Christopher Stevens
CYB469
Section 01
3.6 Assignment: Case Study

Company Case Study: Luigi's

A Luigi's Inc. employee brought a personal laptop into the facility infected (albeit unknowingly) with PSL and connected it to the corporate network via a wireless access point (AP). The system obtained an IP Address using Dynamic Host Configuration Protocol (DHCP) addressing provided by the core corporate network services. Upon connection, the infected system made an Internet connection to the command-and-control server.

Once connected, the threat actor provided the command for the system to scan the local network for available services. While the user noticed that the machine was running slowly, it was late on Friday before a three-day weekend. The user left the machine powered on with plans to look at it again on Tuesday. The scan identified an open File Transfer Protocol (FTP) service on the internal network that allowed anonymous access. The threat actor, still using the compromised machine, logged into the FTP server, compressed the contents and then transferred the data to the control server (over the internet) using an encrypted outbound VPN connection.

Over the weekend, the Network Operations Center (NOC) tracked a large amount of data over an encrypted channel. While they were able to identify both the source and destination, without the encryption keys, they were unable to decrypt the traffic to identify the content. The destination was not on the current list of known malicious sites (the list was out of date by four months). The help desk technician then opened a work ticket for the local desktop services to investigate.

Early Tuesday morning the user noticed that the machine was still acting erratically, even after a reboot. The user then called the help desk to open a ticket. The help desk technician was able to tie IP address of this machine to the traffic identified over the weekend. When the desktop technician arrived, it was determined that the machine in question is not a corporate machine and does not have all the standard protection software. A quick scan using a boot time tool found the PSL signature. At this point, the technician confiscated the machine for forensic investigation and the ticket was closed.

The forensics team determined a known malware tool named PSL compromised the machine. They also found a temporary file, left over by the scanning, that included the directory listing of the FTP site. Many of the folders within the directory were named after previous high-value programs. These files included parts lists, price quotes and even proprietary drawings. Included in the information, were patents from the current Chief Executive Officer (Ms. J. Rabbit) as well as legal documents describing the purchasing and legal aspects of these programs.

1. Clearly state all of the issues that need to be addressed at Luigi's. (How did the attack occur?) (Please use bullets or numbers.)

- Asset Management Failure - An unmanaged, infected personal laptop was allowed to bypass physical and logical security to connect to the corporate network via a wireless Access Point (AP).
- Network Architecture Failure - The network lacked internal segmentation, allowing an untrusted wireless device to scan and communicate with sensitive internal file servers.
- System Configuration Failure - An internal File Transfer Protocol (FTP) server was configured with "Anonymous Access," removing the requirement for any authentication to view or steal data.
- Threat Intelligence Failure - The Network Operations Center (NOC) was operating with a malicious site blocklist that was four months out of date, failing to identify the Command and Control (C2) server.
- Egress Filtering Failure - The network infrastructure allowed a high-volume, encrypted outbound data transfer to an unknown external IP without triggering an automated block.
- Security Culture Failure - An employee observed "erratic" system behavior but failed to report it immediately, and the Help Desk/NOC lacked a rapid weekend response protocol.

2. Which CIS Controls v8 could have helped to prevent the attack that is detailed in the case study? (Please use bullets or numbers.)

a. Why is the Control important? (Answer this for each control listed in #2, 25 word minimum). Be thorough in your response.

- Control 01 - Inventory and Control of Enterprise Assets
  - o Importance: This control is the fundamental starting point for all security because an organization cannot defend assets it does not know are present. By maintaining an automated and up-to-date inventory, Luigi's could have utilized technical gates to ensure that only devices with a pre-approved security profile were granted an IP address. This visibility allows for the automated denial of network access to unmanaged devices, effectively stopping the attack before the malware could ever communicate with its external command-and-control server.

- Control 02: Inventory and Control of Software Assets
  - o Importance: This control is essential because it ensures that only authorized and vetted software is allowed to execute on the corporate network. By maintaining a strict software inventory, Luigi's could have utilized application allow-listing to prevent the "PSL" malware from running, even if the device was physically connected. This prevents unauthorized scripts and malicious binaries from compromising the integrity of the operating environment and accessing sensitive system resources.

- Control 03 - Data Protection
  - o Importance: Luigi's failed to identify and protect their "high-value" drawings and patents, which is the core of their business. This control is essential because it requires organizations to locate, classify, and apply extra security layers to sensitive data. If these files had been properly identified, the FTP server would have been flagged as a high-security asset, requiring encryption and multi-factor authentication, making the anonymous theft of the CEO's intellectual property impossible for an outsider.

- Control 04 - Secure Configuration of Enterprise Assets and Software
  - o Importance: Modern software is often shipped with "open" default settings to prioritize ease of use, which unfortunately creates massive security holes for attackers to exploit. This control is vital because it mandates a strict "hardening" process where unnecessary services, like the anonymous FTP access found in this case, are disabled by default. Had Luigi's enforced these secure configurations, the attacker's internal scan would have found a locked door instead of an open directory of high-value proprietary drawings, patents, and sensitive legal documents.

- Control 05: Account Management
  - o Importance: Managing the full lifecycle of accounts is critical to ensuring that only legitimate users have access to corporate resources. This control is vital because it would have identified the "anonymous" account used on the FTP server as a high-risk security gap. By enforcing unique user accounts and periodic reviews, Luigi's would have ensured that all data access was tied to a verifiable identity, preventing the threat actor from browsing files without credentials.

- Control 06: Access Control Management
  - o Importance: Access control ensures the principle of "least privilege" is applied, granting users access only to the data necessary for their specific roles. This is important because it would have restricted the folders on the FTP site so that general users or guest devices could not view the CEO's patents or legal documents. By limiting access to sensitive directories, Luigi's would have contained the impact of the breach even after the initial network connection occurred.

- Control 07 - Continuous Vulnerability Management
  - Importance: Cybersecurity is not a static setup; it requires constant, automated updates to stay ahead of the evolving tactics used by modern threat actors. This control is critical because it ensures that defensive tools—like the NOC's malicious site lists—are updated daily rather than being left for four months. If this control had been properly maintained, the network monitoring tools would have recognized the PSL malware's signature or its destination address immediately, allowing the security team to block the encrypted data transfer in real-time.

- Control 08: Audit Log Management
  - Importance: Audit logs serve as the "black box" for security incidents, providing the evidence needed to understand how an attack occurred. This control is vital because it requires the collection and analysis of logs from servers and network devices. If Luigi's had central log management, the suspicious compression and transfer of files would have triggered an automated alert, allowing the NOC to respond to the theft in real-time rather than waiting for a manual investigation.

- Control 09: Email and Web Browser Protections
  - Importance: Many malware strains, including PSL, rely on web-based protocols to communicate with Command-and-Control servers. This control is important because it mandates the use of DNS filtering and web content inspections to block connections to known malicious domains. By implementing these protections, the infected laptop would have been unable to "phone home" to the attacker, effectively neutralizing the threat despite the device being connected to the corporate wireless access point.

- Control 10: Malware Defenses
  - Importance: This control provides the active "immune system" for the enterprise by detecting and neutralizing malicious code across all endpoints and network segments. It is important because modern anti-malware tools look for signatures and behaviors of known threats like PSL. Even on an unmanaged device, network-level malware scanning could have intercepted the malicious activity as it tried to move across the network, alerting the help desk to the presence of an infected machine immediately.

- Control 11: Data Recovery
  - Importance: While this attack focused on data theft, a robust recovery plan is the ultimate safety net for organizational resilience. This control is important because it ensures that if an attacker had deleted or encrypted the proprietary drawings after the theft, the company could restore operations without paying a ransom or losing years of work. Maintaining verified, offline backups ensures that the organization can recover from the "worst-case scenario" of a total system compromise.

- Control 12 - Network Infrastructure Management
  - Importance: Proper management of network architecture is essential because it prevents a single compromised device from accessing the entire corporate environment. By implementing network segmentation, Luigi's could have isolated the wireless access points from the internal servers containing proprietary data. This "internal walling" ensures that even if an infected personal device connects to the Wi-Fi, it remains trapped in a restricted zone where it cannot scan or communicate with high-value systems like the FTP server.

- Control 13 - Network Monitoring and Filtering
  - Importance: Network monitoring and filtering are critical because they provide the "eyes and ears" necessary to detect data exfiltration as it happens in real-time. This control is vital because it involves monitoring for unusual traffic patterns, such as a massive encrypted outbound transfer to an unknown external destination. By implementing robust egress filtering, Luigi's could have automatically triggered an alert or a connection block when the volume of data leaving the network exceeded normal thresholds, potentially stopping the theft before the CEO's patents were fully transferred.

- Control 14: Security Awareness and Skills Training
    - o Importance: Technical defenses are only as strong as the people operating them, making training a mandatory layer of any defense-in-depth strategy. This control is important because it empowers employees to recognize early warning signs, such as a machine running slowly or behaving erratically. If the employee at Luigi's had been properly trained, they would have alerted the help desk on Friday afternoon instead of leaving the machine powered on, closing the 72-hour window the attacker used.

- Control 15: Service Provider Management
    - o Importance: Organizations often rely on third-party providers for core network services like DHCP or FTP hosting. This control is important because it ensures that these providers are held to the same rigorous security standards as the internal team. By vetting the security practices of service providers, Luigi's could have ensured that their core network services were not configured with dangerous defaults, such as anonymous access, which ultimately facilitated the data exfiltration.

- Control 16: Application Software Security
    - o Importance: If the FTP service or the tools used to manage patents were developed or managed as internal applications, this control ensures that security is "baked in" from the start. It is essential because it requires regular testing and secure coding practices to prevent vulnerabilities. By following a secure development lifecycle, administrators would have identified the lack of authentication on the FTP server as a critical flaw that needed to be remediated before the system went live.

- Control 17 - Incident Response Management
    - o Importance: Even the best technical defenses can eventually fail, making a rapid, well documented response plan essential to limit the overall damage to the organization. This control ensures that when the NOC identifies suspicious behavior, such as a massive, encrypted data spike over a holiday weekend, there is a clear protocol to escalate and contain the threat immediately. At Luigi's, the absence of an urgent response framework allowed the threat actor a 72-hour window to steal high-value data without any interference.

- Control 18: Penetration Testing
    - o Importance: A penetration test is a simulated attack that identifies gaps in defenses before a real threat actor can exploit them. This control is vital because a skilled tester would have found the "Anonymous FTP" server and the outdated malicious site list months before this incident occurred. By proactively testing the environment, Luigi's would have had the chance to fix these high-risk vulnerabilities, ensuring their intellectual property remained protected from unauthorized access and theft.

3. List the Safeguards for each of the Controls that are listed in question 2, that should have been implemented to prevent the attack. (Please use bullets or numbers.)

a. Why are the Safeguards important? (Answer this for each safeguard listed in #3, 25 word minimum). Be thorough in your response.

- Safeguard 1.1 - Establish and Maintain a Detailed Enterprise Asset Inventory
    - o Importance: This safeguard provides the technical foundation for Network Access Control (NAC), which acts as a digital "bouncer" for the enterprise network. By maintaining a meticulous list of authorized hardware, the organization can ensure that only vetted, company-managed devices are granted an IP address. This prevents the "Shadow IT" risk seen in the case study, where an unmanaged and infected device was allowed to bypass the perimeter and operate within the trusted internal environment.

- Safeguard 2.1: Establish and Maintain a Software Inventory
    - Importance: This safeguard provides the visibility required to ensure that only approved applications are running within the enterprise environment. By maintaining a detailed list of authorized software, the IT department can use automated tools to identify and block the execution of unauthorized programs like the PSL malware. This effectively limits the ability of an attacker to gain a foothold or persist within the network using unmanaged or malicious software tools.

- Safeguard 3.3 - Configure Data Access Control Lists
    - Importance: Access Control Lists are the primary defense against unauthorized data browsing. This safeguard is essential because it ensures that even if a user is on the network, they cannot access sensitive files without explicit permission. By configuring these lists on the FTP server, Luigi's would have ensured that only specific employees with a legitimate business need—not anonymous users—could view folders containing high-value program parts lists, price quotes, and proprietary drawings.

- Safeguard 4.8 - Uninstall or Disable Unnecessary Services
    - Importance: Every active service represents a potential "attack surface" that a threat actor can exploit to gain a foothold or steal data. This safeguard is critical because it requires the removal of legacy or insecure protocols that are not required for business operations. Disabling the anonymous login feature on the FTP server would have forced the attacker to provide credentials, which likely would have halted the data theft and triggered an authentication failure alert for the security team.

- Safeguard 5.1: Establish and Maintain an Inventory of Accounts
    - Importance: Maintaining a central inventory of all user and administrative accounts is essential for tracking who has access to sensitive data. This safeguard is important because it prevents "orphaned" or "anonymous" accounts from becoming blind spots in the security architecture. By ensuring every account is tied to a specific individual and a business purpose, Luigi’s would have been able to audit the FTP access and detect unauthorized users immediately upon connection.

- Safeguard 6.1: Establish an Access Control Process
    - Importance: This safeguard defines the rules for how access to data is granted, ensuring that permissions are based on the user's job function. It is important because it prevents "over-privileged" access where any user on the network can see every file. By implementing a formal access control process, Luigi's would have ensured that proprietary drawings and legal documents were only accessible to the specific staff members who required them, protecting the data from general network scans.

- Safeguard 7.1 - Establish and Maintain a Vulnerability Management Process
    - Importance: Modern threats evolve at a rapid pace, and security teams must have a structured process to ingest new threat data. This safeguard is vital because it would have forced the NOC to update their malicious site list more frequently than once every four months. Having an updated list is the difference between stopping a known malware signature at the door and allowing it to freely exfiltrate data to a command-and-control server.

- Safeguard 8.1: Establish and Maintain an Audit Log Management Process
    - Importance: A formal log management process ensures that the organization is collecting the right data to detect and investigate security incidents. This safeguard is critical because it defines which events—such as large file transfers or failed logins—must be captured and reviewed. Without this process, the NOC at Luigi's was unable to turn the "large amount of data" they saw into a clear picture of an active theft, leading to a delayed and ineffective response.

- Safeguard 9.2: Use DNS Filtering Services
  - Importance: DNS filtering is one of the most effective ways to block connections to malicious infrastructure on the internet. This safeguard is important because it prevents malware from reaching its Command-and-Control server to receive instructions or exfiltrate data. By using a reputable DNS filtering service, Luigi’s could have automatically blocked the laptop’s attempt to connect to the attacker's server, regardless of whether the internal malicious site list was updated manually or not.

- Safeguard 10.1: Deploy and Maintain Anti-Malware Software
  - Importance: Deploying anti-malware across the entire enterprise ensures that there is a consistent layer of defense against known viruses and trojans. This safeguard is essential because it provides automated detection and remediation of threats like the PSL malware. By maintaining this software with current signature updates, Luigi's would have increased the likelihood of catching the infection as it attempted to scan the network, providing the security team with the early warning needed to isolate the device.

- Safeguard 11.1: Establish and Maintain a Data Recovery Process
  - Importance: A documented data recovery process ensures that the organization knows exactly how to restore its systems after a compromise or data loss event. This safeguard is vital because it establishes the timeline and procedures for bringing business operations back online safely. In the event that the threat actor had corrupted the proprietary drawings on the FTP server, this process would have allowed Luigi’s to restore the files from a clean backup, minimizing the impact on the company’s high-value programs.

- Safeguard 12.2 - Establish and Maintain a Secure Network Architecture
  - Importance: A secure architecture replaces the "flat" network model with a "defense-in-depth" approach that uses segmentation to prevent lateral movement by attackers. This safeguard is vital because it keeps different parts of the business isolated; by separating wireless access points from production servers, Luigi's would have ensured that a successful compromise of a laptop would not lead to a compromise of the company’s high-value intellectual property.

- Safeguard 13.4 - Perform Egress Filtering
  - Importance: This safeguard is the last line of defense against data theft, as it monitors and controls what leaves the organization. It is important because it prevents compromised internal systems from communicating with malicious external servers. By filtering outbound traffic, Luigi's could have detected and blocked the encrypted VPN connection to the attacker's server, as the destination would not have been on a pre-approved list of trusted business partners or services.

- Safeguard 14.1: Establish and Maintain a Security Awareness Program
  - Importance: A formal awareness program ensures that all employees understand their role in protecting the organization’s assets. This safeguard is important because it shifts the culture from "passive" to "active" defense. By training staff to recognize social engineering and technical anomalies, Luigi’s could have turned the employee who noticed the "sluggish" laptop into a human sensor, potentially stopping the breach on Friday before the data exfiltration began over the weekend.

- Safeguard 15.1: Establish and Maintain an Inventory of Service Providers
  - Importance: Knowing which third parties have access to your network or manage your data is critical for managing supply chain risk. This safeguard is important because it allows the organization to apply security requirements consistently across all partners. If the FTP service was provided by an outside vendor, this inventory would have triggered a security review, ensuring that the vendor followed Luigi’s internal policy of disabling anonymous access and maintaining updated threat intelligence.

- Safeguard 16.1: Establish and Maintain a Secure Software Development Process
    - Importance: This safeguard ensures that security requirements are considered during every phase of software development and maintenance. It is important because it prevents common vulnerabilities from being introduced into custom-built applications. By following a secure development process, any internal team managing the FTP server would have been required to include authentication as a core requirement, preventing the anonymous access flaw from ever reaching the production environment where sensitive data was stored.

- Safeguard 17.3 - Designate Personnel to Manage Incident Handling
    - Importance: Having specific people responsible for incidents ensures that alerts are not ignored and that the "ball is not dropped" during transitions or holidays. This safeguard is essential because it establishes accountability and clear lines of communication. If a designated incident responder had been active or "on-call" over the weekend, the NOC's observation of high-volume encrypted traffic would have resulted in an immediate isolation of the laptop, stopping the exfiltration mid-stream.

- Safeguard 18.1: Establish and Maintain a Penetration Testing Program
    - Importance: A regular penetration testing program provides an objective assessment of the organization's security posture by attempting to bypass existing controls. This safeguard is essential because it identifies the "unknown unknowns" that automated scanners might miss. By conducting these tests, Luigi's would have discovered that an unauthorized device could easily scan their "flat" network and access sensitive files, providing the evidence needed to justify upgrades to network segmentation and asset management systems.