3.6 Assignment: Case Study

In my opinion, this incident occurred as a result of Luigi's assuming internal network access to be trusted by default. A personal (unmanaged) device was permitted on the corporate Wi-Fi and that one chink in the armor opened the door for malware to access internal services, discover an anonymously accessible FTP repository, and exfiltrate sensitive engineering and legal information. Guided by the CIS Critical Security Controls (v8), I concentrated on the controls and safeguards that would lessen the probability of a BYOD-induced incident, as well as reduce detection and response time.

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.)**
    - A personally owned (unmanaged) laptop was connected to the corporate wireless network and acquired a DHCP address from core services.
    - The personal laptop was missing Luigi’s standard endpoint protection (anti-malware/EDR and centralized management).
    - The infected endpoint could access an external C2 server and get commands (Lack of effective egress controls / threat blocking).
    - The compromised endpoint scanned the internal network for services (lack of segmentation and internal detection).
    - Internal FTP service was configured to allow anonymous login, and the attacker browsed and harvested sensitive folders and files.
    - Sensitive engineering and legal information were placed on the FTP share with insufficient access or data protection measures in place.
    - Exfiltration was done on an encrypted outbound VPN tunnel, could not identify content (visibility and tuning limitations in SOC/NOC).
    - The destination was not on the “known bad” list because the list was not up to date. It was out of date for several months.
    - Incident response was delayed (weekend and user left device on), and there was minimal proactive containment prior to Tuesday.

2. **Which CIS Controls v8 could have helped to prevent the attack that is detailed in the case study? (Please use bullets or numbers.)**
    - CIS Control 1 – Inventory and Control of Enterprise Assets
    - CIS Control 2 – Inventory and Control of Software Assets
    - CIS Control 3 – Data Protection
    - CIS Control 4 – Secure Configuration of Enterprise Assets and Software
    - CIS Control 6 – Access Control Management
    - CIS Control 10 – Malware Defenses
    - CIS Control 12 – Network Infrastructure Management
    - CIS Control 13 – Network Monitoring and Defense
    - CIS Control 14 – Security Awareness and Skills Training
    - CIS Control 17 – Incident Response Management

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

    - **CIS Control 1 – Inventory and Control of Enterprise Assets**
      - Control 1 is important because you can't protect what you can't see. If Luigi's had good asset inventory and controls in place to dictate what is permitted to connect, the personal infected laptop would have been discovered as an unauthorized asset. That would support blocking it from accessing the corporate Wi-Fi or putting it into a restricted guest segment.

    - **CIS Control 2 – Inventory and Control of Software Asset**
      - Control 2 is significant for this scenario because malware typically requires unauthorized or unmanaged software to run, and unmanaged devices generally have an unknown state of software.

By monitoring known, authorized software and implementing allowlisting, Luigi’s would have prevented unknown executables or scripts from running and potentially could have reduced the chance of infected endpoints from introducing risky tools or out-of-date applications onto their network.

- **CIS Control 3 – Data Protection**
  - Control 3 is important since the attacker was successful primarily by exploiting access to sensitive engineering and legal documents. Had Luigi's properly classified sensitive information and applied protection mechanisms (access controls, secure storage locations, monitoring of data movement, etc.), the anonymous FTP repository would not have been a convenient one-stop shop for high-value programs and proprietary drawings.

- **CIS Control 4 – Secure Configuration of Enterprise Assets and Software**
  - Control 4 is important because vulnerabilities are the windows through which attackers enter, and poor configuration choices are a type of vulnerability. Anonymous FTP access is an example of poor configuration, as is leaving insecure services turned on with no hardening applied internally. Secure baseline configuration and regular configuration management would have enforced authenticated access, stronger permissions, and secure defaults.

- **CIS Control 6 – Access Control Management**
  - Control 6 is significant for this case because access is the gatekeeper for both users and systems. The compromised endpoint was able to authenticate (or not authenticate) to internal services, and the attacker could move data out through remote access channels. Strong access controls, least privilege, and MFA on remote access drastically mitigate the potential for abuse and data theft.

- **CIS Control 10 – Malware Defenses**
  - Control 10 is solely focused on prevention of initial compromise and stopping execution. If Luigi’s implemented enforced approved anti-malware/EDR with automatic updates and centralized visibility, the personal laptop would have been blocked from the environment or detected immediately upon contacting C2 or scanning the internal network.

- **CIS Control 12 – Network Infrastructure Management**
  - Control 12 is important because wireless, DHCP, routing, and internal services are components of the network infrastructure, which requires ongoing management. The network architecture can be designed (segmentation, securely configured network devices, hardened services, etc.) to prevent an infected laptop from having wide-reaching internal access, and to limit an attacker's ability to find and reach critical servers such as the FTP system.

- **CIS Control 13 – Network Monitoring and Defense**
  - Control 13 is valuable because Luigi’s NOC reported anomalous encrypted traffic without content identification and the destination was not blocked or flagged. Monitoring, fine-tuned alerts, and network-based detection would detect scanning behavior and suspicious DNS/HTTP/S traffic to C2 as well as data exfiltration traffic patterns. It reduces dwell time and facilitates containment before significant data loss.

- **CIS Control 14 – Security Awareness and Skills Training**
  - Control 14 is important because the incident begins with human behavior: someone bringing their personal laptop to work and connecting it to the corporate network. Awareness training and workforce expectations can help avoid risky behavior, encourage earlier reporting (i.e., before a weekend), and explain to employees what "odd behavior" or unanticipated slowness might indicate.

- **CIS Control 17 – Incident Response Management**
  - Control 17 is important because incidents can still happen despite best efforts and controls. Luigi's did have some response capability-the NOC noticed abnormal encrypted traffic, but Luigi's

team couldn't contain it quickly, partly because of their lack of weekend coverage. An established incident response program has set thresholds, roles, reporting, exercises, and post-incident process improvements to make response timely and consistent.

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.)**

- **CIS Control 1 – Inventory and Control of Enterprise Assets**
    - 1.1 Establish and Maintain Detailed Enterprise Asset Inventory
    - 1.2 Address Unauthorized Assets
    - 1.3 Utilize an Active Discovery Tool
    - 1.4 Use DHCP Logging to Update Enterprise Asset Inventory
    - 1.5 Use a Passive Asset Discovery Tool

- **CIS Control 2 – Inventory and Control of Software Assets**
    - 2.1 Establish and Maintain a Software Inventory
    - 2.2 Ensure Authorized Software is Currently Supported
    - 2.3 Address Unauthorized Software
    - 2.4 Utilize Automated Software Inventory Tools
    - 2.5 Allowlist Authorized Software

- **CIS Control 3 – Data Protection**
    - 3.1 Establish and Maintain a Data Management Process
    - 3.2 Establish and Maintain a Data Inventory
    - 3.3 Configure Data Access Control Lists
    - 3.6 Encrypt Data on End-User Devices
    - 3.13 Deploy a Data Loss Prevention (DLP) Solution

- **CIS Control 4 – Secure Configuration of Enterprise Assets and Software**
    - 4.1 Establish and Maintain a Secure Configuration Process
    - 4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure
    - 4.4 Implement and Manage a Firewall on Servers
    - 4.5 Implement and Manage a Firewall on End-User Devices
    - 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software

- **CIS Control 6 – Access Control Management**
    - 6.1 Establish an Access Granting Process
    - 6.2 Establish an Access Revoking Process
    - 6.3 Require MFA for Externally-Exposed Applications
    - 6.4 Require MFA for Remote Network Access
    - 6.7 Centralize Access Control

- **CIS Control 10 – Malware Defenses**
    - 10.1 Deploy and Maintain Anti-Malware Software
    - 10.2 Configure Automatic Anti-Malware Signature Updates
    - 10.5 Enable Anti-Exploitation Features
    - 10.6 Centrally Manage Anti-Malware Software
    - 10.7 Use Behavior-Based Anti-Malware Software

- **CIS Control 12 – Network Infrastructure Management**
    - 12.1 Ensure Network Infrastructure is Up-to-Date
    - 12.2 Establish and Maintain a Secure Network Architecture
    - 12.4 Establish and Maintain Architecture Diagram(s)
    - 12.5 Centralize Network Authentication, Authorization, and Auditing (AAA)
    - 12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work

- **CIS Control 13 – Network Monitoring and Defense**
  - 13.1 Centralize Security Event Alerting
  - 13.3 Deploy Network Intrusion Detection Solutions
  - 13.4 Perform Traffic Filtering Between Network Segments
  - 13.6 Collect Network Traffic Flow Logs
  - 13.9 Deploy Port-Level Access Control

- **CIS Control 14 – Security Awareness and Skills Training**
  - 14.1 Establish and Maintain a Security Awareness Program
  - 14.2 Train Workforce Members to Recognize Social Engineering Attacks
  - 14.6 Train Workforce Members on Recognizing and Reporting Security Incidents
  - 14.8 Train Workforce on Causes of Unintentional Data Exposure
  - 14.9 Train Workforce Members on the Dangers of Connecting to and Transmitting Corporate Data Over Insecure Networks

- **CIS Control 17 – Incident Response Management**
  - 17.1 Designate Personnel to Manage Incident Handling
  - 17.3 Establish and Maintain an Enterprise Process for Reporting Incidents
  - 17.4 Establish and Maintain an Incident Response Process
  - 17.7 Conduct Routine Incident Response Exercises
  - 17.9 Establish and Maintain Security Incident Thresholds

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

- **CIS Control 1 – Inventory and Control of Enterprise Assets**
  - **1.1 Establish and Maintain Detailed Enterprise Asset Inventory**
    - Detailed inventorying makes it possible to immediately know whether a device is corporate-managed or not. For Luigi's, this would create an enforceable "only known devices" posture, so a personal laptop would be flagged and handled safely.

  - **1.2 Address Unauthorized Assets**
    - This control forces the organization to be active when something unknown is discovered. Here, the personal infected laptop should have been quarantined/blocked from the network (thereby not allowed to access C2 or scan internal network).

  - **1.3 Utilize an Active Discovery Tool**
    - Active discovery would find new devices and services faster, without needing a user ticket. If Luigi's had active scanning/asset discovery, they would be able to find the new endpoint, and associated suspicious activity, sooner, reducing dwell time.

  - **1.4 Use DHCP Logging to Update Enterprise Asset Inventory**
    - DHCP logs the MAC address of a system when assigning an IP address, a valuable log in wireless situations. Luigi's would use this to connect suspect traffic to an individual user and device for faster containment and investigation.

  - **1.5 Use a Passive Asset Discovery Tool**
    - Passive discovery (like monitoring network traffic) can identify assets without creating noise. Passive tools would have seen the new wireless endpoints and scanning behavior for Luigi's, and the NOC would have found the infected laptop much sooner.

- **CIS Control 2 – Inventory and Control of Software Assets**
  - **2.1 Establish and Maintain a Software Inventory**
    - A software inventory helps to mitigate "unknown unknowns". If a device is allowed on the network, Luigi's should still know what software it has. It can be used to track risky

applications, unusual tools, and software which could be indicative of compromise or poor security posture.

- **2.2 Ensure Authorized Software is Currently Supported**
  - Unsupported software is high risk because it no longer receives security patches. If Luigi's enforced supported versions only, it would shrink attack surface and make it harder for malware to leverage known vulnerabilities on endpoints and servers.

- **2.3 Address Unauthorized Software**
  - This control is an action step for when unauthorized software is found. PSL malware, as well as any droppers that are associated with it, would likely fall under the category of "unauthorized" allowing the organization to swiftly remediate it and prevent execution or persistence.

- **2.4 Utilize Automated Software Inventory Tools**
  - Automation is essential for scale and accuracy. Manual inventories get out of date quickly. Automated tools allow Luigi's to rapidly pinpoint unmanaged devices and suspicious software, particularly after weekends or high-volume operational periods.

- **2.5 Allowlist Authorized Software**
  - Allowlisting is one of the most effective means of preventing malware execution, because it inherently restricts what can be executed. If Luigi's had an allowlist of what could run on corporate endpoints (and enforced it for any BYOD that was allowed to connect), PSL would have had a much more difficult time executing.

- **CIS Control 3 – Data Protection**
  - **3.1 Establish and Maintain a Data Management Process**
    - Data management describes how sensitive data is stored, shared, and retired. A defined process would prevent Luigi's engineering drawings and legal documents from residing on an anonymously accessible FTP share without governance.

  - **3.2 Establish and Maintain a Data Inventory**
    - A data inventory lists where "crown jewel" data resides. Had Luigi's known its FTP server contained sensitive program folders, they would have enacted stricter controls (access, monitoring, and change management) prior to an attacker discovering it.

  - **3.3 Configure Data Access Control Lists**
    - Access control lists provide controls against anonymous access and to enforce least privilege. This countermeasure directly affects the anonymous FTP problem by requiring authentication/authorization so that only approved users and service accounts can read sensitive directories.

  - **3.6 Encrypt Data on End-User Devices**
    - Even if an endpoint was stolen or compromised, encryption makes data in storage more difficult to exfiltrate. While Luigi's primary exfil vector was FTP, encrypting data on endpoints limits overall exposure and adds to a defense-in-depth posture.

  - **3.13 Deploy a Data Loss Prevention (DLP) Solution**
    - DLP detects and prevents sensitive data from exiting the organization. In Luigi's case, DLP might have identified large transfers of proprietary drawings or legal documents, particularly to untrusted locations, giving another opportunity to prevent exfiltration.

- **CIS Control 4 – Secure Configuration of Enterprise Assets and Software**
  - **4.1 Establish and Maintain a Secure Configuration Process**
    - Secure configuration is the process of standardizing, hardening, and baselining configurations and tightly controlling any exceptions. In Luigi's case, this would

minimize misconfigurations such as anonymous services and promote consistent, secure configurations across all servers, endpoints, and network devices.

  - **4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure**
    - Network devices (wireless controllers, switches, routers) should have hardened settings as well. This protection also ensures that secure Wi-Fi authentication, segmentation rules, and safe management settings are enforced so an infected endpoint cannot easily access internal services.

  - **4.4 Implement and Manage a Firewall on Servers**
    - Server firewalls restrict who can communicate with sensitive services. Had the FTP server been under stricter firewall rules, only known approved internal systems (or subnets) could have connected to it, instead of a random wireless endpoint.

  - **4.5 Implement and Manage a Firewall on End-User Devices**
    - Endpoint firewalls limit lateral movement and scanning impact. With host firewall policy in place the infected laptop's ability to scan services or accept inbound connections would be reduced, and anomalous behavior could be logged and alerted on.

  - **4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software**
    - Turning off unused services reduces the attack surface. In this example, FTP might not have even been required, or it should have been replaced with a more secure file transfer method. Disabling FTP gets rid of the precise route the attacker took.

- **CIS Control 6 – Access Control Management**
  - **6.1 Establish an Access Granting Process**
    - An access granting process makes access intentional and auditable, rather than “open by default”. For Luigi's it means that services like file repositories aren't accessible to just anyone. This greatly reduces the risk of wide exposure.

  - **6.2 Establish an Access Revoking Process**
    - Revocation eliminates residual access that attackers could exploit. Although the attacker used anonymous FTP in this scenario, strong revocation practices minimize overall risk by ensuring that accounts and permissions are revoked when no longer required.

  - **6.3 Require MFA for Externally-Exposed Applications**
    - MFA prevents many credential-based attacks. If Luigi’s had any externally accessible portals (including remote admin tools), MFA would reduce the risk of attackers using stolen credentials to facilitate persistence or data theft.

  - **6.4 Require MFA for Remote Network Access**
    - Since the attacker was able to exfiltrate data over an encrypted VPN channel, remote access controls are relevant. Multi-factor authentication (MFA) for remote network access can help ensure only approved remote sessions are active and make it more difficult for attackers to misuse VPN services or stolen credentials.

  - **6.7 Centralize Access Control**
    - Centralizing access control increases consistency and makes monitoring simpler. For Luigi, centralized access means it's easier to enforce policies (no anonymous access), apply least privilege, and quickly audit who accessed sensitive data.

- **CIS Control 10 – Malware Defenses**
  - **10.1 Deploy and Maintain Anti-Malware Software**

- This would have been the first line of defense against PSL malware. Consistent anti-malware on endpoints helps prevent infection, detect known threats, and provide defenders with early warning when suspicious files or processes appear.

  - **10.2 Configure Automatic Anti-Malware Signature Updates**
    - Expired signatures mean missed detections. Think of Luigi's issue of his "known bad" list going out of date. Automatic updates mean it's less likely for defenses to go out of date, and less likely for a known malware family such as PSL to evade them.

  - **10.5 Enable Anti-Exploitation Features**
    - Exploit techniques are often used by modern malware to achieve persistence or privilege escalation. Anti-exploitation features (such as memory protection) can block malicious behavior even when there are no signature matches, increasing resilience to new threats.

  - **10.6 Centrally Manage Anti-Malware Software**
    - Central management gives visibility and enforcement. The problem with Luigi's was that the personal laptop was not centrally protected; centralization is one way to help ensure policies are applied, alerts are reviewed and exceptions are investigated.

  - **10.7 Use Behavior-Based Anti-Malware Software**
    - Behavior-based detection is useful when malware variants are frequently changing. PSL contacting C2 and enumerating internal services is abnormal behavior; behavior-based tools may detect that activity even if the file hash is previously unknown.

- **CIS Control 12 – Network Infrastructure Management**
  - **12.1 Ensure Network Infrastructure is Up-to-Date**
    - Current infrastructure hardens attack surfaces of wireless devices, routers, and switches. Luigi's attack was not a device exploit in and of itself, but updated infrastructure limits opportunity for attackers to chain vulnerabilities post-compromise.

  - **12.2 Establish and Maintain a Secure Network Architecture**
    - This defense supports segmentation, limited paths, and bounded trust. With secure architecture, Luigi's BYODs would not be on the same network as their sensitive servers. Scanning could not originate from a wireless endpoint to reach internal file services.

  - **12.4 Establish and Maintain Architecture Diagram(s)**
    - Diagrams make it clear to defenders what should exist and where critical systems live. If Luigi's had kept diagrams up to date, it would have been easy to see that FTP is in the wrong zone, apply segmentation, and rapidly review suspicious paths.

  - **12.5 Centralize Network Authentication, Authorization, and Auditing (AAA)**
    - AAA centralization also makes it simpler to control which devices can connect to the network and to log it. In Luigi's situation, AAA would allow for stronger wireless authentication (as opposed to "any device gets DHCP") and better audit trails for forensics.

  - **12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work**
    - Having admin-specific resources ensures that administrative activity is less likely to take place from a malicious endpoint. This is not the cause in this instance, but I still consider it noteworthy. This is because once attackers pivot, one of the things they will attempt is admin activity; securing admin flows will help mitigate lateral movement.

- **CIS Control 13 – Network Monitoring and Defense**
  - **13.1 Centralize Security Event Alerting**

  - Central alerting is what closes the loop on NOC findings so that we actually get a security response. Luigi's had a ton of encrypted traffic so central alerting with good escalation would have shortened response time and enabled fast containment rather than having to wait until Tuesday.

  - **13.3 Deploy Network Intrusion Detection Solutions**
    - NIDS can identify scanning, suspicious connections and known malicious behavior. In this scenario it could have detected internal service scans, abnormal FTP access patterns, or C2 traffic, and alerted defenders to isolate the endpoint before exfiltration was complete.

  - **13.4 Perform Traffic Filtering Between Network Segments**
    - Segmentation with filtering between segments limits lateral movement. If Luigi's had filtered wireless to server traffic, an infected BYOD device could not have reached the FTP server directly. This is an explicit preventive control for this attack chain.

  - **13.6 Collect Network Traffic Flow Logs**
    - Flow logs show who spoke to whom, when, and how much. Since Luigi's traffic was encrypted, the flow data can still be used for detection (big transfers, odd destinations) and for forensics even without decryption keys.

  - **13.9 Deploy Port-Level Access Control**
    - Port-level access control can prevent unauthorized devices from being able to join. This is one of the best responses to the case: the personal laptop should not have been able to join the corporate network unless it could meet certain security requirements.

- **CIS Control 14 – Security Awareness and Skills Training**
  - **14.1 Establish and Maintain a Security Awareness Program**
    - A formal awareness program leads to a more standard set of expectations and behaviors. For Luigi's, such a program would clearly spell out the policies for personal devices, network access and so on, and what an employee should do if a device misbehaves before they leave on vacation.

  - **14.2 Train Workforce Members to Recognize Social Engineering Attacks**
    - Most malware infections begin with the human element getting fooled first, and awareness training also lowers the odds of an employee unwittingly bringing an already-infected device into the office.

  - **14.6 Train Workforce Members on Recognizing and Reporting Security Incidents**
    - If this employee had reported the performance problems earlier, perhaps before Friday when he left, the laptop may have been quarantined that day. Training to report leads to quicker escalation and less time for the attacker to scan and exfiltrate data.

  - **14.8 Train Workforce on Causes of Unintentional Data Exposure**
    - This control covers accidental activities that result in exposure, like the use of personal devices, copying files to unmanaged drives, or connecting to sensitive networks without permission. It directly enables the prevention of risky decisions like "BYOD on corporate Wi-Fi".

  - **14.9 Train Workforce Members on the Dangers of Connecting to and Transmitting Corporate Data Over Insecure Networks**
    - Training in this area can help employees understand why network segmentation exists, as well as why there are rules about connecting to the corporate network. It helps drive the point home that "convenience connections" can create actual security incidents and supports a culture where employees don't try to circumvent controls.

- **CIS Control 17 – Incident Response Management**
    - **17.1 Designate Personnel to Manage Incident Handling**
      - Assigning responsibility for incident response ensures timely and consistent decision making even during off-hours. If Luigi's had incident commanders and deputies identified, a response to the large, encrypted transfers detected over the weekend would not have waited until the next business day.

    - **17.3 Establish and Maintain an Enterprise Process for Reporting Incidents**
      - Reporting processes should simplify how employees and the NOC raise alarms about suspicious events. A well-defined process would ensure the abnormal traffic, and the user's "slow laptop" symptoms, are treated as a potential incident, not just a routine help desk ticket.

    - **17.4 Establish and Maintain an Incident Response Process**
      - A written IR process spells out containment, evidence preservation, communication, and legal procedures. In Luigi's incident, it would specify how to isolate the infected device, how to preserve logs and track evidence, and how to quickly triage the FTP server to see how much data loss occurred.

    - **17.7 Conduct Routine Incident Response Exercises**
      - Exercises will allow your teams to respond more quickly under stress and help improve cross-team coordination. If Luigi's had exercised the "data exfiltration over encrypted channels" scenarios, the NOC and desktop team could have coordinated containment more quickly, and shortened time to action.

    - **17.9 Establish and Maintain Security Incident Thresholds**
      - Thresholds determine what constitutes escalation conditions (big outbound encrypted data, unknown devices, internal scanning, etc). Luigi's observed a ton of traffic, but thresholds would automate the response and tie the time sensitivity of the escalation to the goal of minimizing the window of opportunity for successful exfiltration.

References:

- CIS. (2023). *CIS Critical Security Controls*. CIS. https://www.cisecurity.org/controls
- Center for Internet Security. (2024). *CIS Controls Version 8*. CIS. https://www.cisecurity.org/controls/v8
- Center for Internet Security. (2019). *Download the CIS Controls*. Cisecurity.org. https://learn.cisecurity.org/cis-controls-download
- Center for Internet Security. (2024). *The 18 CIS Controls*. CIS. https://www.cisecurity.org/controls/cis-controls-list
- *CIS Controls Navigator*. (n.d.). CIS. https://www.cisecurity.org/controls/cis-controls-navigator