant. The scenario states that employees email print jobs to Kyle's assistant. Because Kyle and his assistant have internet access, other employees probably use a local email with the peer-to-peer network to send and redirect to the assistant's computer.

Internet Connection

- Shared through the router provider by Nation Online. Only Kyle and his assistant currently have direct internet access. All the devices connect to the same LAN for local communication.

WAN connection and process

- The company's internet connection is provided by Nation Online (NOL). NOL supplied the router. The router connects to the local network to the Internet using a wired broadband connection, most likely cable or digital subscriber line (DSL). Broadband refers to high-speed internet access connected with a wired connection, like DSL, cable, or fiber (What is broadband, TechTarget).
- The router gives each computer an IP address using the Dynamic Host Configuration Protocol (DHCP) andmanages network traffic through Network Address Translation (What is a Router?, TechTarget). So, the DHCP provides each device with a private IP address to use in the LAN, NAT turns that address into a router's public address. That public address is what is recognized on external networks like the Internet. The internet

communication operates through Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP breaks information into packets to send it across the network.

Forms of security

- There are two possible forms of security for the network, physical and electronic. The company currently has limited security measures. Physical security is the main protection since Kyle locks the doors at night to prevent unauthorized access to the warehouse. This can help prevent a bad actor from accessing the computers that store the company's data and files. For electronic security, there are minimal or probably no security measures. Kyle mentioned the probability of the router having a built-in firewall. There was no other mention of electronic security. Therefore, the only security measure I can confirm is physically locking the warehouse doors.

Part B: Problem/Solution Table

Problem	Impact/Risk	Solution	Justification
Network Type	Peer-to-peer LAN using an outdated switch with no control.	Add a Client-Server network using a Windows Server 2022 system with centralized file and user management.	Provides domain logins and Group Policy access for control. It supports data backups and permission-based access to protect company files (Microsoft, 2025).
Outdated operating systems (Windows 7 Pro)	It is vulnerable to malware and system attacks because Microsoft no longer supports it.	Upgrade all the systems to Windows 11 Pro or optional (Enterprise LTSC, long-term servicing channel).	Windows 11 Pro supports patch management and built-in security tools like Windows Defender, BitLocker, and hardware encryption (Microsoft, 2024).
Outdate switch (8-port)	This switch causes bandwidth congestion and the risks of hardware failure.	Update to a managed 24-port switch that supports VLAN network segments.	A VLAN network separates departments and traffic to reduce congestion, internal attacks, and improve network performance.
Single router/no firewall management.	Little control over incoming/outbound traffic.	Install a business-grade router/firewall that has intrusion prevention and VPN features.	This solution will provide active threat monitoring, remote access encryption, and centralized security.

No wireless encryption or guest isolation	An open Wi-Fi allows unauthorized access and possible threats.	Install a secure Wi-Fi 6 access point using WPA3 Enterprise and a separate guest VLAN (WPA3, Cisco).	This solution encrypts all wireless data and prevents guest users from accessing the company's internal systems.
No data backup or redundancy.	A hardware failure or cyber-attack can cause data loss.	Implement a Network Attached Storage (NAS) with RAID 5 and automated daily backups (What is RAID 5?, TechTarget).	To prevent possible data loss. Also, use AES-encrypted backups stored onsite and in a secure cloud location.
No written security policy or employee training.	Human errors and unreported security activities risk the company's network and data.	Create and implement a security policy and conduct routine cybersecurity training.	Reinforce internal controls, password updates, cyber-attacks like phishing, and incident reporting procedures.

Part C: Proposal Document

Project Justification

Gift of Fortune Enterprise (GoFE) requires a network upgrade to meet expanding business needs. GoFE currently has apeer-to-peer LAN connection, an outdated 8-port switch, and computers running Windows 7 Pro. The infrastructure lacks centralized control, file security, and reliable data backup, leading to inconsistent data access, vulnerability, and reduced productivity. GoFE's current network infrastructure cannot meet future user and business needs. As the company grows, the outdated equipment and unsupported operating systems create a risk of downtime, data loss, and security exposure. Upgrading the network will provide consistent access to shared resources, secure communication between departments, and improved performance in operating modern applications.

Project Goals

Goal 1

- Upgrade GoFE's network to a client-server system that supports centralized file sharing, secure access, and reliable backups. This goal addresses the company's need for better control and data protection. Consistent user logins through a server domain and the ability to access files without downtime are the mark of success.

Goal 2

- Replace outdated Windows 7 Pro computers and network equipment with Windows 11 Pro workstations and a managed 24-port switch. This goal supports daily operations and provides compatibility with new business applications. The mark of success is when all devices operate on the updated hardware and software without performance or security issues.

Goal 3

- Implement stronger network security and data protection using WPA3 wireless encryption, multi-factor authentication (MFA), a firewall with VPN access, and a security policy with employee training. This goal aligns with GoFE's need to protect company and customer data. Verified encryption settings, active MFA for all users, firewall monitoring logs, and confirmation that all employees complete routine cybersecurity training are the mark of success.

Solution Summary

- The proposed solutions work together to update GoFE's network and secure company data. Upgrading to a client-server allows centralized file storage, user authentication, and routine backups. The new Windows 11 Pro workstations and managed 24-port switch improve speed, compatibility, and reliability for daily business operations. The network security updates will protect all users and data within the network. Together, these upgrades create a unified, secure, and scalable infrastructure that supports GoFE's business growth and new software applications. According to The Network Installers (2025), the small business network setup cost typically ranges from $8,000 to $15,000 for companies with 10 - 50 employees (The Network Installers). Based on this estimate, GoFE's project would fall within an average cost of $12,000. The complete network upgrade includes hardware installation, system configuration, staff training, disposal, and staff training to be completed in six to 8 weeks with a buffer for delay and minimal disruption.

Impact

- Upgrading GoFE's network will improve how every user works. Employees will have faster access to shared files, secure logins through a server domain, and reliable network connections with less downtime. The new system allows multiple users to work on shared projects simultaneously, knowing data is protected. One of the challenges may be the minimal downtime during installation and user adaptation. However, the transition can be simplified with proper scheduling and brief training. OTheupgrades will increase company performance, security, and user confidence.

IT Infrastructure Library (ITIL)

- The information Security Management practice was most helpful in this project. It guided my planning and decision-making to identify secure options that protect the company and customer data. I used the practice to evaluate different security methods that align with GoFE's network operation needs.

References

Part 1

1. IBM. *Types of Cybersecurity*, 2025, www.ibm.com/think/topics/cyberthreats-types.
2. TechTarget. *What Is Pretty Good Privacy, and How Does It Work?* , 2025, www.techtarget.com/searchsecurity/definition/Pretty-Good-Privacy.
3. TechTarget. *What Is Kerneros, and How Does It Work?* , 2025, www.techtarget.com/searchsecurity/definition/Kerberos.
4. *How to Secure Data at Rest, in Use and in Motion.* , 2022, www.techtarget.com/searchsecurity/feature/Best-practices-to-secure-data-at-rest-in-use-and-in-motion.

Part 2

1. Enable-IT. *Cat5 Cable Speed 7 Powerful Facts About Cat5 & 5e Ethernet Performance*, 2025, https://enableit.com/cat5-cable-speed/?srsltid=AfmBOoq3LnNzIqEBA9JlEEgdPB_C_dmSAHqowB5WI8aArQe_s0_20slW
2. TechTarget. "Electromagnetic Interference (EMI)." *Electromagnetic Interference (EMI*, 2022, www.techtarget.com/searchmobilecomputing/definition/electromagnetic-interference.
3. GeeksforGeeks. *Difference between Unshielded Twisted Pair and Shielded Twisted Pair Cables*, 2025, www.geeksforgeeks.org/computer-networks/difference-between-unshielded-twisted-pair-utp-and-shielded-twisted-pair-stp-cables/.
4. TechTarget. *Crosstalk*, 2021, www.techtarget.com/searchnetworking/definition/crosstalk.
5. TechTarget. *Broadband*, 2023, www.techtarget.com/searchnetworking/definition/broadband.
6. TechTarget. *What Is a Router*, 2025, www.techtarget.com/searchnetworking/definition/router.

7. Microsoft. *What's New in Windows Server 2022*, 2025, https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2022

8. Microsoft. *Windows 11 Security Features* , 2024, www.microsoft.com/en-us/windows/learning-center/windows-11-security-features.

9. Cisco. *WPA3 Deployment* , 2025, www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/wpa3-dg.html.

10. TechTarget. *What Is RAID 5* , 2025, www.techtarget.com/searchstorage/definition/RAID-5-redundant-array-of-independent-disks.

11. The Network Installers. *The Network Installers,* 2025, https://thenetworkinstallers.com/blog/small-business-network-setup-cost/