JEDSON JERUME
1/22/26

Company Case Study: Luigi's

1. Issues at Luigi's that need to be addressed:

Unmanaged / Unauthorized Device Issues

- Employee connected a *personal, infected* laptop to the corporate Wi-Fi.
- No enforcement of BYOD restrictions or device-health checks.
- No NAC (Network Access Control)–unknown devices allowed full internal access.

Network Segmentation & Architecture Failures

- Wi-Fi network was not segmented from core corporate systems.
- Personal laptop could directly scan and access internal FTP server.
- Weak or absent firewall/ACL controls between segments.

Data Protection & Access Control Failures

- FTP server allowed **anonymous access**.
- High-value proprietary data stored on an insecure internal FTP service.
- No data classification, encryption, or "need-to-know" permissions.

Endpoint Security Gaps

- Personal laptop had **no corporate anti-malware** or endpoint protection.
- No security baseline enforcement on connecting devices.

Monitoring & Threat Intelligence Failures

- NOC observed large encrypted outbound traffic but did not treat it as an incident.
- Threat-intel list was 4 months out of date.
- No automated detection/alerting for unusual egress patterns.

Incident Response Weaknesses

- Weekend activity not escalated despite red flags.
- User noticed slow behavior Friday but left the laptop on all weekend.
- Ticketing workflow delayed actual response until Tuesday.

Security Awareness Weaknesses

- User unaware of BYOD risks.
- User failed to report suspicious system behavior.
- Staff lacked training to treat anomalies as potential incidents.

JEDSON JERUME
1/22/26

Company Case Study: Luigi's

2. CIS Controls v8 That Could Have Prevented the Attack

2.1 CIS Control 1 – Inventory and Control of Enterprise Assets

Why this control is important:

This control makes sure that the organization knows about all the devices on its network that are allowed and not allowed. Luigi's could have stopped or isolated the personal laptop before it could connect to the internal Wi-Fi and start scanning internal systems if they had a good inventory of their assets and could automatically find unknown hardware. The infection would have been stopped at the edge of the network.

2.2 CIS Control 3 – Data Protection

Why this control is important:

Data Protection forces organizations to classify, store, and restrict access to sensitive data. Luigi's proprietary documents, legal files, and patents should never have been on an anonymously accessible FTP server. Proper classification, encryption, access controls, and segmentation would have prevented the malware from reaching or exfiltrating highly sensitive business information.

2.3 CIS Control 10 – Malware Defenses

Why this control is important:

Malware defenses make sure that all endpoints have anti-malware tools that are up to date and administered from one place. If Luigi had required compliance endpoint protection before letting the laptop connect to the network, the infected laptop would have been found, blocked, or put in quarantine right away. This would have stopped PSL malware from spreading around the network without anyone knowing for a few days.

2.4 CIS Control 12 – Network Infrastructure Management

Company Case Study: Luigi's

Why this control is important:

This control requires organizations to build secure network architecture, enforce segmentation, and tightly manage network devices. Luigi's Wi-Fi network should have been isolated from sensitive corporate systems using VLANs and firewall rules. The infected laptop should never have been able to communicate with the internal FTP server or reach internal corporate resources.

2.5 CIS Control 13 – Network Monitoring and Defense

Why this control is important:

This control makes sure that businesses keep an eye on traffic patterns, employ NIDS/NIPS, keep their threat intel up to date, and find strange things. Luigi witnessed encrypted egress traffic that seemed suspicious, but he didn't report it as an issue. Alerts would have gone off if proper monitoring and up-to-date intelligence feeds had been in place. This would have led to prompt containment instead of waiting till the long weekend was over.

2.6 CIS Control 14 – Security Awareness and Skills Training

Why this control is important:

Awareness training prevents dangerous user behavior. Luigi's employee connected an unmanaged personal laptop and ignored clear signs of malware infection. With proper training, staff would know not to connect BYOD devices, recognize suspicious behavior, and report incidents immediately instead of leaving an infected machine connected for days.

2.7 CIS Control 17 – Incident Response Management

Why this control is important:

Incident Response Management provides structured processes to identify, escalate, contain, and recover from incidents. Luigi's lacked clear escalation workflows, leading to days-long delays. With proper IR processes, the anomalous encrypted traffic observed over the weekend would have triggered rapid triage and containment, dramatically reducing data loss.

JEDSON JERUME
1/22/26

Company Case Study: Luigi's

3. Safeguards Needed for Each Control

CIS Control 1 – Inventory & Control of Enterprise Assets

1.1 – Establish and Maintain Asset Inventory
Luigi's needs a real-time catalog of all authorized devices. This inventory is the foundation for identifying rogue systems such as the personal laptop, which should have been blocked or isolated from corporate networks immediately.

1.2 – Address Unauthorized Assets

This safeguard requires removing, quarantining, or isolating unknown devices. Luigi's could have automatically blocked the personal laptop at Wi-Fi onboarding, stopping malware activity before it began.

1.3 – Utilize an Active Discovery Tool
Active scanning tools continuously detect devices attached to the network. Luigi's could have discovered the unmanaged laptop instantly, triggering alerts and preventing lateral reconnaissance to the FTP server.

1.4 – Use DHCP Logging to Update Inventory
DHCP logs would show new, unknown devices receiving IP addresses. Correlating these logs with asset inventory could have highlighted the personal laptop as non-corporate, prompting immediate action.

CIS Control 3 – Data Protection

3.2 – Establish and Maintain a Data Inventory
Luigi's would have formally identified sensitive information, like proprietary drawings and patents. Once classified as "high sensitivity," such data would require stronger protections and would not sit on an anonymous FTP server.

3.3 – Configure and Enforce Data ACLs
Proper access control lists would prevent anonymous or unnecessary access. Malware using anonymous FTP login would have been denied access entirely, preventing exfiltration.

3.7 – Implement Data Classification Scheme
This ensures sensitive data receives the highest safeguards. With a classification program, Luigi's

Company Case Study: Luigi's

would place engineering documents behind strong authentication and controlled storage—not on a publicly accessible file service.

CIS Control 10 – Malware Defenses

10.1 – Deploy and Maintain Anti-Malware Software
Luigi's needs anti-malware installed on all devices connecting to the network. This safeguard would prevent infected devices from joining the network or detect PSL malware immediately.

10.2 – Ensure Automatic Signature Updating
Up-to-date signatures are critical for detecting new threats. Luigi's could have identified PSL earlier if anti-malware was required and automatically updated on all endpoints.

10.6 – Centrally Manage Anti-Malware (IG2)
Central management allows Luigi's to enforce minimum health requirements, block non-compliant devices, and see real-time infection events across the enterprise.

CIS Control 12 – Network Infrastructure Management

12.2 – Secure Network Architecture
Segmentation prevents lateral spread. Luigi's Wi-Fi should never allow direct access to sensitive internal systems. Proper architecture blocks BYOD from reaching core assets.

12.5 – Centralize Network AAA
User/device authentication ensures only authorized systems join internal networks. Luigi's would have identified the personal laptop as untrusted and restricted it automatically.

12.6 – Use Secure Authentication for Wi-Fi (e.g., 802.1X)
Advanced Wi-Fi authentication prevents unknown devices from joining trusted networks. This safeguard would have confined the personal laptop to a restricted guest network.

CIS Control 13 – Network Monitoring & Defense

13.1 – Centralize Security Event Alerting
A SIEM would correlate logs (DHCP, traffic anomalies, FTP access). Luigi's could have escalated the suspicious encrypted traffic immediately.

13.3 – Deploy NIDS/NIPS
Intrusion detection could catch malware scanning and unusual outbound VPN activity. Luigi's would have seen clear indicators of compromise early.

JEDSON JERUME
1/22/26

Company Case Study: Luigi's

13.4 – Enforce Traffic Filtering
Filters between networks block unauthorized communications. Luigi's could have prevented Wi-Fi clients from ever communicating with the internal FTP server.

13.6 – Collect Flow Logs
Flow logs reveal patterns like large exfiltration bursts. Luigi's NOC would have had stronger evidence to escalate the incident over the weekend.

CIS Control 14 – Security Awareness & Skills Training

14.1 – Security Awareness Program
Users must understand why BYOD is restricted and how malware behaves. This safeguard helps prevent risky user behaviors like connecting unvetted devices.

14.6 – Train Workforce to Report Incidents
Training reduces dwell time. The employee should have disconnected the laptop immediately instead of leaving it on for days.

CIS Control 17 – Incident Response Management

17.1 – Designate Incident Handling Roles
Clear responsibility ensures red flags (like Luigi's weekend traffic spike) get immediate attention.

17.3 – Establish an Incident Reporting Process
Staff need a clear method to escalate suspicious activity. A defined process would have triggered containment earlier.

17.4 – Maintain an Incident Response Plan
Playbooks guide real-time response. Luigi's would have isolated the laptop and FTP server sooner, minimizing data theft.