Source: *TODAY*, p38
Date: 21 July 2017

FOR BETTER SOLUTIONS, FACTOR IN HUMAN BEHAVIOUR TOO

Cyber security needs a nuanced approach

HAWYEE AUYONG AND SHAWN TEOW

With the recent spate of cyber attacks, cyber security has suddenly become the cause celebre of the world. Ransomware attacks such as WannaCry, which temporarily affected Britain's National Health Service, and the Petya/NotPetya attacks that forced shipping giant Maersk to revert to handwritten information for 48 hours have certainly driven this issue into the public spotlight.

Moreover, all these attacks have happened in a year when the United States is still investigating the full extent of foreign interference in a tumultuous presidential election.

Recent cyber attacks differ from those in the past, such as 2000's ILOVEYOU virus, in two key aspects. First, they are more mercenary in nature, in that the perpetrators have monetary or strategic objectives that extend beyond simple vandalism.

Second, the permeation of computing devices and the Internet throughout almost every facet of our lives has greatly expanded the ways in which such hacks can hurt or inconvenience us.

As a result, some of these attacks are able to cause real physical damage beyond just digital havoc. For example, 2009's Stuxnet malware silently accelerated a few hundred Iranian nuclear centrifuges until they destroyed themselves.

Since 2015, Ukraine has come under nearly continuous cyber attack. Two days before Christmas 2015, at precisely midnight, a cyber attack cut electricity to some 250,000 Ukrainians.

In a public statement in December last year, Ukraine's President Petro Poroshenko reported that there had been 6,500 cyber attacks on 36 Ukrainian targets in the previous two months alone.

What is more worrying is that these attacks could be state-backed, and they represent a quiet arms race between the great powers of the world to develop cyber-warfare capabilities that can cripple whole countries.

Thankfully, Singapore has remained almost entirely unaffected by such large-scale, targeted cyber attacks.

It appears that hackers have been — for the most part — content to forgo Singapore for what they perceive to be less-hardened targets relative to expected payoff. Perhaps that is one of the advantages of being a relatively smaller nation.

But Singapore's Government and companies are not standing by idly. Sixty per cent of banks plan to increase expenditure on IT security, beyond spending on IT systems; and 93 per cent of companies in Singapore plan to hire more staff to manage their online security.

The Government has proposed a new Cyber Security Bill and has pre-emptively cut off access to the Internet for more than 100,000 civil servants. Unauthorised USB devices (such as personal thumb drives) will also be locked out from government computers from July 25.

Nevertheless, cyber security requires a more nuanced approach than rushing headlong into the cyber-security marketplace to snap up the shiniest solutions, sanctioning wholesale Internet separation, or locking out USB devices entirely.

Senior managers and decision makers have to carefully weigh the distributed, often untabulated costs of productivity loss against the supposed effectiveness of these solutions.

Internet separation, for example, presents a number of challenges to everyday tasks and may further weaken information control.

The Internet has become such an indispensable resource in modern work life that conscientious, well-meaning employees may often feel compelled to shift an ever-greater proportion of their work and sensitive information away from quarantined workstations to Internet-connected devices, including personal devices not subject to onerous corporate IT policies. This defeats the intended purpose of Internet separation.

Senior management of large organisations should also be wary of blanket cyber-security policies that conflict with local operational needs. Individual IT teams caught between top-down corporate policies and localised operational needs may end up compromising with sub-par solutions.

In some large organisations where blanket Internet separation for workstations has been imposed, local IT departments have taken to issuing additional mobile devices that can nonetheless access both the public Internet and internal corporate networks, following the letter of Internet separation policies, but violating their spirit.

Recent cyber attacks differ from those in the past in two key aspects: First, they are more mercenary in nature, and second, the permeation of computing devices and the Internet into our lives has greatly expanded the ways in which such hacks can hurt or inconvenience us.
PHOTO: REUTERS

Effective cyber-security policies must also take into account how human behaviour often interacts with policies to dull their effectiveness. Make cyber security too onerous and employees shift confidential work away from workstations.

Make password rules too complicated and the changes too frequent, and employees come up with predictable rules to generate new passwords.

In many cases, interventions at the human level can be orders of magnitude more effective than technical solutions.

For example, spending resources on employee training to spot phishing attacks often yields much better results than expensive and easily defeated email filtering software. The same goes for being careful about untrusted USB devices.

Moreover, over-reliance on technical solutions may not only generate a false sense of security, but could make systems more hackable.

Poorly implemented cyber-security software can increase a system's vulnerability to attacks, by enlarging the "surface area" exposed to hackers by giving them more targets to hack.

In fact, Google Chrome's security chief Justin Schuh once lamented that antivirus software was "my single biggest impediment to shipping a secure browser", because of the way that antivirus software forces itself into other pieces of software, including into an operating system's core components.

Given that antivirus software are themselves not bug-free, such intrusive behaviour can re-inject vulnerabilities after software vendors work to remove them.

Finally, organisations need to redesign their internal processes such that sensitive data remains secure and privacy stays intact even when hacking attempts inevitably prove successful.

Critical databases need to be encrypted, and passwords especially need to be stored in a way that is not even accessible by employees.

With proper data-handling protocols, data leaks like those affecting 300,000 K Box customers and millions of Sony customers in 2014 would not have been possible even if the initial hacking attempts were successful.

For Singapore in particular, serious thought needs to be given to whether we are over-reliant on NRIC numbers as a means of identification, along with the casual way in which they are usually handled.

Because the way NRIC numbers are issued makes them permanently tied to individuals, leaks of such numbers make their victims permanently vulnerable to identity theft and other crimes. NRIC numbers should rightly be used as a means of identification only as a last resort, and handled with the utmost care even then.

In the end, cyber-security measures should make organisations more resilient, and not introduce unnecessary tedium in core operations. After all, the costs of a cyber attack may very well be outweighed by the productivity loss and business costs incurred in preventing it.

As a common quip in the cyber-security industry goes: The only unhackable computer is a computer that is switched off.

● Hawyee Auyong is a research fellow at the Lee Kuan Yew School of Public Policy, Shawn Teow is an independent researcher and writer in the tech/start-up space.