1)

To protect digital assets from being abused, a strategic plan must be formed to ensure the security of assets such as hardware, software and data.

In terms of hardware, assets such as servers, switches and hubs should be enclosed and locked within a container such as a server rack. These containers should also be positioned in a location that does not have a lot of people or a location that only allows staff entries. This ensures that unauthorized personnel may be kept away from the location where important hardware are located in and reduces attacks to a minimum. For extra security, close circuit television (CCTV) cameras should also be installed near the entrance to server rooms to monitor traffic around the location.

In terms of software, assets should also regularly check for updates to ensure the latest security patches are applied. During software installations, some software also allow users to verify the checksums of the downloaded software. This ensures that no security loopholes and backdoors are created during the software installation and confirms that the software is genuine and legal. When using a software, authorized users must also ensure that no unauthorized individuals are nearby to prevent them from peeking at confidential data stored within the software.

In terms of data, assets should use encryption protocols such as Secure Socket Layer (SSL) or Transfer Layer Shell (TLS) to transfer data over a network. This prevents third parties from eavesdropping on the network communication and steal important data. Data should always be safely backed up in a specific location, such as in a hard drive or in the cloud on the Internet, to prevent accidental data loss. This is because data is said to be irreplaceable and measures should be taken to ensure the integrity of the original data.

2)

Malwares, short form for “malicious software”, is a malicious virus that contains an executable file. This executable file will not be executed unless the malware is opened by a user. There are 7 types of malwares, namely: trojan, worm, timebomb, zombie, rabbit, ransomware, spyware. Malwares may infect any software or hardware platforms, access hidden and read-only files, appear anywhere in the system, and spread anywhere where sharing occurs. They can be malevolent, benign or benevolent. Luckily, malwares can be removed from volatile memory whenever there is a complete reboot.

A specific malware that is in the types of malwares listed above is ransomware. Ransomwares are a type of malware that behaves in such a way, that it encrypts and locks user access to system data and applications. After that, they demand ransoms from users and only allow user information to be decrypted if users performs the given instructions. Ransoms may come in the form of payments, providing classified data, and other given instructions.

They are harmful in nature as they prevent users from accessing their data easily and may cause financial or confidential loss. They may also demand users to conduct unlawful activities, using the user’s identity as a shield from the law for the attacker’s own benefits. The victim is given no other options from choosing to expose their own secrets or to do what the attacker says and risk themselves being sent to prison for conducting unlawful acts. They may also hinder urgent activities because of disabling the use of computer systems.

An example of a ransomware is the WannaCry ransomware, which had took the world by storm for preventing users access to computer systems that have been essential in industries such as in the medical field, causing loss of lives and money.