Hello [Manager],

Please find below a brief analysis of Premium House Lights Inc.'s current network architecture, followed by recommendations for security improvements. Please note that this is only a brief assessment, and that I do recommend a full Risk Assessment be performed in order to gain a more complete understanding of PHL inc.'s security posture and needed improvements.

Organization Configuration Analysis and Associated Risks

The current configuration of the network is as follows: The Production VLAN and Employees VLAN are on separate subnets (***10.10.1.0/24*** and ***10.10.5.0/24*** respectively), each with their own dedicated switch. The Production VLAN encompasses three servers: the Webserver (***10.10.1.2***, which is also accessible from the internet as it hosts PHL's website), the Database (***10.10.1.3***) and the File Server (No IP Address given); the Employees VLAN hosts the physical store's WIFI network, which includes both the laptops and tablets for the store. Both of these networks are protected via a Firewall from regular internet traffic, but the web server, again, is accessible from the internet via the company's website.

The first major risk that can be seen is that while the Production VLAN appears to be protected from internet traffic, it is actually exposed due to the presence of the Web Server, and thus places the Database and File Servers both at risk. The next major risk is that the Employees Network operates as a Wifi network for both the laptops and tablets, which means that if the network is compromised, it is open to exploitation. Furthermore, as there is no guest Wifi, it can be assumed that employees are connecting their devices to the store's wifi, enabling additional threat vectors.

Key Vulnerabilities and Threats

From the above assessment, it can be observed that PHL inc.'s security posture is dubious at best. From the web server acting as a potential backdoor to the production network, to the wireless network's ubiquitous use in the brick and mortar store, there are many opportunities for abuse of the system by malicious actors. Key areas to focus remedial efforts on are as follows:

- **External Threats**
    - **Web Server:** The web server's configuration and relative positioning in the network make it a source of many threats:
        - SQL Injection: If the website's code is not properly audited and secured, attackers could exploit it to access or manipulate the Database server, which is on the same VLAN.
        - Cross-site scripting (XSS): Attackers could inject malicious scripts into the website, potentially stealing confidential data or compromising user sessions.
        - Cross-Site Request Forgery (CSRF): Users could be tricked into performing actions on the website without their knowledge

        - DDoS Attacks: The external-facing web server could be targeted by Distributed Denial of Service (DDoS) attacks, overwhelming itt and causing downtime.
        - Unpatched Software: Any software or systems used on the web server or database might have vulnerabilities that can be exploited if not kept up-to-date with the latest stable security patches.
- **Internal Threats:**
    - **Network Segmentation Issues:** The current network configuration is the root of many threats, such as:
        - Inadequate Isolation: If there are any misconfigurations in the VLAN, an attacker gaining access to the Employees VLAN could potentially reach the Production VLAN, especially if there are no user group permissions established.
        - Insider Threats: Employees or ex-employees with malicious intent or compromised credentials could access sensitive data or systems.
    - **Unsecured WiFI Network:** The Employees VLAN is vulnerable to exploitation if not properly secured. Weak WI-Fi encryption or poor password practices could expose it to unauthorized access.
- **Data Security Threats:**
    - **Data Breaches:** The database and file server containing customer and organizational data are high-value targets. Unauthorized access to these systems could lead to a breach of sensitive data.
    - **Inadequate Data Encryption:** If data at rest (e.g., in the database or on the file server) or data in transit (e.g., between the web server and customers) is not properly encrypted, it could be intercepted or accessed by unauthorized parties.
- **Operational Threats:**
    - **Configuration Errors:** Misconfigurations in the firewall or network settings could inadvertently expose internal systems or data to the public or unauthorized users.
    - **Lack of Redundancy:** If the company's critical systems (e.g., web server, database) do not have redundancy or backup measures, a hardware failure or attack could lead to significant downtime or data loss.
    - **Physical Security:** The brick-and-mortar store's physical security needs to be considered to protect against theft or tampering with inventory tablets and other equipment.

Assessing and applying risk management processes

Based on the criteria listed above, it is evident that there are many unmitigated risks for PHL inc.'s operations. In order to ensure that all major risks are assessed and have mitigation applied to them, I suggest applying the ***National Institute for Standards and Technology's Risk Management Framework (NIST RMF)***. This will allow for a more in-depth and continuous review of PHL inc.'s operational risks and security posture, while also offering avenues of improvement in the form of applicable controls. Best of all, there are no fees attached to the ***NIST RMF*** documentation, which makes it fit into any budget, and the controls are

system-agnostic - that is to say, they do not reference any specific technology implementations, allowing organizations to choose solutions based on their budget and technological stack.

Examples of ***NIST 800-53 Controls*** that would be applicable to the risks outlined in the previous section are:

- **AT-02 LITERACY TRAINING AND AWARENESS**
    - Provides a framework for how to apply policies and implement training.
- **CP-02 CONTINGENCY PLAN**
    - Provides a framework for identifying mission-critical assets and business functions.
- **PL-02 SYSTEM SECURITY AND PRIVACY PLANS**
    - Provides a framework for identifying security and privacy concerns given the usual business functions.
- **RA-03 RISK ASSESSMENT**
    - Details how to run a full risk assessment
- **SC-05 DENIAL-OF-SERVICE PROTECTION**
    - Provides a framework for identifying and mitigating DDoS attacks.

Key security policy inclusions

Given the concerns outlined above, it is clear that while there are guidelines to actions that can help improve the organization's security posture, there are also certain needs that must be immediately codified and acted upon. These actions include, but are not limited to:

- **Website security policies**
    - Implement Web Application Firewall (WAF) to protect against common web vulnerabilities.
    - Regularly update and patch the web server and application software.
    - Conduct regular security assessments and vulnerability scans.
- **Network security policies**
    - Ensure VLANs are properly isolated and implement strict firewall rules between them.
    - Use strong encryption for Wi-Fi networks and secure access points with complex passwords and up-to-date security protocols (ex: WPA3).
    - Segregate the web server from the production environment on its own VLAN.
    - Add a "Guest" Wi-Fi network VLAN for the brick-and-mortar store, which has traffic monitored and no access to the store's operations VLAN, the web server or the Production VLAN.
    - Implement monitoring and logging to detect suspicious network traffic and operations.
- **Data Protection**
    - Encrypt sensitive data both in transit and at rest.
    - Implement strong access controls and regularly review access permissions.
    - Backup critical data regularly and test the restore process.

- **Insider Threats**
    - Conduct regular employee training on security best practices, phishing awareness, and access to privileged devices such as laptops and tablets.
    - Implement monitoring and logging to detect suspicious activities on an internal level.
    - Ensure that when an employee's working relationship is terminated, that their access is immediately revoked in order to limit their impact on the organization.
    - Implement GPS tracking software on all trusted devices to ensure that they do not leave
- **Operational Resilience**
    - Develop and test an incident response plan for handling security breaches and other emergencies
    - Ensure redundancy and failover mechanisms are in place for critical business and technological systems.

Setting up monitoring of IoCs specific to the organization's needs and the threats it faces

So far, the proposed improvements in this email provide a solid foundation for PHL inc.'s security posture, but the changes listed above are not sufficient to warn of a threat that is being exploited in real-time. Monitoring network and system traffic, as well as operations, is required to have an overview of PHL inc.'s security profile; this section will highlight some ***Indicators of Compromise (IoC's)*** that should be monitored in order to ensure that the organizational data integrity is preserved.

- **HTTP Load time**
    - Monitor the time it takes for an HTTP request to be resolved against the web server
    - May be used to indicate malicious redirects, DDoS attacks or content injection
- **Database Queries**
    - Monitor a database by running a pre-configured query
    - As SQL injection attacks are hard to detect, long wait times in SQL query execution can indicate multiple chained SQL queries. These can be indicative of data manipulation, copying or destruction
- **File Server**
    - Monitor changes to files and timestamps
    - May be used to guard against data manipulation, destruction as well as defacement
- **Bandwidth Usage**
    - Monitor bandwidth usage across the network
    - May be used to verify network traffic via bandwidth usage, as well as possible data exfiltration over web services
- **Trusted Device Usage**
    - Log who has access to trusted devices such as tablets and laptops, when they are being used and by whom.

- **Security Software Status**
    - Monitor the status of the security software (Firewalls, antivirus, etc…) to ensure they are active and up to date
    - Deactivation of security software can indicate an attack is taking place
- **User Creation and Privileges**
    - Monitor the creation of users as well as the escalation of their privileges
    - Can be used to identify an attack in progress, as attackers attempt to increase their access level on the system.

While the list above is detail-rich, it should not be assumed to be an exhaustive investigation of PHL inc.'s cybersecurity posture. The purpose of this brief assessment is to illustrate some of the current gaps in PHL inc.'s security vis-a-vis their stated commitments to protecting customer data, as well as securing their own operational procedures and records from uninvited actors.

I invite you to share this with the C-Suite, as well as any other interested stakeholders (such as the management of the brick-and-mortar store), and am also prepared to make a more detailed presentation in order to give a more complete picture; there are some principles that were not presented in this report that can help add to the organization's security posture, such as implementing the Least Privilege Principle, that I do not have time to detail here. I don't foresee the presentation taking more than 15 minutes, and I would definitely leave room to answer any questions or concerns that the stakeholders might have.

Lastly, I will leave you with the following information: *According to IBM's metrics, the average cost of a data breach in 2024 was **4.88 million USD*** (Source). You can ask the stakeholders how much they would be willing to invest in order to prevent a loss of that magnitude, and they might seem more receptive to some minor expenditures.