Cyber Best Practices

By: Danielle Daza

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document aims to provide a detailed summary of several best practices that would be beneficial in an organization's business operations. As well as detailing their essential importance in a company's network environment, the risks posed without such best practices being followed and additional actionable items to complete in conjunction with the key practice for ease of acclimatization for both employees and for senior management. The cyber best practices being explored in this report are strong passwords, password expiry policies, Multi-Factor Authentication (MFA), personal certificates in regards to securing emails, IPSec VPNs on laptops, and encrypting hard drives and flash drives to protect mobile devices.

In regards to password and account security, setting a strong, unique password for each account is essential to prevent unauthorized access. A complex password makes it much harder for attackers to guess or crack, protecting user's personal and professional data which may or may not be intertwined via passwords. With the ever-evolving threat landscape of technological advancements, the strength of a password is not enough to ensure the security of an account and company data, it would also be beneficial if it is time-restrictive. A password expiry policy would ensure that passwords are regularly updated, reducing the risk of unauthorized access over time. By forcing periodic password changes, this practice helps minimize the chances of old credentials or even accounts being exploited. In addition to a strong password that also updates in set intervals, enabling Multi-Factor Authentication (MFA) adds an extra layer of security by requiring not just a password, but also a second factor, such as a code from a mobile app or a fingerprint, making it much harder for attackers to gain access.

In terms of ensuring confidentiality and integrity in communications, encryption is fundamental requirement. As emails are such an essential part of business communications, using a personal certificate to secure email communications ensuring that messages are encrypted would

guarantee that the content and parties involved are authenticated and therefore verified as trustworthy. Such personal certificates protect sensitive information from being intercepted during transmission and verifies the sender's identity. In order to ensure security in networks, using an IPSec VPN on laptops ensures that internet traffic is encrypted, protecting transmitted data when working remotely or on public networks. It secures a user's connection and keeps sensitive information safe from third-party interception as a result of the message authentication algorithm that VPNs use. With the security of communications solidified with personal certificates and IPSec VPNs, ensuring that the hard drives and flash disks that contain all of an organization's information – financial records, customer and employee data, intellectual property, etc. – are encrypted securely as well is crucial in fortifying a company's security defensive posture. Encrypting hard drives and flash disks on mobile devices protects the data stored on them in case of theft or loss. Even if the device is physically accessed, the data remains secure and unreadable without the encryption key.

Each of these practices are important in establishing a layered defense to ensure an organization's communications and data are as secure as reasonably and logistically possible.

STRONG PASSWORD

A strong password is crucial in protecting one's credentials, and by extension, sensitive information and maintaining the security of digital systems, especially in an organization's network. This can be enforced within an organization with policies outlining a clearly defined complexity standard for passwords for employees to adhere to. The following sections will cover the importance of ensuring strong passwords are being set in a company-environment and the risks to consider that are posed in its absence.

IMPORTANCE

Below is a brief summary of key points of security importance of enforcing strong password in user accounts.

Key Consideration	Description
Protecting Sensitive Data	Strong passwords make it more difficult for unauthorized users to gain access to systems that store sensitive data such as critical business data, customer information, intellectual property, and financial records.
Preventing Data Breaches	Weak or reused passwords are easier for unauthorized users to guess or brute-force. A strong password policy helps reduce the likelihood of a successful breach, which can lead to major financial losses, legal consequences, and damage to a company's reputation.
Compliance with Regulations	Data protection regulations (such as GDPR, HIPAA, PCI-DSS) require the implementation of strong security measures, including password management. Failing to comply can lead to expensive legal penalties and loss of business.
Protecting User Accounts	Employees often have access to a variety of systems (i.e. email, databases, cloud services, internal tools), and weak passwords across these systems could lead to further compromise as compromised password leads to further breaches in other areas of the user's accounts within the company.

RISKS IN ITS ABSENCE

Below is a comprehensive table outlining the relevant risks if strong passwords are not an enforced standard in an organization.

Risk	Description
Increased Vulnerability to Cyberattacks	Without strong password policies (e.g., enforcing complexity and length), attacks such as brute force, and phishing become easier and more likely to succeed. Additionally, many employees reuse passwords across different services. If a password is exposed in one breach, unauthorized users can use it to attempt logins on other systems, potentially compromising multiple company accounts. According to a study of confirmed data breaches, 82% of breaches can be attributed to weak-reused, or stolen passwords (The Problem with Pa

	sswords , 2024).
Data Breaches and Financial Loss	Weak passwords are one of the most common causes of data breaches. A breach can lead to massive financial losses through direct theft, business disruptions, compliance fines, and the costs associated with handling and recovering from a data breach (forensics, legal fees, reputation repair). For reference, the average cost of a data breach in Canada from 2023 was $5.13 million USD (PetrosyanAni, 2024)
Loss of Customer Trust	A data breach resulting from weak security measures, such as poor password management, can significantly harm a company's reputation as customers are likely to lose trust in the company's ability to protect their personal information. For reference, in a recent survey from young adults to seniors revealed that 56% of consumers would “Not at all” trust their personal information with a company previously affected by data breaches (Statista R essearch Department, 2024).
Legal and Compliance Consequences	Many industries have strict requirements for how personal data must be protected. Failure to follow proper security practices, including enforcing strong password policies, could result in fines and penalties, and even lawsuits from affected customers. Additionally, by law, data breaches must be reported both publicly to inform customers and to the regulating authorities. This in term will, in turn, influence customer perception of the breached company’s ability to protect their information.

RECOMMENDED GUIDELINES

Below are suggestions for recommended guidelines in enforcing password complexity and strength standards.

Guideline	Actions
Follow Industry-Standards for Passwords	In the most recent NIST publication regarding strong passwords, it is recommended to have a password at least 8 characters, preferably 15 but should be allowed to go up to 64 characters to create a more complex password or passphrase (GracyMeeba, 2024).
Utilize Password Managers	Use a password manager to store passwords for lower sensitivity accounts but not for sensitive accounts such as those with administrative privileges or banking credentials and ensure the password manager is from a secure website and that it is updated regularly (Canadian Centre for Cyber Security, 2024).
Outline Password-Setting Mistakes	Within the password-setting standards, also identify the most common password-setting mistakes that result in accounts becoming more vulnerable to compromise so as to clarify what would make a password realistically strong and therefore secure.

PASSWORD EXPIRATION POLICY

A password expiration policy refers to a set of rules that require users to change their passwords at regular intervals, typically every 30, 60, or 90 days. The following sections will delve into the importance of such a policy, the risks that exist without it, potential drawbacks with this policy and recommended guidelines in order to address the drawbacks and for general policy management.

IMPORTANCE

Key Consideration	Description
Limiting the Impact of Compromised Passwords	If a password is compromised without the user's knowledge, an expiration policy limits the window of time the attacker can use the stolen credentials. The shorter the password lifespan, the less time the malicious actor has to exploit it, thus mitigating its long-term exposure in the event of a compromised password. In a 2023 report, it has been observed 83% of compromised passwords satisfied the length and complexity of regulatory password standards (WhiteMarcus, 2024), making it evident that password strength in itself is not enough to protect one's credentials.
Compliance with Industry Standards and Regulations	Many industries (e.g., financial services, healthcare, government) have regulations that mandate periodic password changes for certain types of accounts. Enforcing a password expiration policy helps ensure that the company remains compliant with these standards. Additionally, industry-standardized security frameworks such as NIST (National Institute of Standards and Technology) provide guidelines on password management, which include recommendations on expiration periods to improve overall security (BarretEllis, 2024).
Reducing Risk from Inactive Credentials	If employees or contractors leave the company or change roles, their access should be revoked. A password expiration policy helps ensure that even if access is not properly revoked, the credentials won't remain valid for an extended period of time. Additionally, accounts that are no longer in use may become forgotten, but periodic password changes help ensure that such accounts are not left vulnerable over time.

RISKS IN ITS ABSENCE

Below is an outline of the main risks posed in a company network that does not have a password expiration policy in place.

Risk	Description
Increased Risk of Stale or Compromised Passwords	If passwords are never required to expire, compromised passwords could provide long-term unauthorized access to critical systems and data. This is especially dangerous if a password has been stolen or leaked without the user's knowledge as it allows for long-term access until the compromised account has been identified. Additionally, without regular password changes, inactive accounts may

	become targets for cybercriminals who could exploit them to gain access to sensitive systems.
Password Reuse	Without expiration policies, users may get complacent and reuse passwords across multiple platforms or services. This increases the risk of a breach in one system compromising access to others. According to a recent Forbes study, 23% of users reuse a password for 3-4 different accounts and 14% reuse a password for 5-6 accounts (HaanKatherine, 2024). Moreover, a recent survey revealed that 91% of participants understood the risk of password reuse but 59% did it anyway (The Hacker News, 2024).
Inability to Detect and React to Compromise	If a company doesn't require regular password changes, an attacker who compromises a password might remain undetected for months or years. A password expiration policy would at least force periodic re-authentication, giving administrators a higher chance of detecting unauthorized users attempting to gain access. A password expiration policy minimizes the time frame these accounts can remain vulnerable. In a Varonis globally-reaching study of financial service companies of varying sizes found that 59% of companies have over 500 passwords that never expire (Varonis, 2021). This would leave their systems vulnerable to attackers manipulating non-expiring passwords for an extended period of time.
Increased Insider Threat Risk	If ex-employees retain access to corporate accounts, they could potentially misuse their credentials. While disabling accounts is the most direct approach, requiring regular password changes helps ensure that even if an account is overlooked, old passwords will eventually expire. Additionally, temporary accounts such as for temporary employees and contractors are often forgotten in the system – these are ghost accounts. A password expiration policy minimizes the time frame these accounts can remain vulnerable. As mentioned, in a Varonis globally-reaching study of financial service companies of varying sizes found that 59% of companies have over 500 passwords that never expire and nearly 40% of those companies have more than 10,000 ghost users still present in their systems (Varonis, 2021). This leaves their systems incredibly vulnerable to attackers having access to their systems for extended periods of time without detection as they are technically using authorized accounts.

POTENTIAL DRAWBACKS

Despite its benefits, password expiration policies have certain drawbacks such as user fatigue, decreased security with frequent changes, and password management complexity.

Requiring frequent password changes may lead to **frustration and fatigue** among users, causing them to adopt poor security practices such as writing passwords down or choosing weak, easily guessable passwords. In a recent Forbes study, 38% of respondents admit to writing down their passwords (HaanKatherine, 2024), a common but incredibly risky method of password

management. Weak passwords were also revealed to be the main reason respondents' accounts were breached with 35% of users identifying weak passwords as the cause (HaanKatherine, 2024).

When forced to change passwords too often, **users may resort to simple or predictable passwords** to make it easier to remember them. This can inadvertently reduce overall security. In a recent study among IT experts, employees and heads of organizations, 30% of respondents said they have experienced a security breach due to weak passwords (SebastianNathan, 2025).

With the release of the Second Public Draft of NIST SP 800-63B-4 in August 2024, experts have even suggested that overly frequent password changes **may encourage bad behavior** and might not provide as much benefit as once thought (GracyMeeba, 2024). Though it may be of use to balance the frequency of the password changes in order to minimize poor password hygiene.

Password expiration policies require robust systems for tracking expiration dates and ensuring that users are notified to change their passwords on time. It can also create an **administrative burden** to manage the periodic resets.

RECOMMENDED GUIDELINES

Below is a summary of suggestions for recommended guidelines to employ in addition to a password expiry policy if such a policy were agreed to. These recommended guidelines aim to address the potential drawbacks of managing and enforcing a password expiry policy that were outlined in the previous section.

Guideline	Description
Balance frequency	Set password expiration intervals that balance security with user convenience (e.g., 90-120 days). Avoid excessively short periods that might encourage weak passwords as this bad habit is one of the reasons why NIST no longer encourages password expiry (GracyMeeba, 2024).
Standardize strong passwords in the policy	Pair password expiration with strong password requirements (e.g., a mix of letters, numbers, special characters, and sufficient length).
Multi-Factor Authentication (MFA)	Use MFA in conjunction with password expiration to add an additional layer of security, especially for critical systems (MITRE ATT&CK, 2024).
Monitor account activity	Ensure that any changes to passwords, especially for high-value accounts, are accompanied by active monitoring to detect any unusual activity.

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is a critical security measure that requires users to provide two or more verification factors to access a system or application, making it significantly harder for unauthorized individuals to gain access. MFA typically involves something the user knows (like a password), something the user has (like a smartphone or hardware token), or something the user is (like biometric data). MFA is a highly effective defense against many types of cyberattacks, such as phishing, brute force attacks, and credential stuffing (NIST, 2024).

IMPORTANCE

Below is an outline of the key points of importance of implementing MFA in an organization's network.

Key Consideration	Description
Increased Security	Even if a password is stolen or leaked, MFA significantly reduces the likelihood of unauthorized access. Attackers would need to obtain the second (or third) factor to successfully log in. MFA helps protect against common attacks such as phishing, where attackers steal passwords via user input, and brute-force attacks, where attackers try numerous combinations to guess passwords (NIST, 2024). With MFA in place, the attacker still needs to bypass the second factor.
Compliance and Regulation	Many regulations and compliance standards (such as GDPR, HIPAA, PCI-DSS, and others) require the use of MFA for access to sensitive data, especially for systems handling financial, health, or personal information. Using MFA is often seen as a best practice for companies to demonstrate that they are taking reasonable steps to protect data.
Risk Reduction	Even if attackers manage to obtain a user's password, MFA acts as a barrier. This significantly reduces the potential for successful attacks. MFA can be applied to a variety of systems, including email, virtual private networks (VPNs), cloud storage, internal company portals, and more. This makes it harder for attackers to access multiple systems even if they steal a password. In a large dataset of Microsoft Azure Active Directory users exhibiting suspicious activity revealed that MFA reduces risk of compromise by 99.22% across the entire population and by 98.56% in cases of leaked credentials (Microsoft, 2024).

USER CONCERNS – FATIGUE AND INCONVENIENCE

Despite its advantages, MFA can introduce certain frustrations for users, which could lead to resistance or neglect of security protocols. The main concerns related to MFA implementation and enforcement in a policy is fatigue from repeated logins, usability challenges, and device dependency.

For users who need to authenticate frequently throughout the day, entering MFA credentials each time can feel tedious. This is especially true for employees who are working across multiple systems or tools that require separate logins. These repeated logins result in **fatigue from the time-consuming repeated logins**. Moreover, if MFA is required at every login or for each system access, it can interrupt a user's workflow. This might lead to reduced productivity or even cause users to circumvent security measures, such as writing down their codes or turning off MFA for convenience.

In regards to **usability challenges**, depending on the type of MFA used (e.g., SMS codes, authentication apps, biometric data), users may face issues such as not having their phone nearby, facing poor reception for SMS, or struggling with facial recognition due to lighting conditions or other factors.

Lastly, in terms of **device dependency**, if MFA relies on a smartphone or hardware token, losing that device can lock users out of systems. Although backup methods (such as secondary authentication options) can be provided, this could still lead to delays and frustrations among users. There is also the potential concern of dual-device reliance as users who rely on their mobile phones for MFA may experience issues if their phone is dead, out of service, or experiencing technical difficulties.

COSTS AND CHALLENGES FOR IMPLEMENTATION

While MFA provides clear security benefits, some companies may be deterred from implementing it due to perceived costs and challenges. The major points of concern are the initial setup costs, ongoing maintenance costs, employee training, and logistically costly challenge.

The MFA **initial setup** costs derive from the purchase of the necessary software/setup of the MFA infrastructure, and the process of system integration. Implementing MFA may require purchasing third-party software, hardware tokens, or setting up an MFA infrastructure (e.g., for SMS or email-based authentication) (Microsoft, 2024). This can represent a significant upfront investment which typically leads to MFA becoming a lower priority in business expenses. In a global study regarding MFA awareness and implementation among varying business sizes, 35% of respondents cite funding for MFA tooling being the most challenging part of MFA implementation.

In regards to the **ongoing maintenance** costs, companies will need to provide user support for MFA-related issues. Employees may forget their MFA device, have trouble with authentication, or need help with backup codes. This can lead to additional helpdesk workload and operational costs. Moreover, the subscription and licensing fees are also an aspect of the maintenance fees to consider. If using third-party MFA services (e.g., for SMS-based authentication or biometric systems), companies will incur recurring fees. In the previously cited study, 12% of respondents citing that resources with maintenance being the most challenging aspect of MFA implementation (Cyber Readiness Institute, 2022).

There is also the cost of **employee training** to consider. Employees may require training to understand the new MFA system, how to properly use their authentication devices, and how to resolve common issues. This incurs additional time and resources which would result in a period of time where productivity is somewhat stalled during the transition. Additionally, some employees might resist MFA due to the perceived inconvenience, leading to the need for additional efforts to get buy-in and compliance from staff.

Lastly, the costs of MFA would greatly depend on the company size. In larger companies, rolling out MFA across many users and systems can be a challenge in terms of the **logistical rollout**. Managing permissions, ensuring that all systems are compatible with MFA, and ensuring scalability as the organization grows can add complexity to the implementation. Furthermore, the growing trend of remote work presents challenges in terms of securing a wide variety of endpoints (e.g., personal laptops, mobile devices), requiring additional configuration and setup to ensure consistent security measures across all devices.

ADDRESSING USER CONCERNS AND MITIGATING COSTS

Below is an outline of suggestions to address potential user concerns and mitigate the costs associated with MFA implementation.

Suggestion	Concerns/Costs Addressed	Rationale
Streamline MFA Methods	• User Fatigue	Implementing adaptive MFA adjusts the level of authentication required based on the risk level, user behavior, or device type (Cyber Ark, 2023). For example, MFA might only be prompted when logging in from a new device or location, reducing the number of times users are asked to authenticate.
	• User fatigue	Combining Single Sign-On (SSO) with MFA allows users to log in once with both their password and MFA, and then access multiple applications without needing to authenticate again (C yber Ark, 2023). This helps reduce the frequency of MFA requests and streamlines access.
Offer Multiple Authentication Options	• Usability challenges • Device dependency	Providing multiple authentication methods, such as mobile apps (Google Authenticator, Authy), push notifications, or biometrics, gives users flexibility and helps ensure that MFA remains convenient even in different contexts (e.g., at home vs. at the office) (SheldonRobert, 2023).
	• Device dependency	Allow users to set up backup authentication methods, such as backup codes or alternative devices, to mitigate the risk of being locked out if their primary device is unavailable.
Educate Employees	• User fatigue • Employee training	Offering clear and concise training on the benefits of MFA and how to use it properly can help employees understand its importance and reduce resistance. Making sure employees know how to resolve any issues they encounter (e.g., lost devices) also improves overall adoption. In a recent study across several countries regarding MFA, 28% of employees respond that the reason they resist MFA is simple because they do not know how to set it up (Cyber Read iness Institute, 2022). Additionally, in that same study, 50% of respondents cite employee resistance being the least challenging in MFA implementation (Cyber Readiness Institute, 2022).
Gradual Rollout and Scaling	• Initial setup • Logistical rollout	A phased or pilot rollout of MFA can help businesses manage costs and address any issues on a smaller scale before implementing it across the entire company.
	• Ongoing maintenanc e • Logistical rollout	Cloud-based solutions (such as those provided by Microsoft, Okta, or Duo) offer a more cost-effective, scalable approach compared to on-premise solutions, as they eliminate the need for significant infrastructure and are easier to integrate with cloud services (KrystrianMarisa, 2024).

SECURE EMAIL WITH PERSONAL CERTIFICATE

A secure email with personal certificates plays a critical role in ensuring confidentiality, authenticity, and integrity in email communications within a company. Personal certificates, also known as digital certificates, are used to encrypt email contents and verify the identity of the sender. They are issued by trusted authorities (Certificate Authorities or CAs) and serve as a form of public-key infrastructure (PKI).

HOW PERSONAL CERTIFICATES WORK

For reference, this is a simplified explanation of the process of how the use of personal certificates are used in email messaging.

Step	Actions
1. Issuance of Personal Certificate	• The user obtains a personal certificate from a trusted Certificate Authority (CA). The CA verifies the identity of the person requesting the certificate (BarveApurva, 2023). • The personal certificate contains both a public key and a private key (BarveApurva, 2023).
2. Encrypting and Signing the Email	• Encryption: The sender uses the recipient's public key (which the sender has obtained, either directly or via the CA) to encrypt the contents of the email (BarveApurva, 2023). Only the recipient, with their private key, can decrypt and read it. • Digital Signing: The sender uses their own private key to sign the email, ensuring its authenticity and integrity (BarveApurva, 2023).
3. Receiving the Email	• The recipient receives the email, which is both encrypted and signed. • Decryption: The recipient uses their private key to decrypt the message and read the contents (BarveApurva, 2023). • Signature Verification: The recipient can verify the sender's digital signature using the sender's public key (often distributed via the CA or embedded in the email) (BarveApurva, 2023). This confirms that the email has not been altered and was indeed sent by the stated sender.

IMPORTANCE

Below is an outline of the main points of concern regarding the transmission of emails that personal certificates would ensure is addressed. NIST recommends the use of certificate authentication methods in the transmission of emails (RoseScott, NightingaleJ.S., GarfinkelSimson, C handramouliRamaswamy, 2019).

Key Consideration	Description
Confidentiality	Personal certificates enable email encryption, meaning that only the intended recipient with the appropriate private key can decrypt and read the contents of the email. This prevents unauthorized individuals (e.g., attackers or malicious insiders) from intercepting and reading sensitive data

	sent via email.
Authenticity	Digital certificates ensure that the email actually came from the claimed sender and has not been spoofed or impersonated. This is especially important in a corporate environment where email is a primary form of communication (Perception Point, 2023). Without a personal certificate, an attacker could forge the "From" address in an email, making it appear to come from someone within the company (e.g., a senior executive), potentially leading to fraudulent actions like wire transfers or unauthorized access to company resources.
Integrity	Personal certificates can also ensure the integrity of the message. If the email's content is tampered with during transmission, the encryption will fail, and the recipient will know that the email was altered (BarveApurva, 20 23). This is vital for preventing data manipulation or the spread of misinformation. Personal certificates ensure that the sender cannot deny having sent the email. This is important for legal and audit purposes. For instance, if a company sends sensitive information or performs an action (e.g., confirming a contract), the email can serve as an irrefutable record of that action (Perception Point, 2023).
Compliance with Regulations	Many industries have strict regulations around data protection, such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), or Payment Card Industry Data Security Standard (PCI-DSS), which require that sensitive or confidential information is transmitted securely (CarterScott, 2024). Using personal certificates for email encryption can help ensure compliance with these regulations and avoid fines or penalties.

RISKS IN ITS ABSENCE

Below is an outline of the major risks posed in a company environment without personal certificates used in email transmissions.

Risks	Description
Data Breaches	Email is often transmitted over the internet in an unsecured manner, and without encryption, the contents can be easily exposed during transit. A lack of secure email practices could expose, for example, financial reports, trade secrets, or customer data, leading to identity theft, financial fraud, and severe reputational damage. It has been reported that Man in the Middle (MITM) attacks – wherein a third party is able to intercept a 2-way transmission of data – via email has increased by 35% since 2022 as reported into Q1 2023 (SmithGary, 2024).
Impersonation and Phishing Attacks	Without digital certificates, it becomes easier for attackers to impersonate company executives, employees, or clients. Attackers can send fraudulent emails, such as fake invoices or requests for wire transfers, hoping to trick recipients into taking unauthorized actions. This is a common tactic used in business email compromise (BEC) attacks, which can result in significant

	financial losses. In a report done by security company Egress, 94% of organizations reportedly fell victim to phishing attacks in 2023 (Trend Micro, 2024). The use of personal certificates would ensure that email senders are appropriately authenticated to avoid this very common cyber-attack which typically lead to other more serious incidents of attack such as malware and ransomware.
Legal and Compliance Violations	As mentioned, many industries are bound by strict data protection laws that require secure communications of sensitive information (CarterScott, 2024). If a company does not use secure email or personal certificates, it could violate regulations such as GDPR, HIPAA, or PCI-DSS. This can lead to legal actions, fines, and penalties.

RECOMMENDED GUIDELINES

Below are some suggestions of supplementary actions to implement in conjunction with the use of personal certificates in email transmissions.

Guideline	Description
Implement Mandatory Email Encryption	Require the use of personal certificates for all email communications that contain sensitive or confidential data. Ensure that emails are encrypted by default, especially when communicating with external clients or stakeholders.
Educate Employees	Train employees on how to use digital certificates and why it's essential to sign and encrypt emails. Provide guidance on how to verify the authenticity of an email, especially when receiving attachments or links.
Use Digital Signatures	Enforce the use of digital signatures to confirm the sender's identity and ensure that the email content has not been altered. This adds an additional layer of security and helps prevent phishing attacks.
Adopt Strong Email Security Tools	Utilize email security software that automatically handles encryption and signing. Ensure that both inbound and outbound emails are scanned for malicious content, and that encryption is enforced as necessary.
Regularly Update Certificates	Ensure that personal certificates are regularly updated and renewed to maintain their validity. Expired or invalid certificates can compromise the security of email communications.

IPSEC VPN ON THE LAPTOPS

VPN stands for **Virtual Private Network**, and **IPsec** is short for **Internet Protocol Security**. Together, a VPN with IPsec on laptops provides a secure way for employees to connect to their company's network, especially when working remotely or using public internet connections, like at cafes or airports.

A **VPN** creates a secure tunnel between the laptop and the company's network as if the laptop is within the company's physical environment for network connection. This tunnel encrypts all the data sent and received over the internet, ensuring that no one can read or intercept it, even

when using a public Wi-Fi network (BarkerElaine, DangQuynh, FrankelSheila, ScarfoneKaren, WoutersPaul, 2020).

IPsec is a technology used within the VPN to encrypt and secure the communication between the laptop and the company's network (Maricris, 2023). With an IPSec VPN, remote users can send and receive data wherever they are, and the risks of data loss or interception are low. Companies can also integrate an IPSec VPN into firewall setups, extending cybersecurity protection to network devices in bedrooms, airport lounges, or coffee shops (Nord Layer, 2024).

When working remotely or on public networks, data can be exposed to cyber threats. For example, attackers can use tools to intercept data on an unprotected Wi-Fi network. A VPN with IPsec prevents this by encrypting a user's data, making it unreadable to anyone trying to intercept it.

IMPORTANCE

Below is an outline of key points of importance in utilizing IPSec VPN on laptops.

Key Consideration	Description
Confidentiality	All data transmitted between a user's laptop and the company's network is encrypted, so even if attackers try to access it, they will not be able to read it. As VPNs use symmetric cryptography, this method of encryption generally more efficient and requires less processing power than asymmetric cryptography, which is why symmetric encryption is typically used to encrypt the bulk of the data being sent over a VPN (BarkerElaine, DangQuynh, Frankel Sheila, ScarfoneKaren, WoutersPaul, 2020).
Safe Remote Access	Employees can securely connect to the company network from any location, whether they are at home, traveling, or working from a coffee shop (Nord Lay er, 2024).
Integrity and Authentication	Integrity is provided by a message authentication algorithm. The authentication algorithm takes the input data and secret integrity key and produces a MAC (a digital fingerprint). After the data and MAC are sent across the network, the receiver calculates the MAC on the received data using the same secret integrity key (which has been previously established between the sender and receiver). If there is any change in the message and/or its MAC, a verification of the MAC will fail, and the message must be discarded (BarkerElaine, DangQuynh, FrankelSheila, ScarfoneKaren, WoutersP aul, 2020). In short, if the digital fingerprint of the original message changes, the message will be discarded which ensures that all communications are authentic.

RISKS IN ITS ABSENCE

Below is an outline of the main risks associated with not using IPSec VPNs with laptops that are worth considering.

Risk	Description
Unprotected Data	Without a VPN, data sent over the internet, especially on public Wi-Fi, is vulnerable to interception, meaning attackers could access sensitive company information or personal data.
Increased Exposure to Attacks	Employees connecting without a secure VPN could be at risk of phishing, malware, or data breaches, especially when working from unsecured networks.
Loss of Confidential Information	If a hacker gains access to unencrypted communication, they could obtain sensitive business data, client information, or even login credentials.

RECOMMENDED GUIDELINES

Guideline	Actions
Use Strong Authentication	Ensure the VPN login credentials (username/password) are long, unique, and complex, potentially using a password manager to store them securely. If possible, enabling two-factor authentication (2FA) for added security would also be beneficial.
Keep Software Updated	Always make sure that the VPN software being used is up-to-date with the latest patches. This helps protect against vulnerabilities and ensures users are using the most secure version of the software. Enable automatic updates for both the VPN client and the operating system on the laptop.
Enable Kill Switch or Always-On VPN	A kill switch is a feature that automatically disconnects the internet if the VPN connection drops. This prevents data from being exposed if the VPN unexpectedly disconnects. Use Always-On VPN settings if possible. This ensures that the VPN connection is active as soon as the laptop connects to the internet, so there are no moments of unencrypted data transmission.
Secure the Laptop	Enable full disk encryption on users' laptops to protect the data if the laptop gets lost or stolen. Ensure that users' laptops have strong local security, like a password or biometric authentication (fingerprint or face recognition), to prevent unauthorized access.

ENCRYPTED HARD DRIVES/FLASH DISKS

ENCRYPTION

Full Disk Encryption (FDE) encrypts the entire hard drive of a laptop or external hard drive. This means that everything on the device—documents, applications, system files, etc.—is encrypted and can only be accessed with the correct password or decryption key (PekkarinenLassi, 2022). Common tools for full disk encryption include BitLocker (Windows), FileVault (Mac), and Linux Unified Key Setup (LUKS).

USB flash drives are smaller, portable, and often used for transferring files between devices. By encrypting a USB drive, it is ensured that any data stored on it is secure, even if the USB drive is lost or stolen. Many USB flash drives come with built-in hardware encryption, meaning the drive itself is encrypted and can only be accessed by authorized users (PekkarinenLassi, 2022).

IMPORTANCE

Below is a summary of the key points of importance of encryption in regards to protecting portable mobile devices.

Key Consideration	Description
Password Protection and Key Management	Encryption will always require a key/password, meaning users need to enter a password or use a decryption key to unlock the device and access the data. This adds an extra layer of security on top of encryption. Proper key management is essential. If the encryption key is lost or forgotten, the data on the encrypted device could be inaccessible. Companies should have a secure method for managing encryption keys, such as using password managers or centralized encryption management solutions.
Protects Sensitive Data and Prevents Data Breaches	Data encryption ensures that even if one's portable device is lost or stolen, the data on it remains unreadable to unauthorized people. Encryption ensures that stolen devices do not become a gateway for attackers to access valuable company data, passwords, or intellectual property (Encrypt Sensitive Information , 2019). This is especially important for devices that store personal information, confidential business data, or customer details. It is also important for remotely-working employees who are at a higher risk of losing their physical devices in public spaces. For example, if an employee's laptop or a USB stick containing sensitive company documents is stolen, encryption ensures that no one can access that data without the decryption key.
Compliance with Regulations	Many industries have strict regulations around data protection, such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and PCI-DSS. These regulations often require encryption to ensure that personal or sensitive data is protected (Subabrata, 2024). If sensitive data is stored unencrypted on a portable device and it gets lost or stolen, a company could face heavy penalties or legal repercussions for violating these data protection laws.

RISKS IN ITS ABSENCE

Below are the main risks associated with not encrypting hard drives and flash disks.

Risk	Description
Data Breaches and Leaks	If sensitive data is stored unencrypted on a portable device and it gets

	lost or stolen, the consequences can be severe. The stolen data could be used for identity theft, financial fraud, or corporate espionage, leading to data breaches or leaks (Encrypt Sensitive Information , 2019).
Legal Consequences	Many industries are governed by strict regulations that require sensitive data to be encrypted. If a company fails to encrypt devices and a data breach occurs, it could face legal penalties, fines, or lawsuits due to non-compliance with data protection laws. For example, PCI-DSS fines can start from $5000 per month for 1-3 months of non-compliance and goes up to $100,000 per month when the period of non-compliance exceeds 7 months (Subabrata, 2024).
Loss of Confidential Information	Without encryption, if an employee's laptop or USB drive is lost, valuable company data (e.g., intellectual property, business contracts, customer information) could fall into the wrong hands, potentially resulting in competitive disadvantages or financial loss.
Ransomware Risks	If unencrypted devices are compromised, ransomware attacks can be more devastating. An attacker could gain access to all the unprotected data and hold it hostage for a ransom, which could disrupt business operations resulting in further financial consequences. In a recent survey among 350 CISOs, 24% of organizations paid a ransom yet could still not recover their data (Veeam, 2024).

RECOMMENDED GUIDELINES

Below are suggestions for additional actions to take in regards to the encryption of hard drives and flash disks.

Guideline	Description
Utilize Built-in Encryption Tools	Enable full disk encryption on laptops and other devices using the built-in tools, such as BitLocker (Windows), FileVault (Mac), or LUKS (Linux). For flash drives, choose drives with hardware encryption or use software like VeraCrypt to manually encrypt the drive (BartschAndre, 2022).
Set Strong Passwords	Ensure that encryption is combined with strong passwords or passphrases. A weak password can ultimately undermine the security of the encryption.
Backup Encryption Keys	Securely store backup copies of encryption keys or passwords. If a key is lost, the data will be inaccessible, so it's important to have a secure backup and recovery process.
Implement Company-Wide Encryption Policies	Enforce company-wide encryption policies for all portable devices. Ensure that all employees understand the importance of encryption and are using it for laptops, flash drives, external hard drives, and any other portable storage devices.
Educate Employees	Provide training on the importance of data encryption and how to properly use encryption tools. Employees should be aware of the risks associated with unencrypted devices and understand how to ensure their devices are secured.

REFERENCES

Encrypt Sensitive Information . (2019, June 11). Retrieved from MITRE ATT&CK: https://attack.mitre.org/mitigations/M1041/

Barker, E., Dang, Q., Frankel, S., Scarfone, K., & Wouters, P. (2020). *Guide to IPSec VPNs.* Toronto: National Institue of Standards and Technology.

Barret, E. (2024, February 10). *What's new - NIST Password Guidelines September 2024*. Retrieved from oneAdvanced: https://www.oneadvanced.com/news-and-opinion/whats-new---nist-password-guidelines-september-2024/

Bartsch, A. (2022). *Guide to VeraCrypt – Safely Encrypt Files.* Retrieved from Experte: https://www.experte.com/it-security/veracrypt

Barve, A. (2023). *What is a S/MIME Certificate and How Does It Work?* . Retrieved from SSL2BUY: https://www.ssl2buy.com/wiki/what-is-smime-certificate-how-does-it-work

Canadian Centre for Cyber Security. (2024, February). *Best practices for passphrases and passwords (ITSAP.30.032).* Retrieved from Canadian Centre for Cyber Security: https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032

Carter, S. (2024, August 27). *Why Are Email Certificates Necessary?* Retrieved from Venafi: https://venafi.com/blog/why-are-email-certificates-necessary/

Cyber Ark. (2023). *What is Adaptive Multi-Factor Authentication (MFA)?* Retrieved from Cyber Ark: https://www.cyberark.com/what-is/adaptive-mfa/

Cyber Readiness Institute. (2022). *Global Small Business Multi-Factor.*

Gracy, M. (2024, November 27). *NIST Password Guidelines: 11 Rules to Follow (Latest Version Updated).* Retrieved from Sprinto: https://sprinto.com/blog/nist-password-guidelines/

Haan, K. (2024, June 3). *America's Password Habits*. Retrieved from Forbes: https://www.forbes.com/advisor/business/software/american-password-habits/

Keeper. (2023). *Password Management Report.*

Krystrian, M. (2024, September 19). *Top 10 multi-factor authentication (MFA) providers and software*. Retrieved from Rippling: https://www.rippling.com/blog/mfa-providers

Maricris. (2023, October 24). *Do Laptops Support IPsec VPN Protocols? (Explained)*. Retrieved from Medium: https://medium.com/@maricris5/do-laptops-support-ipsec-vpn-protocols-explained-ee9479652d13

Microsoft. (2024). *How effective is multifactor.* Retrieved from Microsoft: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW166lD

MITRE ATT&CK. (2024, October 14). *Modify Authentication Process: Multi-Factor Authentication*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/techniques/T1556/006/

NIST. (2024, March 12). *Multi-Factor Authentication.* Retrieved from NIST: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication

Nord Layer. (2024). *IPsec (Internet Protocol Security) VPN*. Retrieved from Nord Layer: https://nordlayer.com/learn/vpn/ipsec/

Pekkarinen, L. (2022). *Hard Drive and Full Disk Encryption: What, Why, and How?* Retrieved from Miradore: https://www.miradore.com/blog/hard-drive-encryption-full-disk-encryption/

Perception Point. (2023). *Email Security Protocols: SMTPS, STARTTLS, DMARC, and More*. Retrieved from Perception: https://perception-point.io/guides/email-security/email-security-protocols/

Petrosyan, A. (2024, Sept 12). *Statista*. Retrieved from Average cost of a data breach in Canada from 2019 to 2024 : https://www.statista.com/statistics/1346934/canada-average-cost-incurred-by-a-data-breach/

Rose, S. W., Nightingale, J., Garfinkel, S., & Chandramouli, R. (2019, February 25). *Trustworty Email*. Retrieved from NIST: https://www.nist.gov/publications/trustworthy-email-0

Sebastian, N. (2025, January 9). *Top Password Strengths and Vulnerabilities: Threats, Preventive Measures, and Recoveries.* Retrieved from GoodFirms: https://www.goodfirms.co/resources/top-password-strengths-and-vulnerabilities

Sheldon, R. (2023, October). *Google Authenticator* . Retrieved from Tech Target: https://www.techtarget.com/searchsecurity/definition/Google-Authenticator

Smith, G. (2024, December 10). *Cyber Security Breach Statistics 2025*. Retrieved from Station X: https://www.stationx.net/cyber-security-breach-statistics/

Statista Ressearch Department. (2024, August 2). *Share of adults in the United States who would trust with their personal information a company previously affected by data breaches as of May 2024, by age*. Retrieved from Statista: https://www.statista.com/statistics/1483268/us-trust-personal-information-company-data-breach/

Strong Password Policy. (2023). Retrieved from MITRE: https://d3fend.mitre.org/technique/d3f:StrongPasswordPolicy/

Subabrata. (2024, October 10). *PCI DSS Fines: How Much Will It Cost?* Retrieved from Sprinto: https://sprinto.com/blog/pci-dss-fines/

The Hacker News. (2024, September 23). *Why 'Never Expire' Passwords Can Be a Risky Decision* . Retrieved from The Hacker News: https://thehackernews.com/2024/09/why-never-expire-passwords-can-be-risky.html

The Problem with Passwords . (2024, January 23). Retrieved from Elatec: https://www.elatec-rfid.com/int/blog/is-the-password-obsolete-cracking-the-password-problem

Trend Micro. (2024, June 20). *Worldwide 2023 Email Phishing Statistics and Examples*. Retrieved from Trend Micro: https://www.trendmicro.com/en_ca/ciso/23/e/worldwide-email-

phishing-stats-examples-2023.html

Varonis. (2021). *2021 Data Risk Report.*

Veeam. (2024). *2024 Ransomware Trends Report.* Retrieved from Veeam: https://go.veeam.com/ransomware-trends-executive-summary-2024-na?st=adwordspaidsearch&utm_source=google&utm_medium=cpc&utm_campaign=01P-PMIX_NA_EN_CAN_Paid-Search_WP_Ransomware-Trends-2024-NB_1AW&utm_content=cid|22089686798_ntw|g_adgr|178710907611_creativ

White, M. (2024, October 21). *Never expire passwords? Why we shouldn't ditch password expiry just yet.* . Retrieved from Specops: https://specopssoft.com/blog/why-we-shouldnt-ditch-password-expiry/