Assignment 4

Sindhuja Yerramalla

Q1. Why would the police spend so much time talking to the help desk employees?

It is possible that the police are spending a significant amount of time communicating with IT help desk staff because they suspect that the individual responsible for the theft may have received technical aid or gained unauthorized access to systems or data through the help desk. The authorities may be examining whether any IT help desk personnel assisted the insider in carrying out the crime, or if there were any security flaws in the system that the insider could have taken advantage of.

Q2. If it is Insider threat/misuse, then how it can happen?

The theft could have been caused by an insider threat, specifically the Payroll Department manager, who may have used their authorized access to the company's payroll account to initiate the unauthorized wire transfer. They could have also used their technical knowledge or social engineering skills to bypass security controls and access sensitive information. Additionally, an external threat actor may have coerced or bribed the insider into carrying out the theft. It is crucial to implement robust access controls, monitor employee behaviour, and conduct regular security awareness training to reduce the risk of insider threats.

Q3. Did the payroll employee foolishly write down his/her password for others to see, if that is the case how this financial fraud can happen?

The scenario doesn't mention the Payroll Department manager carelessly sharing their password with others. However, if such an action had occurred, the chances of financial fraud would be higher. Sharing passwords or writing them down is a security hazard and can make it simpler for unauthorized individuals to gain access to confidential data or systems. It highlights the significance of enforcing stringent password policies, including the use of strong, unique passwords and multi-factor authentication to enhance security.

Q4. Why are the police looking at the trash (for discarded hard drive) to solve this computer crime?

In this given situation, the police could be searching through the garbage to discover any electronic equipment or hard drives that were used in the computer crime. These devices often contain important evidence such as login details, traces of illegal activities, or malware. Individuals who commit cybercrimes may try to get rid of this evidence by either destroying or disposing of their electronic devices. As a result, looking through the trash could potentially help the investigation by locating crucial evidence.

Q5. Was it social network apps/sites launch spear phishing attack by installing spyware in branch manager's machine, explain such a possibility.

While the scenario doesn't specifically mention spear phishing or spyware as the cause of the theft, it's possible that such attacks could have occurred. Spear phishing is a targeted form of phishing that uses personal information to create convincing messages that seem legitimate. Attackers may also use spyware to obtain sensitive data and credentials, which can then be used for fraudulent purposes. To prevent such attacks, it's important to educate employees about social engineering risks and implement robust security measures, such as intrusion detection systems and antivirus software.

Note: Worked with Vamshidhar Reddy Chirumani.