Dealing with cyber threats – the weakest link by Leonard Yong

"It takes many years to develop a reputation and just a few minutes of a cyber incident to destroy it".

The internet and cyber security could be regarded as 2-sides of the same coin. Businesses and their customers want assurance that the internet is highly secure before doing business on it. Parents too have a duty of care to their children. To access the internet, you'd normally require your own password (just to access the computer systems). And the password is supposed to be the one of the most sacred things you've ever kept; so guard it with your life! Some cyber security experts recommend that your password should consist of at least 15 characters long (consisting of capital letters, numbers, symbols, lower-case letters, etc). You'd think that kind of password code would be rather difficult to crack, unless you are using a quantum computer (more on than later). Some people might say that having access to the computer systems (via password, facial recognition, thumb print, speech, etc) is the weakest link. So before you'd access any websites, open an email attachment, saying "like" to a social media feature, etc, think again! Your personal data could well have been captured and stored onto a database without your knowledge.

Cyber security awareness

It is crucial that the community (including companies) are fully aware of the cyber risks and threats. The internet is eliminating boundaries between nations, leading to many regulatory issues. One of the scariest aspects of cyber threats is via social media and the "dark-web", targeting and bullying and cyber-stalking young people to increase their suffering, eg, often with fake news. Cyber security experts should continually warn about the risks in visiting the terrible or suspicious websites. Students (for online learning) should constantly be reminded that they should only use genuine approved websites and that they are just a click away from a cyber incident. But surely the main problem is: "how does a student know that the website is a dangerous website?". How to ensure it is a genuine and trustworthy website? It is arguable that you'd soon find out whether a website is trustworthy or not- but that is usually too late. e.g, is there a "trust-certificate" on the website, assuring people about the credential as well as the security of the website? Does it have "end-to-end" encryption? Do the ID cards to identify ourselves in cyberspace work effectively?

Use of Virtual Private Network (VPN) or Intranet

A Virtual Private Network (VPN) often covers a public network and allows users to share data across mutual networks as if their IoT (Internet of Things) were connected directly to a private network. In other words, a VPN routs your computer's internet link via a more secure VPN's private server. Users need to go through various types of authentication in order to get onto the VPN; also connecting to proxy servers to further protect personal identification. In various systems applications, it is important that network-to-network links and keys are secure, eg, use of digital certificates and/or facilitating non-intervention from systems administration.

There is heavy reliance in areas such as on-line sales/purchases, marketing & delivery of services, monetary transfers, educating students, social-media, etc. The key cyber incidents include:

- Phishing (compromised credentials)
- Compromised or stolen credentials (various methods used by criminals); identity theft
- Brute attack (compromised credentials)
- Hacking
- Ransomware
- Malware
- Side-channel attacks: unauthorised use of computer electronic signals during computation, eg, discovery of secret encryption keys

Aligning the cyber security mindsets

We need to align our mindsets with the new reality of cyber security; regularly evaluating the risks and threats of cyber security. In designing a cyber security plan, we need to cover actions such as an evaluation of where we are at (eg, the level of integration of the operating systems with the VPNs), where we need to go and progressive actions to reach the ultimate in cyber security. Companies should always consider emerging cyber security technology, eg, new techniques and tools in encryption, to make their systems more secure.