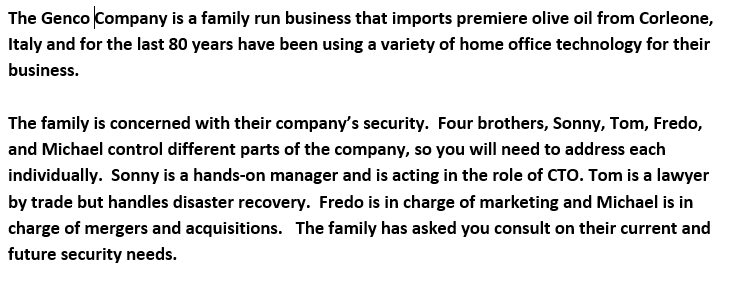
**

Response:

**a)** From a technical perspective, Tom’s solution to protect customers’ personally identifiable information (PII) using a polyalphabetic substitution of the data is not sufficient. Using a polyalphabetic substitution entails performing multiple alphabetic substitutions of the contents of the clear data, as defined by a key of alphabets to produce a ciphertext of alphabets so that the original contents of the data can be hidden. However, this method of encryption, which was also used by the Vigenere cipher is easy to break. An attacker can analyze the ciphertext to determine which groups of the same letter words appear multiple times, and then figure out the key of alphabets used to encrypt the groups by a particular shift value each time. Additionally, the technique allows the person to deduce the possible key length. The attacker can also use frequency analysis to study the frequency of letters appearing in the ciphertext, and then find their likely corresponding plaintext alphabets by exploiting the uneven distribution of alphabets in a language, which eventually allows him or her to determine the key used to encrypt. Hence, polyalphabetic substitution methods or polyalphabetic cipher, which uses this encryption technique, shouldn’t be used to protect confidential or sensitive data such as PII. Their encryption method is merely weak, easy to break, and doesn’t prevent customers’ data from leaking.

**b)** The solution I propose to Tom in response to addressing his customers’ data leaking concern and complying with state regulations involves using a more rigorous cipher that utilizes Initialization vector or nonce to implement random encryption of data. The reason behind using them is that such ciphers are harder to break into or have a higher work factor. Additionally, they are not vulnerable to frequency analysis due to the increased unpredictability of ciphertext they produce and have larger key lengths compared to polyalphabetic ciphers. Some of these robust encryption algorithms I would suggest are the block cipher, AES-256, and the asymmetric algorithm, RSA-2048 (when collecting PII over the internet). These algorithms perform more complex computations and make it difficult for an attacker to determine the original message from a given encrypted data. The implementation of such ciphers is essential to protect confidential or sensitive information such as PII of customers from being leaked.

Response:

**a)** The major concerns with symmetric key exchanges are challenges associated with securely distributing keys across unsecured medium and guaranteeing that no one would be able to tap the communication channels. As a result, securely exchanging key would require an out of band key exchange where Fredo and another party would share a symmetric key in one communication channel and then exchange the data that is encrypted in a different communication channel. However, this technique of exchange is inconvenient. Additionally, communication with multiple entities requires Fredo to establish distinct keys with each entity, resulting in an increased total amount of keys needed for communication.

**b)** Fredo can securely exchange cryptographic keys using a hybrid cryptography method, which is a combination of asymmetric key cryptography and symmetric cryptography. The asymmetric cryptography part of the method allows him to exchange the keys over an insecure channel without any pre-established shared secret with the person he is going to communicate with while the symmetric part of the method allows him to encrypt and decrypt the marketing data faster. For example, let say we are using RSA algorithm for asymmetric cryptography and AES for symmetric cryptography. Fredo wants to work with Alexis, who works for a marketing firm, to develop plans to market the company’s new olive oil products based on the available marketing data of the company. Alexis first sends her RSA public key to Fredo. Fredo then encrypts the AES symmetric key with her RSA public key. He also encrypts the secret marketing data with the AES symmetric key and sends it to her together. Alexis then decrypts the symmetric key with her RSA private key. She also decrypts the message containing the marketing data with the AES symmetric key. Alexis and Fredo can now encrypt and decrypt messages to each other using the symmetric key or session key since it has been securely exchanged.

Another method for key exchange is Diffie-Hellman. When using Diffie-Hellman, Fredo and Alexis exchange each other’s public keys, a large prime number, and a generator which is a number smaller than the prime number. Then, both of them use the prime number, the generator, each other’s public key, and their own private key to calculate a shared secret key through a series of mathematical computations. Once they have the shared secret key, they establish a session to encrypt and decrypt messages to each other.

One thing to note here is that both mechanisms for securely exchanging keys can be vulnerable to a man-in-the-middle-attack. An attacker listening to the traffic between Fredo and Alexis can intercept, impersonate each one of them and send his public key to establish the shared secret key with one of them. Due to this, a Certificate Authority that both Fredo and Alexis trust should be used to confirm that the public key really came from the expected person and that their identity is correct.

Response:

**a)** Some of the ways that Michael could defeat the cryptosystems used by his rival firms include interrupting, intercepting, and modifying the rival’s cryptographic systems through different types of passive and active attacks. These attacks vary from attacking the cryptographic key to attacking the cipher or algorithm, analyzing the cryptosystem implementation to find weaknesses, manipulating the captured data to find clues about the keys used, and attacking the people themselves. Examples of such types of attacks include:

1) Reverse Engineering: If Michael gets a hold of the rivals’ weak encryption devices, then he could deconstruct and extract the plaintext data. 2) Guessing and frequency analysis: If the rival firms have weak ciphers, Michael can study the frequency of letters appearing in the ciphertext and find their likely corresponding plaintext alphabets, which eventually allows him to determine the keys used and the plaintext data. 3) Brute force-Dictionary attack: Michael could attempt to crack the rivals’ encrypted data by using a carefully constructed table of ciphertext and corresponding plaintext through a series of trial and error approaches to access the system. 4) Known plaintext and ciphertext-only attack: If Michael captured the rivals’ ciphertext and plaintext data or just the ciphertext data, he might be able to find the key. 5) chosen plaintext and ciphertext attack: If Michael gets access to the rivals’ weak cryptographic algorithms, he could encrypt and decrypt random data to figure out the encryption key used.

6) Man in the middle-Session Hijacking: Michael can sniff the traffic between the rivals’ and the resource that they want to access such as a server, interject himself and compromise the session token sent back to the rivals’ by presenting his identification to the rival. 7) Replay attack: During the sniffing period, Michael can also collect legitimate traffic that provides him authentication to the resource the rival company wants to access. 8) Social engineering attack: Michael can find a way to trick the rival company’s employee/s into giving confidential competitor data. 9) Memory Residue/OS flaws: If Michael finds remote or physical access to the rival firms’ virtual memory and storage devices, he might also be able to obtain key information that may have been cached, especially if the devices were physically left without being properly disposed or destructed.

**b)** Some of the obstacles Michael could face are strong resistance to attacks by the rival firms, increased work factor, and increased learning curve to be able to attack. The rival firms might already have robust access controls in place to protect confidential data, strong enterprise network design, social engineering aware employees, and proper destruction of device practices. Additionally, if the firms have rigorous cryptosystems, they can be hard to break into or take much time. They are also not vulnerable to easy attacks such as reverse engineering and frequency analysis. At the same time, some attacking or cracking tools might also require experience for him to use. However, Michael could face advantages and get access to competitor data if the rival firms have poorly destructed devices, use weak cryptosystems and weak algorithms that are easy to break into and vulnerable to simple attacks. Furthermore, If the rival firms’ employees’ don’t have strong knowledge against social engineering attacks, he can trick them into providing the data and take over their business.

Response:

**a)** The types of cryptographic controls that can be used for the integrity of data at rest include encrypting hard drives, flash drives, tapes, any optical media, disk encryption, and full disk encryption especially if the data at reset is stored on portable devices. A full disk encryption (FDE) based product, in this case, a software, works by redirecting the device’s master boot record (MBR) which is the sector on the media that determines what OS utility gets executed when the device boots up. FDE software redirects the MBR to a pre-boot environment (PRE) that requests the user to authenticate using some form of identification. After successful authentication, the FDE software decrypts the boot sector for the OS. The boot loader in the boot sector then starts to load the OS. During this process, the FDE software decrypts the files which are stored on the device. Once the booting is complete, the user will authenticate to the device and use it. The FDE software decrypts and encrypts the necessary sectors of the storage device transparently as the user opens, encrypts, and saves files or performs other operations involving the device’s storage. FDE software can be built into any computer, hard drives, discs, and other common storage devices. In addition to secure encryption of data at rest, FDE software doesn’t place cryptographic keys in memory, which could expose the keys to threats. It can also be centrally managed, making the key management efficient. Another lower level method of protecting data at rest is through volume encryption. It is a special form of FDE and is most commonly used to encrypt USB flash drives, CDs, DVDs, and external hard drives. Volume encryption involves encrypting the entire logical volume allowing access to data only after proper authentication. However, unlike FDE, the booted software running on the OS that is used to access the volume is responsible for decrypting and encrypting the appropriate sectors of the storage device as needed when users perform different actions (Scarfone, Souppaya, & Sexton, 2007).

**b)** Sonny can specifically deploy the cryptographic controls at Genco by following a series of steps. First, he identifies which devices contain data that needs protection. Then, Sonny selects a recommended encryption algorithm as well as proper key lengths for the data. He also chooses authentication methods for users and administrators who interact with the data followed by what encryption techniques (FDE, Volume, etc.) to implement. Sonny also makes sure that the storage devices, hardware, OS, and software support the minimum requirements for the encryption. Based on the custom cryptographic control he designed, Sonny installs the prototype from the vendor who provides such control and tests it to evaluate the security of the data stored. Finally, he will gradually migrate storage devices and employees to the cryptographic control while also tracking the encryption progress of devices without interrupting workflow. This technique allows administrators and employees to be trained and resolve any technical and configuration issues with storage devices (Scarfone, Souppaya, & Sexton, 2007). During the migration phase, Sonny should also confirm the existence of a layered defense that includes physical security, proper disposal of storage devices, and technical access controls to protect the data. The mechanism is crucial since data at rest on tapes, hard drives, portable devices, and optical media can be exposed when these devices are stolen or accidentally lost, leaked without proper disposal, and decrypted and modified by unauthorized individuals.

References

Scarfone, k., Souppaya, M., & Sexton, M. (2007). U.S. Department of Commerce, The National Institute of Standards and Technology, NIST Computer Security Resource Center. *Guide to Storage Encryption Technologies for End User Devices*.Recommendations of the National Institute of Standards and Technology (NIST SP - 800-111). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf