Digital Resilience Assessment

"A high-tech car is actually a computer with wheels".

The Internet of Things (IoT) now encompasses many things from DNA testing equipment, 3D printers, CT scanning, refrigerators, prosthetics, alarm systems, smart robots, predictive analytics, machine-learning, etc. The IoT revolves around big data since networks generate huge amounts of data for on-line access. And technology, eg, blockchain technology [defn see below], should be utilised to gain further assurance in relation to data integrity. They need to be greatly trustworthy as they have "operating by remote control connectivity". It seems that everything could be operated by remote control these days; even hackers are learning and improving various technical tools to illegally operate by remote control. And that is indeed, quite scary. Imagine that in a ransom-ware situation, it could be almost impossible to identify where the culprit came from as he/she has rather sophisticated remote systems.

The importance of big data cannot be overstated. Just recently, a major government department had confirmed that 180,000 customers' personal details had been exposed in cyber security breach; millions of documents may have been compromised. There is a clear need to raise awareness of scams and empower people to better protect their own identities when working online.

Becoming digital resilient

Being resilient means the capability to be well-prepared for the worst-case scenario. That means, frequently performing scenarios analyses; a subset of a risk analysis framework. It is important to understand where the cyber risks are from and how to deal, minimise and manage the cyber risks. In other words, aim to prioritise the critical assets (including information assets) and embrace a broad and proper cyber security strategy. And one question to be constantly asking: What cyber risks or scenarios keep you awake at night? Of course, it would be good (health-wise) not to be worrying these issues too much at night.   It is noteworthy that we can't make any computer system 100% safe for usage, but we could minimise or manage the cyber security strategic risks. It is noteworthy that a typical computer software is rather complex and some have about a few millions lines of software code and errors are expected (particularly for very old computer systems). Also, the typical computer program has in excess of a dozen vulnerabilities; each of them a potential weak entry point for hackers to access.

In recent times, the AICPA listed "Securing the IT environment" at the top of the list. For many years, safeguarding IT assets has been the top priority in the US survey. It is noteworthy that the following is the **top technology initiative rankings**:

1 Securing the IT environment

2 Managing and Retaining Data

3 Ensuring Privacy

4 Managing IT Risks and Compliance

5 Preventing & Responding to Computer Fraud

6 Enabling Decision Support and Analytics

7 Managing System implementation

8 Governing and Managing Our IT investment

9 Managing Vendors and Service Providers

10 Leveraging Emerging Technologies

So the key question is: "*Has your company's current priority list changed?".* I suspect the issues are still the same, except, perhaps there is now a closer look at the use of Artificial Intelligence (AI) or the impending arrival of quantum computing, which could well change things on how we store and recover big data.

Digital footprint

People have been talking about carbon footprint recently but have we been focusing on our digital footprint? Whenever we do shopping online or enabling the locality on the mobile phones apps or using the search engines, we have created or added to our footprints. And just as we are going for a job interview, I am sure most potential employers have actually known about our digital footprints via say, FB or LinkedIn systems. Current technologies revolve around a 24/7 basis; cloud technologies revolve around cross-platforms. Digital footprints can be defined as "a trail of data you create during the use of the internet". It covers the websites you have accessed, your personal emails as well as the data you have communicated via any online services. So remember that big brother/sister could always locate your digital footprints and it is best to be extremely careful before we say or do anything on the internet!

Leonard Yong, M.Acc (UOW), CA, FCPA, MACS(Snr)

Convenor, CPA Cyber Security Forum;

Chairman, Digital Economy Committee, ShireBiz.

A **blockchain** is a database that is shared across a network of computers. Once a record has been added to the chain it is very difficult to change. ... The records that the network accepted are added to a block. Each block contains a unique code called a hash. It also contains the hash of the previous block in the chain