**Strengthening Cybersecurity Measures Safeguarding Employees and Corporate Resources**

Introduction: In today’s digital era where information technology is the lifeblood of every company, the security of both personal and confidential data is paramount of importance. As the newly appointed Cyber Security Manager, I present a detailed report about essential strategies and methodologies to safeguard the organization from cyber threats. This report is tailored to individuals with varying levels of technical expertise, offering insights to strengthen the cyber security framework.

**Key points to safeguard your company’s and employees network.**

1. **Prioritize Robust Passwords:**

• Emphasizing the importance of strong passwords as the first line of defense

* + Staff members should be trained and made aware of what constitutes a strong password as well as the potential consequences of a cyber-attack on the company and the individuals.
* Guiding employees on creating complex and secure passwords.
  + Staff members will have to create passwords that include upper and lower cases, a number, a special character, and the length will be a minimum of 12 characters.

1. **Cooldown after a certain number of failed attempts:**

* Cooldown after too many numbers of unsuccessful attempts
  + If a staff member has too many unsuccessful attempts within a span of 1 hour, for example (the number of attempts can be determined by the organization or by GRC), he will be locked out of his workstation/device.
* To have access to his workstation/device after too many failed attempts the staff will have to contact the IT department or wait for the cooldown period.

1. **Reinforcing Password Expiry Policies:**

• Explain the importance of periodic password updates (every 90 days, for example).

* + The system should/will automatically request a staff member to change their password every 90 days. This will ensure that any breaches or leaks of old credentials are rendered obsolete.
* Balancing the equation between security and user convenience through thoughtfully designed policies.
  + This affects the activities of the organization. It is important to have a secure organization. However, the policies must not be too restrictive for the company. For instance, it is possible to create a system that requires the users to log 4 different passwords of a minimum of 12 characters each. The organization would be more secure, but it would slow down the operations. People forget their passwords easily, and it will slow down everyone if they are locked out of their workstations for every failed attempt on 4 different passwords.

1. **Multi-Factor Authentication (MFA):**

• Inform the staff members about the efficiency of MFA in enhancing security layers.

• Illustrate the effect of the combine effects of MFA to proactively authorized access entry.

* + When connecting from a new device, even if all the credentials are correct, It is suggested to have the user answer a question through text message or through email to confirm their identity. This would reduce the chances of having an unauthorize party log into the staff’s account.

• Create a path/ flow to integrate MFA into our operational landscape.

* + The MFA is an effective solution to protect systems from being infiltrated, but the process needs a bit of structure. For instance, we need to create conditions of it’s implementation. The example above is a good one. Do we require MFA when someone is connecting from a new device, when someone is connecting from outside the office, from outside the country, etc. Creating clear guidelines and workflow will create an optimal use of MFA and limit unnecessary interruption of the company.

1. **Elevating Email Security with Personal Certificates:**

• Making email communication more secure through the utilization of personal certificates only you and the person you are reaching out to can understand

• Enabling encryption of email content and attachments using asymmetric keys, which involves a pair of keys – a public key for encryption and a private key for decryption – adding an extra layer of protection.

* + Making emails like “secret codes” that only the sender and the receiver can understand using a special pair of keys. One key to lock the email/message and the other to unlock it.

1. **Securing Remote Work with VPN IPSec:**

• Using the potential of VPN IPSec to ensure secure remote access using symmetric keys, where the same key is used for both encryption and decryption, ensuring secure communication between remote locations.

• Creating a strong communication channel for off-site personnel.

* + Using virtualization to create that communication would be optimal to secure the organization. It is the principle of segmenting your communication infrastructure, by isolating different networks and systems to prevent unauthorized access and potential breaches. This approach enhances security by establishing controlled boundaries and minimizing impact of potential vulnerabilities.

1. **Safekeeping Portable Devices Through Encryption:**

• Elaborating on disk encryption and its role in protecting portable devices using symmetric keys, providing a straightforward method to secure data on these devices.

* + The mention of a symmetric key indicates that the encryption method involves using the same key for encrypting and decrypting the data. In the context of disc encryption, symmetric keys are used to secure and access the data.

**Improving our Cyber Security Landscape:** To solidify our organization's digital resilience, a comprehensive review and enhancement of our cyber security policy is essential. By collaboration among stakeholders, we can align our practices with emerging threats and regulatory mandates, creating a unified stance against potential breaches.

**Conclusion**: In an era where digital landscapes define our progress, the protection of our employees and sensitive data is a shared commitment. By integrating the strategies detailed in this report, we erect a barrier against cyber threats, ensuring the integrity of our digital ecosystem. Together, we forge ahead towards a more secure, resilient, and fortified future.

**References/Weblinks:**

1. <https://www.comparitech.com/blog/information-security/cryptanalysis-explained/>
2. <https://www.nist.gov/cryptography>
3. <https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111>
4. <https://cybercoastal.com/cryptography-cheat-sheet-for-beginners/>
5. <https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html>