LIGHTHOUSE LAB

CYBERSECURITY

CYBER BEST PRACTICES

OLADAPO OLUWAYALE

Content **Page**

Executive Summary

As the newly appointed Cyber Security Manager, it is imperative to implement a proactive and comprehensive cybersecurity strategy to safeguard the company's employees, sensitive data, and digital infrastructure. With the increasing frequency and sophistication of cyber threats, employing a range of basic yet essential security measures is critical for minimizing risks and ensuring the organization remains protected.

This report outlines key cybersecurity practices that should be implemented across the company, focusing on both technical and non-technical employees. These measures include:

1. Strong Passwords
2. Password Expiration Policy
3. Multi-Factor Authentication (MFA)
4. Secure Email with Personal Certificates
5. VPN IPSec on Laptops
6. Encrypted Hard Drives/Flash Disks

By implementing these best practices, the company can build a strong security foundation that protects both its employees and critical data from cyber threats. This strategy is cost-effective, scalable, and easy to deploy, providing both short-term and long-term security benefits. As the Cyber Security Manager, my goal is to ensure these policies are effectively communicated and executed across all departments, fostering a culture of security awareness and responsibility.

Moving forward, it is essential to continuously monitor and update these security measures to stay ahead of evolving threats and ensure the organization's infrastructure remains resilient against potential breaches.

Key Cybersecurity Measures

1. **Strong Passwords**
   Strong passwords are a critical first line of defense against unauthorized access. A strong password typically contains a combination of uppercase letters, lowercase letters, numbers, and special characters. Using an easy-to-guess password is like locking the door but leaving the key in the lock. Weak passwords can quickly be broken by computer hackers. But it's impossible to remember a unique strong password for every account (CISA, 2025). The longer and more complex the password, the more difficult it is for attackers to crack it using brute force techniques. Encouraging employees to create unique passwords for different accounts and platforms reduces the risk of credential theft across multiple services.

Recommendation: Speak with your IT department or security manager to require strong passwords. Often, you can create settings that require user passwords to meet certain standards and criteria (such as length). Given the current threat environment, review the

policies around customer password strength and consider increasing those requirements to help them protect themselves (CISA 2025). Implement a policy requiring passwords of at least 12 characters, with complexity rules that include a mix of character types. Additionally, provide employees with guidelines for creating memorable yet secure passwords.

2. **Password Expiration Policy**
   A password expiration policy limits the risk of an attacker guessing or cracking a password before it changes. (Tenable, 2025). Passwords that are in use for extended periods increase the likelihood of an account being compromised. A password expiration policy ensures that passwords are regularly updated, reducing the time available for potential attackers to exploit outdated credentials. Regularly changing passwords minimizes the impact of any potential data breaches.

   Recommendation: Enforce a policy where passwords must be changed every 60 to 90 days. Remind employees of the importance of updating passwords and providing secure channels for resetting them when necessary. Users should change passwords regularly to ensure the network's security. Where security is a concern, good values are 30,60, or 90 days. (Microsoft, 2010)

3. **Multi-Factor Authentication (MFA)**
   MFA provides an extra layer of protection so that threat actors do not immediately gain access to your account and the sensitive information contained within if they succeed in compromising your password. (CISA, 2025). It requires users to provide multiple forms of verification, such as something they know (password or passphrase) and something they have (a mobile device or hardware token).

   Recommendation: Mandate MFA for accessing all critical systems and data. This includes using security questions, smartphone apps for one-time passwords or integrating biometric verification, where possible.

4. **Secure Email with Personal Certificates**
   Email has been a primary communication tool in the workplace for more than two decades. More than 333 billion emails are sent and received daily worldwide, and employees get an average of 120 emails daily. This spells opportunity for cybercriminals who use business email compromise attacks, malware, phishing campaigns, and a host of other methods to steal valuable information from businesses. (Microsoft, 2025). Email remains one of the most common vectors for cyberattacks, particularly phishing and business email compromise (BEC). Using personal certificates to secure email communication adds an encryption layer, ensuring that sensitive information remains

confidential during transmission. These certificates verify the identity of the sender and prevent unauthorized tampering with the message content.

Recommendation: Implement secure email standards such as S/MIME (Secure/Multipurpose Internet Mail Extensions) to encrypt and digitally sign emails containing sensitive information. Encourage employees to adopt personal certificates for email exchanges involving confidential data. By signing your email with an S/MIME certificate from SSL.com, you can assure receivers that the messages you send are *really* from you, and they can prove that *you* really sent them. Furthermore, you can use S/MIME to encrypt your email communications securely, shielding them from prying eyes while in transit. When S/MIME email is deployed throughout a business or other organization, employees can be certain that messages from their colleagues are genuine, and clients and customers can trust email sent from within the organization. (SSL.com, 2025)

5. **VPN IPSec on Laptops**
   VPN connections are essential business tools for enabling remote work. They extend an organization's network and provide the ability for remote employees to securely access company data and resources. This is done by encrypting traffic and tunneling that traffic from one location to another. (Palo Alto Networks, 2025). Virtual Private Networks (VPNs) create a secure, encrypted connection between remote devices (e.g., laptops, smartphones) and the company's internal network. Using IPsec (Internet Protocol Security) ensures data is securely transmitted over the internet by encrypting all communication. This is especially crucial for remote workers accessing the corporate network from public or unsecured networks, such as coffee shops or airports.

   Recommendation: Require all employees to connect to the company's network using a VPN, especially when working remotely. Use VPNs with IPsec protocols for enhanced security and ensure the VPN client software is regularly updated.

6. **Encrypted Hard Drives/Flash Disks for Portable Devices**
   Portable devices, such as laptops and flash drives, are often lost or stolen, leading to potential data breaches. Encrypting these devices ensures that if they are lost or stolen, unauthorized individuals cannot access the sensitive information stored on them. Full disk encryption (FDE) ensures that all data on a device is automatically encrypted, preventing unauthorized access even if the device is physically compromised. If you encrypt your flash drive, it is much more difficult for attackers to get unauthorized access to the data it contains, even if they steal it or you misplace it. (Proton, 2025)

   Recommendation: Enforce the use of encryption on all laptops and portable devices that store sensitive information. Provide employees with encrypted flash drives for

transferring sensitive files and ensure proper encryption key management protocols are followed.

Conclusion

In the current cybersecurity landscape, safeguarding company employees and information requires a multi-layered approach. By implementing strong password policies, enforcing password expiration, utilizing MFA, securing email communications with personal certificates, requiring VPNs with IPsec for remote access, and encrypting portable devices, the company can significantly reduce the risk of cyberattacks and data breaches. These basic cybersecurity practices are both cost-effective and easy to implement, offering a strong foundation for further security enhancements. As the Cyber Security Manager, it is essential to continue fostering a security-aware culture and work closely with all departments to ensure these measures are effectively implemented.

Next Steps

- Communicate the security policies to all employees and provide training on best practices.
- Implement technical tools to enforce the policies, such as password managers, MFA solutions, and encrypted storage options.
- Continuously monitor and audit security practices to ensure compliance and address emerging threats.

By taking these steps, we can ensure the company's data, resources, and employees are protected from potential cybersecurity threats.

Reference

Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). *Use strong passwords*. U.S. Department of Homeland Security. Retrieved January 11, 2025, from https://www.cisa.gov/secure-our-world/use-strong-passwords

Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). *Require strong passwords*. U.S. Department of Homeland Security. Retrieved January 11, 2025, from https://www.cisa.gov/secure-our-world/require-strong-passwords

Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). *Why strong passwords aren't enough: Your guide to multifactor authentication*. U.S. Department of Homeland Security. Retrieved January 11, 2025, from https://www.cisa.gov/resources-tools/training/why-strong-password-isnt-enough-your-guide-multifactor-authentication

Tenable. (n.d.). *C-PASSWORD-DONT-EXPIRE*. Tenable, Inc. Retrieved January 11, 2025, from https://www.tenable.com/indicators/ioe/ad/C-PASSWORD-DONT-EXPIRE

Microsoft. (2010, August 1). *Windows password requirements and recommendations*. Microsoft. Retrieved January 11, 2025, from https://learn.microsoft.com/en-us/previous-versions/technet-magazine/ff741764(v=msdn.10)

Microsoft. (n.d.). *What is email security?* Microsoft. Retrieved January 11, 2025, from https://www.microsoft.com/en-us/security/business/security-101/what-is-email-security

SSL.com. (n.d.). *Sending secure email with S/MIME*. SSL Corporation. Retrieved January 11, 2025, from https://www.ssl.com/article/sending-secure-email-with-s-mime/

Palo Alto Networks. (n.d.). *What is a VPN?* Palo Alto Networks. Retrieved January 11, 2025, from https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn

Proton. (n.d.). *USB encryption: How to protect your USB drives*. Proton. Retrieved January 11, 2025, from https://proton.me/blog/usb-encryption