Comprehensive Cybersecurity Measures

Protecting Company Information and Employees

Curtis Crawford

Table of Contents

Introduction [1](#_Toc174525753)

Strong Password Policy 2

Password Expiration Policy 3

Multi-Factor Authentication (MFA) 4

Secure Email with Personal Certificates 5

[Encrypted Hard Drives / Flash Drives 6](#_Toc174525758)

[Conclusion 7](#_Toc174525758)

Introduction

In our digital world, resilient cybersecurity is of vital importance. As the newly appointed Cyber Security Manager, it is my duty to make sure that we employ cybersecurity best practices to defend our information assets as well as our employees from growing cyber threats. The report below describes the most important cybersecurity practices to implement. These practices will serve as a blueprint for our future security strategy.

The following recommendations focus on strengthening our defence against the most common attack vectors, ensuring that we are in compliance with the relevant regulations, and protecting the reputation of the company.

# Strong Password Policy

Why It Matters:

Passwords are usually the main victim of a cyber attack. As a result, access by hackers to sensitive systems and confidential data might occur easily if employees are using weak or simple passwords. These security breaches can also lead to the loss of company confidential information. A policy for password formats protects the company against attacks and allows employees to create complex passwords that cannot be guessed or uncovered by brute-force and other methods of password-cracking.

Recommendations:

Password Complexity: Require passwords to be at least 12 characters in length and include a combination of uppercase and lowercase letters as well numbers and special characters (such as @, #, $).

Password Uniqueness: Enforces a stiff policy against reuse. That everyone ought to use a different password for every account so that if a system is breached and those passwords made available to the public, then your other accounts have a better chance of not being hacked.

Password Management Tools: Encourage the use of password managers to help employees generate and store complex passwords securely.

Benefits:

Reduces the risk of unauthorized access due to weak or reused passwords.

Enhances overall security posture by making it more difficult for attackers to compromise accounts.

# Password Expiration Policy

Why It Matters:

While passwords, even strong ones, can be cracked eventually because of the computing power available, if a password goes awry and is actually stolen, a bad actor might have continuous access to the account until the password is changed. Password expiration is a means of ensuring that passwords are refreshed on a regular basis so that a stolen password is not compromised for very long.

Recommendation:

Expiration Interval: Implement a policy requiring employees to change their passwords every 90 days.

Alerts and Reminders: Automate reminders to employees when their passwords are about to expire.

Password History: Prevent users from recycling any of their last five passwords to force them to choose a different strong password each time.

Benefits:

Minimizes the risk of long-term unauthorized access due to stolen credentials.

Encourages employees to regularly update their security practices.

# Multi-Factor Authentication (MFA)

Why It Matters:

Multi-Factor Authentication (MFA) adds a third layer of security and requires something extra in addition to entering the correct password once you get to the account sign-in page. Even if a hacker somehow guesses a password and steals it, he would still need the second factor (such as a code you receive on your mobile phone, a fingerprint scan, etc.) to get in. With MFA, the chances of an identity thief accessing your account are pretty much zero – even if they are highly sophisticated in spear-phishing or social engineering. Massive data breaches at key points have occurred, but we can still engage in self-protection.

Recommendation:

Extend MFA to All Critical Systems: Email, VPN, financial systems, whatever the critical system is.

Types of MFA: Require more than one authentication factor to be entered, for example one-time password (OTP) sent by SMS or email; authentication app, such as Google Authenticator; or biometric log-in, such as fingerprint or facial recognition.

Backups: If the main MFA isn’t available, the backup options that are in place are: Backup codes, hardware tokens, backup emails, etc.

Benefits:

Significantly reduces the likelihood of successful account compromises.

Provides an additional layer of protection for sensitive systems and data.

# Secure Email with Personal Certificates

Why It Matters:

Email is ubiquitous within business, and so are potentially sensitive emails – while the current alternative to TLS involves using third-party encrypted email services, a properly configured certificate can guarantee strong email encryption and digital signature. Without the proper use of TLS, emails can be retrieved, altered or faked, allowing someone to impersonate our companies and allowing for the intrusion of phishing attacks, wire fraud and data breaches.

Recommendation:

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a protocol for encrypting email that also allows digital signatures. Use it.

Issuing Personal Certificates: Send around personal certificates to everyone in the organisation so they can start signing email. Keep these certificates in a locked safe, among other secure documentation, long enough so that the certificates expire, and send around new ones.

Training: Train employees on how to use secure email features; train employees on what to look for in suspicious emails.

Benefits:

Protects sensitive information in email communications from interception and unauthorized access. Prevents the forgery or alteration of a message enroute and denies others the ability to add new messages to a thread. Provides protection against fake emails/websites designed to steal your information or gain access to your accounts (phishing and email spoofing attacks are significantly harder to pull off).

# VPN IPSec on Laptops

Why It Matters:

As more and more employees work from home or remote sites, they access company resources over the Internet: this increases the risk of eavesdropping onto data in transit, and of data being tampered with as it crosses from one system to the other. Using a VPN (Virtual Private Network) with IPSec (a protocol for providing authentication, confidentiality, and integrity in IP communications) ensures that all the data travelling between the employee’s device and the company’s internal network passes through a secure and encrypted communications channel.

Recommendation:

FORCED VPN USAGE: Force all remote workers to connect via VPN IPSec. Make this a requirement of connecting to any company resources and enforce this on all laptops and other devices issued by the company.

Automatic VPN, Security Group, File-sharing, Intranet: Set up devices to automatically connect to your VPN when connected to the internet or your company systems outside the office.

Regular updates: Make sure all updates are installed in the VPN software to fix security vulnerabilities and performance issues.

Benefits:

Provides a secure communication channel for remote employees, protecting sensitive data from interception.

Minimises the danger of man-in-the-middle attacks, particularly for employees operating from a public or otherwise non-protected Wi-Fi connection.

# Encrypted Hard Drives/Flash Drives

Why It Matters:

Laptops, external hard drives and USB flash drives are commonly mislaid and stolen, and thus the information they contain can fall into the hands of unauthorised persons. With encryption, any such unauthorised persons could attempt to read the now-encrypted data only if they had the decryption key.

Recommendation:

Full-Disk Encryption: Laptops and mobile devices issued by your organisation should all have full-disk encryption (such as BitLocker for Windows, or FileVault for macOS).

Portable Storage Encryption: Require encryption of all external storage media such as USB drives and external hard drives used by employees for work purposes.

Encryption Policies: Have a clearly defined policy on portable storage devices, with encryption required for sensitive data.

Benefits:

Offers data protection for sensitive information stored on mobile devices, in the event the device is lost or stolen.

Ensures compliance with data protection regulations that mandate the encryption of sensitive information.

# Conclusion

Putting in place cybersecurity measures to protect our company’s information and employees is crucial, especially when facing an increasing threat landscape nowadays. These measures should be implemented so as to reduce the risk of our information being breached and reducing the risk of any attacks on our systems.

By making sure that employees use strong password formats, two factor authentications, encryption of email communications, use of VPN and encryption of portable devices, the company will be sure that cybercriminals cannot easily access their systems and steal or destroy their useful information.