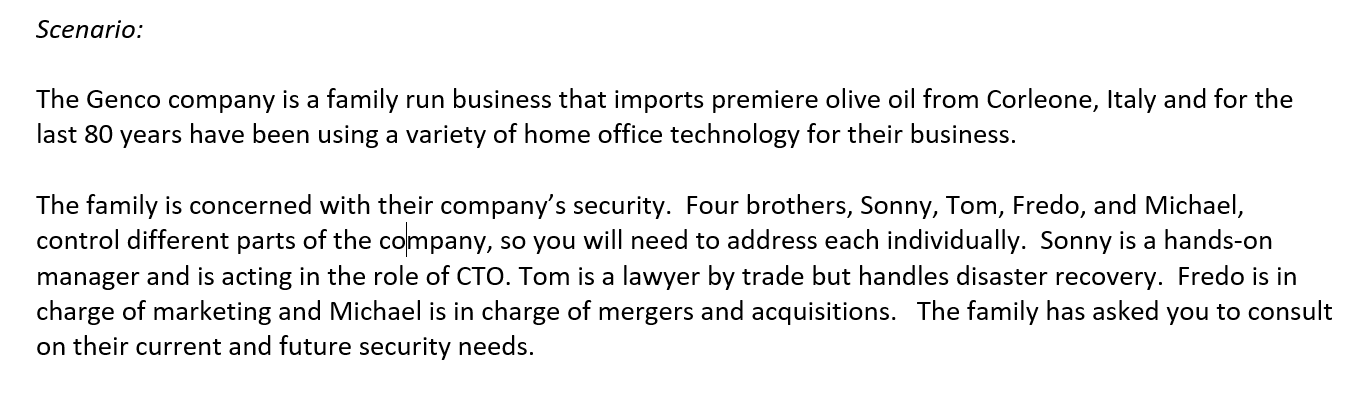
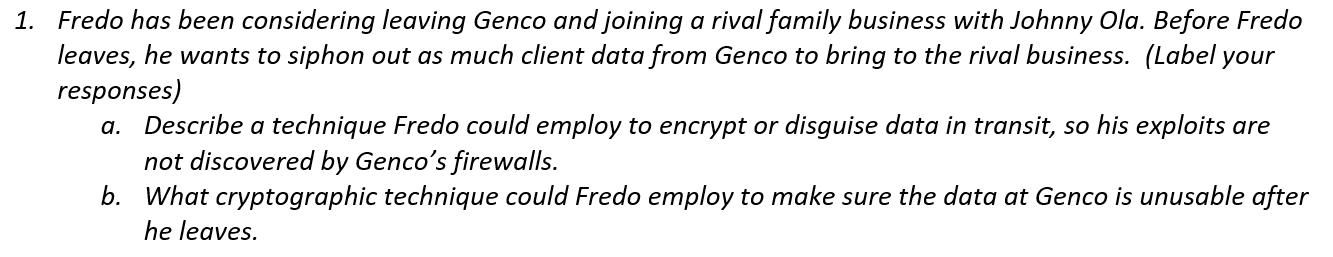
|  |  |
| --- | --- |
|  |  |

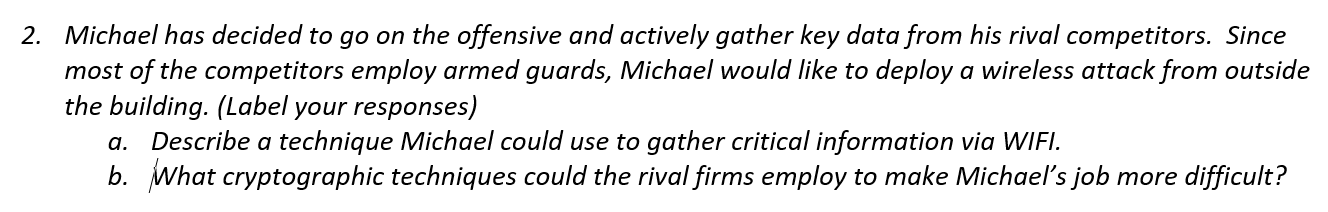




Response:

**a)** Before Fredo leaves Genco to join Johnny Ola, a technique that he could employ to encrypt or disguise data in transit is using Virtual Private Networks (VPN). Once Fredo establishes a VPN connection, it can be difficult to detect his activities since VPN clients typically use ports such as 443 over UDP or TCP which are usually open or accepted traffic on a firewall (Delaney, 2017). This technique can help him hide the client data he plans to siphon out without his exploits being discovered by Genco’s firewalls. A VPN works by creating an encrypted tunnel for secure data connection over the internet between Fredo and a remote VPN server past Genco’s firewall. The encrypted connection between the two allows Fredo’s internet activity to be routed through the VPN server connection allowing him to access services such as his personal Google drive to store the stolen client data from Genco (Delaney, 2017). There are a wide variety of VPN service providers that Fredo can choose from to accomplish his goal. For instance, he could use NordVPN, which is a cloud VPN provider that has an application for different operating systems and mobile devices. Nevertheless, the provider of his choice should likely utilize the VPN protocol, Internet Protocol Security (IPsec) or Layer 2 Tunneling Protocol (L2TP) with IPsec. The reason behind it is that L2TP does not provide encryption on its own. However, IPsec functioning in tunnel mode encrypts the message header as well as the application data or payload (Ballad, Banks & Chapple, 2017). Hence, IPsec allows the data packets that Fredo exports from Genco to be encrypted as they are sent over an IP address to his storage destination. As a result, individuals like Fredo can use VPN for suspicious and/or harmful activities.

**b)** A cryptographic technique that Fredo could employ to make sure that the data is unusable after he leaves would be to deploy a Ransomware, which is a type of malware that encrypts all files or locks devices thus preventing the regular access to a system or files. Hence, ransomware isn’t about someone reading sensitive data. Instead, it is about someone like Fredo stopping Genco from getting to the data (Bates, 2017). Additionally, even though there is no guarantee, one would be requested to pay to get the decryption keys or to get the unencrypted files in some form of payment such as bitcoin. For his purpose, Fredo could use a phishing email, for example, to deliver ransomware such as Cryptolocker and infect the device containing the data. Once in the device, Cryptolocker scans hard drives for file extensions. It also scans for other backup drives connected via USB or even cloud systems and starts encrypting the files. It does not matter whether Genco already encrypted specific files or even the entire hard drive. Fredo will use the ransomware to encrypt it again, which mean Genco’s key will not work until his key is used. Cryptolocker’s encryption technique utilizes AES 256 and RSA 2048-bit key encryption, which is also very strong to break, rendering the data unusable for Genco (Bates, 2017). Furthermore, the fact that the company can even lose access to its backed-up data also means that it might not be possible for Genco to restore normal business operations in addition to being unable to use the data after Fredo leaves.



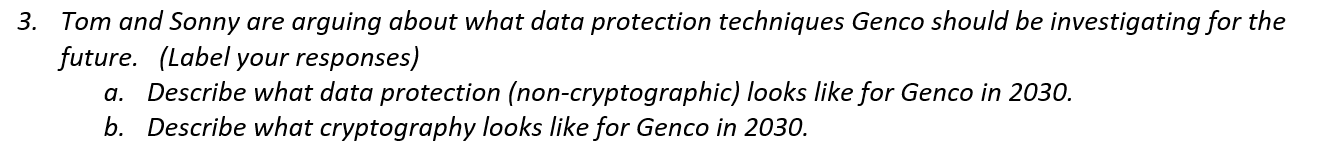
Response:

**a)** To gather key data from his rival competitors from outside the building via WIFI, Michael could primarily use a wardriving technique. This mechanism requires Michael to drive around a building in a car looking for open WIFI networks. The vehicle should be equipped with an antenna that is placed inside the car or mounted on the top of a car. Michael would also need a laptop, a GPS device, and wardrive software to accomplish his goal. He can then use these items to locate all the WIFI signal around the building. That is, the GPS receiver records the location of the vehicle while the antenna detects the signals available. The Wardriving software is also used to record the location of the signal, its strength, and its status, such as whether it is open, encrypted, and what type of encryption the WIFI uses. Once Michael finds an available WIFI which is open, unsecured or secured with weak passwords, he can use it to map to all the possible rival firm’s WIFI signals around the building or use it by itself to intercept traffic and access or steal the rival firm’s data (Christensson, 2017). By breaking a weak security algorithm such as WEP, he will also be able to spoof the rival company’s access point and redirect them to his site by launching a man in the middle attack to steal information.

Another technique that Michael could use to steal the rival firm’s data is by creating an evil twin. A wireless evil twin is typically established once he finds a weak WIFI with weak or no passwords so that it is easy to duplicate its access point. In this process, Michael would buy a wireless access point and configure it the same way as the competitor’s existing network, including the same WIFI name and security settings. He also increases its signal so that this WIFI is easily discoverable by devices and that anyone in the company can connect to it. Once employees connect to it, Michael can launch the same method to intercept and steal information (“Rogue Access Points and Evil Twins - CompTIA Security+ SY0-401 ...”, n.d.). Hence, any device connected to this network will be accessible to Michael, including any activity the user operates on these devices.

**b)** The cryptographic techniques that the rival firms could employ to make Michael’s gathering of critical information difficult include appropriate security safeguards that will limit WIFI access to authorized users only. These safeguards include the rival firms use of secure wireless algorithms such as WPA and WPA2. WPA and WPA2 provide a good security layer with secure AES encryption if they are correctly configured. Any firm that uses the WPA2 pre-shared key with AES or WPA2-PSK (AES) can make Michael’s job very difficult since they have the latest encryption standard with the latest AES encryption protocol (Hoffman, 2017). Additionally, if these firms use Virtual Private Networks (VPN), Michael’s job becomes challenging since VPN establishes encrypted tunnels so that all the router traffic can be to be routed through the VPN server connection making it hard for him to figure out what the rival firm’s data involves. This technique is possible through VPN providers that utilize the Internet Protocol Security (IPsec) protocol or Layer 2 Tunneling Protocol (L2TP) with IPsec.

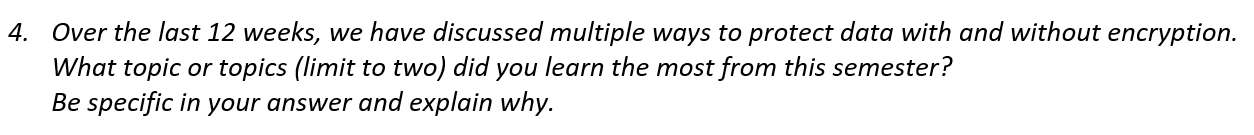
Other safeguards the rival firms could have incorporated with the cryptographic techniques include disabled WIFI protected set up (WPS) to prevent Michael from using the WPS PINs to recover WPA/WPA2 passphrases, ability to identify rogue access points, not broadcasting the SSID or name of their WIFI, using firewalls to reduce chances and block attempts to access network by outsiders, strong passwords, and 802.1X (Network Access Control) which requires users to authenticate regardless of the connection type (“Rogue Access Points and Evil Twins - CompTIA Security+ SY0-401 ...”, n.d.).



Response:

**a)** Data protection (non-cryptographic) in 2030 will require Genco to be vigilant in addressing the continuously changing attack surface resulting from the growing number of IoT devices being used, virtual employee workforce, allowing employees to use personal devices (BYOD), third party contractors, and advanced persistent threats (APT). IoT device vulnerabilities can be addressed by changing the default usernames and passwords, changing the default privacy and security settings including activating two-factor authentication, disabling features that the company doesn’t need, and keeping the software on the devices up to date (Sharma, 2018). The other attack surfaces can be addressed by applying data-centric concepts, which includes data classification, detection and discovery, and protection and prevention. When it comes to data classification, Genco needs to identify the data on devices or stored data that enables it to achieve its business objectives. Detection and discovery require the company to monitor for anomalous events and ensure timely and adequate awareness to address potential threats. Protection and prevention allow Genco to consistently manage data within the organization using tools such as data loss prevention (DLP) technologies so that the confidentiality, integrity and availability of the data is adequately maintained. Protection can also be accompanied by information protection security policies and procedures (NIST Special Publication 800-53 Revision 5, Security and Privacy Controls…”, 2017). Furthermore, Genco can protect its data by maintaining network integrity through appropriate network segmentation, which involves segregating the internal network into subnetworks. Establishing adaptive network zones for defense purposes can also enhance this protecting mechanism. Hence, these combined data protection (non-cryptographic) techniques can help Genco protect its critical infrastructure data, maintain its intellectual property, preserve its reputation, and legally comply with rules and regulations in the future.

**b)** For Genco, current cryptography is likely going to be ineffective in 2030 for protecting the company’s data unless the company moves to more rigorous cryptographic algorithms that are resistant to attacks caused by decreased work factor and time which result from using an increased computational power. It is known that quantum key distribution solutions which use quantum mechanics to securely exchange cryptographic keys in symmetric cryptography are available. However, researchers have identified that even though they are currently unstable to be used largely, quantum computers could enhance the processing power we have today through classical and supercomputers. Due to this power, quantum computing can be a threat in a little more than a decade (in 2030) or even sooner if stable and full processing power versions of these computers are to be built as expected (Giles, 2019a). Their existence affects current cryptography because it could break all the public-key cryptographic algorithms that companies, including Genco, use today (in SSL/TLS) for securing electronic communications such as online transactions. That is, quantum computers can solve the complex mathematical factoring problem used by RSA and the discrete logarithm problems used by Diffe-Hellman, and elliptic curve cryptography in real-time (Aumasson, 2018). Classical algorithms used in digital signatures that validate the authenticity and integrity of data are also at risk since they rely on these public-key cryptographic algorithms. Hence, Genco needs to consider NIST’s recommendation to switch to the new algorithms (Hanacek/NIST, 2016) expected to be standardized in 2022 (Giles, 2019b) in its investigation of future data protection techniques to safeguard the company’s data from current and future attacks (Hanacek/NIST, 2016). Additionally, if the company uses a vendor, it should also require the vendor solutions to include quantum-resistant cryptography (QRC) algorithms to keep Genco’s data safe before the existing algorithms are compromised. Furthermore, since these new algorithms are going to be embedded in many different systems (Giles, 2019b), Genco should develop third party management (TPM) risk policies to address and mitigate the risks these technologies can pose in the instance that they get implemented without proper understanding (Aumasson, 2018) or if attackers find ways to exploit them. These combined techniques would allow Genco to protect its data adequately in the future.



Response:

Over the last 12 weeks, the class addressed each of the various ways to protect data. Through student class presentations that focused on data protection topics and recent data breaches, we covered the importance of encryption, data classification, access controls, non-collection of data, appropriate network design, and proper disposal or destruction of devices as part of the ways to protect data. We also covered legal and compliance topics through a guest speaker from Pepsico. Additionally, weekly lectures touched on these various ways to protect data at a higher level or gave in-depth details. Nevertheless, the two topics I learned the most from this semester are asymmetric cryptography and network design.

The first reason why I learned the most from asymmetric cryptography lies in the way the topic was presented. The class primarily had gone over symmetric cryptography, the history behind it, how it works, for what purposes it is used for, and its weaknesses. This technique made it easy for me to learn asymmetric cryptography, also known as public-key cryptography. I was able to understand the problem it was trying to solve with symmetric cryptography, how it works with symmetric cryptography, the variety of algorithms it consists of, and for what security purposes it is used for compared to symmetric cryptography. Second, the various videos the lectures presented and the hands-on labs with Python, including the Diffie-Hellman key exchange lab allowed me to perceive the topic adequately. I was also able to analyze the process used in asymmetric cryptography from different perspectives and interconnect them to enhance my understanding. The capability of public-key cryptography discussed in the subsequent lectures on SSL/TLS and HTTPS while protecting data in transit also allowed me to learn and appreciate its use in electronic communications such as online transactions.

Proper network design is the other topic I learned the most from this semester. First, the various data breach scenario presentations, including mine, clearly emphasized the lack of appropriate network design that caused the network compromises. The scenarios explained the lack of incorporating network segmentation as appropriate within the internal company network to establish multiple small subnetworks for the various business functions as the root cause. Second, the class lecture on network protection also presented the Target breach as another scenario to provide lessons learned and the importance of network segmentation. The lecture also enhanced my understanding of the topic by incorporating the OSI model, how networking devices function at these layers, and how they can be used to maintain network integrity. Furthermore, it introduced adaptive network zones for defense purposes in relation to network segmentation, which provided me with a broader grasp of the topic by introducing practical examples and tools that exist in a typical corporate network infrastructure. Lastly, the week’s scenario assignment to explain to the CEO of the organization as to why the network should not be flattened but instead segmented allowed me to analyze and interpret my understanding of the topic by developing a simple analogy to explain the technical concept behind establishing an effective network design.

References

Aumasson, Jean-Philippe. (2018). *Serious Cryptography*. San Francisco, CA: No starch press.

Ballad, B., Banks, E, K., Chapple, M., Ballad, B. (2017). *Access Control, Authentication, and Public Key Infrastructure, Second Edition.* Burlington, MA. Jones & Bartlett Learning.

Bates, P. (2017). Why Encrypting Your Data Won’t Protect You From Ransomware. Retrieved from https://www.makeuseof.com/tag/encrypting-data-wont-protect-ransomware/

Christensson, P. (2017). Wardriving Definition. Retrieved from https://techterms.com

Delaney, D. (2017). How to Passively Detect VPN Clients on Your Network. Retrieved from https://www.netfort.com/blog/detect-vpn-clients-network/

Giles, M. (2019a). MIT Technology Review Explainer: What is a quantum computer? Retrieved from https://www.technologyreview.com/s/612844/what-is-quantum-computing/

Giles, M. (2019b). MIT Technology Review Explainer: What is post quantum cryptography? Retrieved from https://www.technologyreview.com/s/612844/what-is-quantum-computing/

Hanacek/NIST. (2016). NIST Kicks Off Effort to Defend Encrypted Data from Quantum. Retrieved from https://www.nist.gov/news-events/news/2016/04/nist-kicks-effort-defend-encrypted-data-quantum-computer-threat

Hoffman, C. (2017). Wi-Fi Security: Should You Use WPA2-AES, WPA2-TKIP, or Both? Retrieved from https://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/

NIST Special Publication 800-53 Revision 5. *Security and Privacy Control for Federal Information Systems and Organizations*. (2017). Retrieved from: https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

Rogue Access Points and Evil Twins - CompTIA Security+ SY0-401. Retrieved from https://www.professormesser.com/security-plus/sy0-401/rogue-access-points-and-evil-twins-3/

Sharma, R. (2018). IoT device security: A guide for every tech leader — and user. Retrieved from http://techgenix.com/iot-device-security-guide/