**PROJECT 8**

**Report on Encryption Best Practices**

***By Titobiloluwa (Tito) Ilori***

**Table of Content**

|  | **Sections** | | **Page No.** | |
| --- | --- | --- | --- | --- |
| **1** | **Executive Summary** | | | **3** |
| **2** | **Introduction** | | | **3** |
| **3** | **Discussion** | | | **4** |
| **3.1** | | **Use of strong passwords** | | **4** |
| **3.2** | | **Implement Password Expiration Policy** | | **5** |
| **3.3** | | **The use of Multi-Factor Authentication (MFA)** | | **6** |
| **3.4** | | **Securing Email with Personal Certificate** | | **7** |
| **3.5** | | **Virtual Private Network (VPN) configured with IPsec on the Laptops for Remote Employees** | | **8** |
| **3.6** | | **Encrypted hard and flash disks to protect portable/mobile devices** | | **9** |
| **4** | **Conclusion** | | | **9** |
|  | **Appendix A: Citations** | | | **11** |

**1. Executive Summary**

In today's ever-evolving cybersecurity landscape, implementing robust encryption approaches and practices is paramount for organizational security. The adoption of strong passwords, coupled with a well-defined password expiration policy, forms the first line of defence. This preventive measure bolsters access controls, reducing the risk of unauthorized entry and potential data breaches. Complementing this, the incorporation of Multi-Factor Authentication (MFA) significantly elevates security levels. By requiring multiple forms of verification, MFA adds an extra layer of protection against unauthorized access, even in the event of password compromise.

Securing email communications through personal certificates enhances data privacy and authenticity. This cryptographic method ensures that only intended recipients can decipher the content, preventing data leakage and tampering. Moreover, implementing a Virtual Private Network (VPN) with IPsec on laptops for remote employees establishes secure connections, safeguarding sensitive information during remote access. Encryption extends to portable devices as well, with encrypted hard and flash disks mitigating data exposure risks should these devices be lost or stolen. By integrating these encryption strategies, organizations can foster a resilient security posture, fortifying against an array of potential threats and vulnerabilities.

**2. Introduction**

Cybersecurity provides a set of measures and procedures to ensure Internet security, protecting computers, cell phones, personnel, programs, networks, servers, and data against intrusions and cybercriminal actions. It aims to prevent, identify early, and quickly eliminate vulnerabilities that could harm the company's technological infrastructure and digital data security. Therefore, in this project, I will be writing a report that explains how some basic security approaches and practices can be used to protect company assets - employees, IT devices and information from a potential Cyber Security breach.

Here are the security approaches and practices that should be used to ensure confidentiality (or privacy) and integrity of company data and authentication of employees, safely into the technological infrastructure of the company according to approved access or authorization.

* Use of strong passwords
* Password expiration policy.
* The use of Multi-Factor Authentication (MFA).
* Securing email with a personal certificate.
* Virtual Private Network (VPN) configured with IPsec on the Laptops for Remote Employees.
* Encrypted hard and flash disks to protect portable/mobile devices.

These concepts will be discussed in the Discussion section below.

**3. Discussion**

**3.1 Use of strong passwords**

According to Kaspersky.com, a strong password is the main barrier keeping most of your online accounts from being hacked1. Weak, easy-to-crack passwords are still used en masse, and a lot of people use the same password across multiple accounts they own, leaving all their data dangerously exposed to those trying to steal it.2

As a company, it is crucial that everyone employee that interacts with sensitive data, customers, and intellectual property on the internet and within the company’s technological infrastructure comply with the best practices when creating passwords. The diagram below (from Hive Systems) shows how quickly it takes a cybercriminal to crack or predict a given password depending on the complexity of it. What determines the complexity of a password is if it contains numbers, upper- and lower-case letters with symbols and its length.



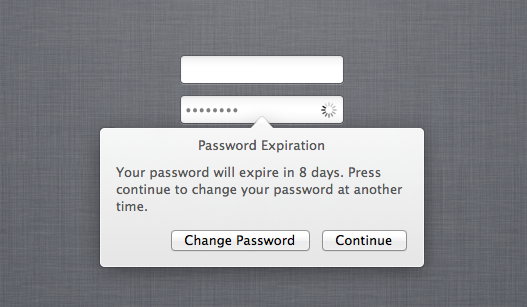
*Fig 1. Time estimates for password cracking in 2023 by Hive Systems2*

*Hive calculated these time estimates by working out how long it would take to crack different types of passwords after acquiring their “hash” values. “Hashing” is a concept in computing used to protect passwords, within which a collection of characters (i.e. a person’s password) is transformed into some other value.2*

**Recommendation:** Therefore, inferring from the above analysis, it is important to note that a password length of 12 characters and more with numbers, upper- and lower-case letters with symbols can be regarded as a “strong password”. This takes more than a lifetime (226 years) to crack.

**3.2 Implement Password Expiration Policy**

This is another best practice in cybersecurity that ensures confidentiality and authentication. The idea behind implementing password expiration is simple. If your credentials are always changing, it’s harder for an attacker to know what they are at any given time. For example, a cybercriminal might stumble upon a list of leaked passwords. But if the leak is three months old, and you rotate your password every 90 days, the information will be out of date. The attacker can’t use those credentials to get into your account.3



*Fig. 2: Notification to change password due to password expiration policy implemented.10*

However, Microsoft’s Password Guidance recommends that passwords be set to never expire. Microsoft argues, “Password expiration policies do more harm than good because these policies drive users to very predictable passwords composed of sequential words and numbers which are closely related to each other.”4

Also, NIST’s guidance suggests, “Verifiers should not require memorized secrets [passwords] to be changed arbitrarily. However, verifiers shall force a change if there is evidence of compromise of the authenticator.”5 These concerns and suggestions are valid, but we believe that moving away from password expiration policies altogether is problematic as it can lead to a weakened security posture.6

**Recommendation:** The recommendation is that passwords to highly sensitive information and critical services must meet strong password requirements and require the use of MFA and are set to expire yearly or whenever there is evidence of compromise. We should also enforce a password history policy with a password expiration policy with at least ten previous passwords remembered. This will prevent passwords that have been cracked or exposed to cybercriminals from being usable.

**3.3 The use of Multi-Factor Authentication (MFA)**

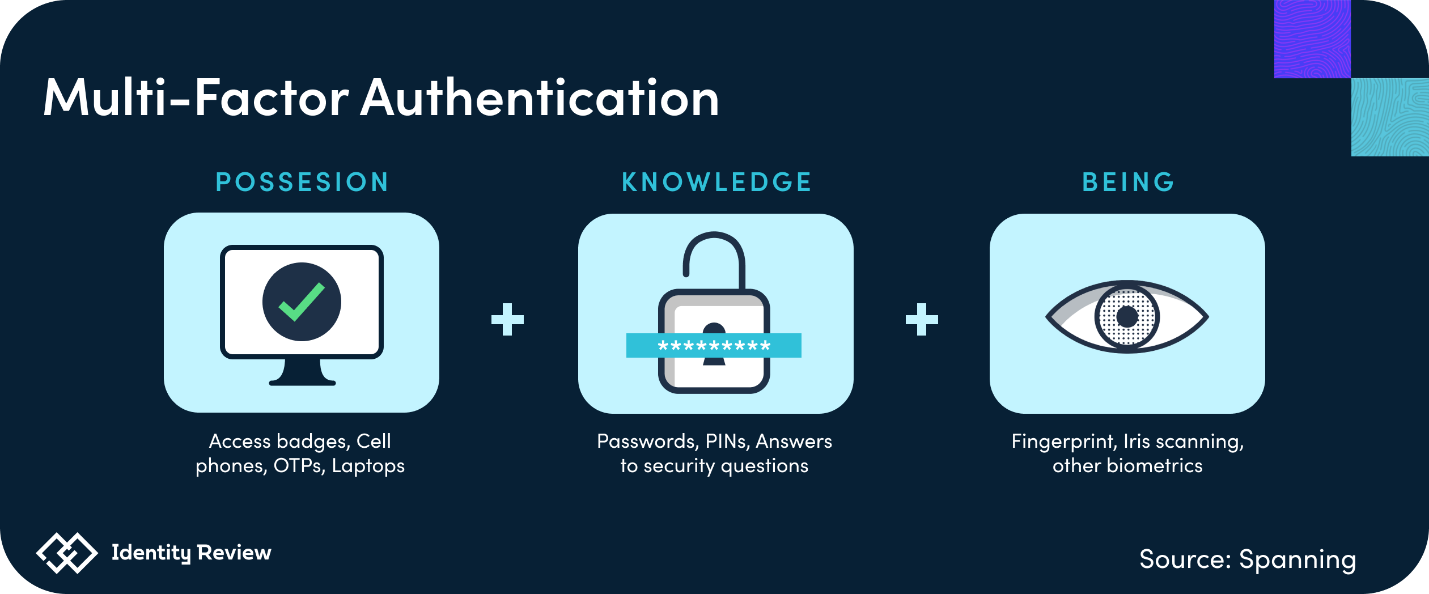
Multifactor authentication is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user’s identity for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database.7

Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. In addition, adversaries harvest credentials through phishing emails or by identifying passwords reused from other systems. MFA adds strong protection against account takeover by greatly increasing the level of difficulty for adversaries.8

**How does MFA Work?**

According to CISA (Cybersecurity & Infrastructure Security Agency), a typical MFA login would require the user to present some combination of the following:8

* Something you know (knowledge): like a password or Personal Identification Number (PIN)
* Something you have (possession): like a smart card, mobile token, or hardware token; and,
* Something you are (inherent): biometrics e.g., fingerprint, palm print, or voice recognition).



*Fig. 3: Diagram showing the types of MFA*

For example, MFA could require users to insert a smart card or a bank card into a card reader (first factor) and then enter a password or a PIN (second factor).

**Recommendation**: we will enforce MFA on all Internet-facing systems, such as email, remote desktop, and Virtual Private Networks (VPNs).

**3.4 Securing Email with Personal Certificate**

According to Digicert.com, Email encryption is a must-have in today’s digital world, especially for growing companies and global enterprises. 300 billion emails travel the internet every day, and most are completely exposed to anyone interested in stealing information, manipulating messages, or monitoring senders and recipients.9 The email recipient can be certain that the email has originated from a reliable source and hasn't been tampered with or exposed in transit by using an email encryption certificate, which is a digital (personal) certificate used to sign the email.



*Fig. 4: How a personal digital certificate is applied to an email sent to ensure authenticity and privacy.11*

Client/personal Certificates are digital certificates that identify and validate individual email senders. They are also known as Personal ID certificates, but the technical name for them is S/MIME certificates. Client certificates allow organizations to authorize or block access to apps, websites, databases, and devices.12

An S/MIME, which stands for Secure/Multipurpose Internet Extensions - certificate provides you with a public and private key pair. Your secret private key signs messages you send, and decrypts messages sent to you. The public key is shared so people receiving your messages can verify your signature, and it encrypts messages so only you can read them.9

**Recommendation**: We should use digital certificates to encrypt all outgoing emails, ensuring secure communication. This approach enhances data confidentiality, compliance, and our cybersecurity reputation.

**3.5 Virtual Private Network (VPN) Configured with IPsec on the Laptops for Remote Employees**

According to Cloudflare.com, a virtual private network (VPN) is an Internet security service that allows users to access the Internet as though they were connected to a private network. Some of the most common reasons people use VPNs are to protect against snooping on public Wi-Fi, to circumvent Internet censorship, or to connect to a business’s internal network for the purpose of remote work.13

A screen shot of a computer

Description automatically generated

*Fig. 5: Diagram illustrating VPN connections (without IPsec)13*

Meanwhile, using VPN only does not guarantee an increased level of security. It is prone to data loss due to dishonest VPN providers.13 This is why VPN configured with IPsec adds more security to the connection. IPsec (“Internet Protocol” and “Secure”) is a group of protocols for securing connections between devices. IPsec helps keep data sent over public networks secure. It works by encrypting IP packets (communication traffic or information over a network (Wi-Fi or Public internet)), along with authenticating the source where the packets come from.14

IPsec connections involve key exchange to establish encryption keys. It is like making sure your messages are safe when you send them online. It helps devices share special codes to lock and unlock messages, adds extra info to packets of data to prove they're real, and keeps the actual message hidden from anyone trying to sneak a peek. These secure packets travel through the internet using a special path, and on the other side, the messages are unlocked and ready to be used by apps.

**Recommendation**: Using an IPsec VPN is highly recommended because it comprises protocols that play a vital role in ensuring data integrity, confidentiality, and secure key negotiation across networked systems, thereby bolstering overall network security.14

**3.6 Encrypted hard and flash disks to protect portable/mobile devices.**

Encrypting both flash drives and hard drives is primarily done to prevent unauthorized individuals from accessing the data stored on them. Listed below are the benefits of encrypted hard drives and flash drives.

1. If the company’s flash drive or hard drive is lost or stolen, someone could simply plug it into a computer and access the information, unless it's encrypted.15
2. Non-encrypted hard drives and flash drives can leave the company’s technological infrastructure vulnerable to malware and other device security threats.16
3. This will help the company to comply with data protection laws such as GDPR.17
4. It will also ensure the company does not suffer loss of earnings, time, or customer loyalty.17

Therefore, to encrypt complete hard drives and flash drives, contemporary operating systems such as Windows, macOS, and Linux provide integrated encryption utilities that offer this capability. Notable instances encompass BitLocker for Windows, FileVault for macOS, and LUKS for Linux, each facilitating the encryption of drives. There is other third-party hard drive encryption software as well.18

**4. Conclusion**

In conclusion, the dynamic landscape of cybersecurity underscores the critical importance of robust encryption practices for organizational safeguarding. The establishment of strong passwords coupled with a clear password expiration policy act as an initial line of defence, enhancing access controls and minimizing unauthorized access risks. Augmenting this defence, Multi-Factor Authentication (MFA) provides an additional security layer, safeguarding against unauthorized entry even if passwords are compromised.

The utilization of personal certificates for securing email communications ensures data privacy and legitimacy, preventing unauthorized access and tampering. Furthermore, the deployment of Virtual Private Networks (VPNs) with IPsec for remote employees and encrypted hard and flash disks for portable devices solidifies data protection measures against potential threats and vulnerabilities. The amalgamation of these encryption strategies empowers organizations to establish a resilient security framework.

**Appendix A: CITATIONS**

1. Tips for Generating Strong and Unique Passwords | 2023 AO Kaspersky Lab - <https://usa.kaspersky.com/resource-center/threats/how-to-create-a-strong-password>

2. How Long Does It Take for a Hacker to Crack a Password? | Aaron Drapkin (July 14, 2023) - <https://tech.co/password-managers/how-long-hacker-crack-password#:~:text=Unfortunately%2C%20in%202023%2C%20it's%20pretty,cracked%20in%20under%2024%20hours>.

3. Do you really need to change your password every 90 days? | Nick Summers (Feb 15, 2022) - <https://blog.1password.com/should-you-change-passwords-every-90-days/#:~:text=The%20idea%20behind%20forced%20password,a%20list%20of%20leaked%20passwords>.

4. Microsoft Password Guidance | Robyn Hicock - <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf>

5. NIST Special Publication 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management | Paul A., James L., et al. - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>

6. Password Expiration Policy and Best Practices | Sarah Harvey (July 5, 2018) - <https://kirkpatrickprice.com/blog/password-expiration-policy-and-best-practices/>

7. Multi-Factor Authentication (MFA) | CISA (Jan 5, 2022) - <https://www.cisa.gov/resources-tools/resources/multi-factor-authentication-mfa>

8. Multi-Factor Authentication (MFA) | CISA (January, 2022) - <https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf>

9. Client (S/MIME) Certificates | What is a Client Certificate? | Digicert - <https://www.digicert.com/tls-ssl/client-certificates#:~:text=By%20securing%20your%20personal%20or,in%2Dthe%2Dmiddle%20attacks>.

10. NO PASSWORD EXPIRY WARNING AT THE LOGIN WINDOW ON 10.9 | Macmule - <https://macmule.com/2014/03/29/no-password-expiry-warning-at-the-login-window-on-10-9/>

11. How to encrypt email (Gmail, Outlook, iOS, Android) | Clare Stouffer (November 19, 2021) - <https://us.norton.com/blog/how-to/how-to-encrypt-email>

12. What are Client Certificates? | DigiCert FAQ - <https://www.digicert.com/faq/email-trust/what-are-client-certificates#:~:text=Client%20Certificates%20are%20digital%20certificates,%2C%20websites%2C%20databases%20and%20devices>.

13. What is a VPN? | Cloudflare - <https://www.cloudflare.com/learning/access-management/what-is-a-vpn/>

14. What is IPsec? | How IPsec VPNs work | Cloudfare - <https://www.cloudflare.com/learning/network-layer/what-is-ipsec/>

15. How to Encrypt a Flash Drive in 7 Easy Steps | Ubie (January 31, 2022) - <https://www.usbmemorydirect.com/blog/how-to-encrypt-a-flash-drive/>

16.How to encrypt a flash drive | Alison Grace Johansen ( July 13, 2020) - <https://us.norton.com/blog/how-to/encrypt-a-flash-drive>

17. Why should you use an encrypted USB Flash Drive? | USB2U (November 7, 2017) - <https://www.usb2u.co.uk/articles/2017/11/why-should-you-use-an-encrypted-usb-flash-drive/>

18. How to secure data on your external hard drives and USB peripherals | Proton Team (November 9, 2022) - <https://proton.me/blog/usb-encryption>