Publication: The Straits Times (Pg A20)
Date: 26 July 2017
Headline: Why the public needs to be involved in improving Cyber Security Bill

Why the public needs to be involved in improving Cyber Security Bill

Cyber threats are growing; safeguards are needed to protect everyone today, as well as future generations

Steven Wong

For The Straits Times

Singapore has recently achieved yet another top global ranking, this time for topping the United Nations International Telecommunication Union Global Cybersecurity Index. However, that does not mean Singapore can rest on its laurels as nothing in cyberspace is ever fully secured.

Therefore, it seems only sensible that the Republic is introducing a holistic Cyber Security Bill that seeks to improve cyber resilience in a landscape where cyber threats are dynamic and ever growing. The war in cyber space is real and taking place every day. Everyone is part of that war, whether they like it or not.

In the past, cyber attacks were mainly carried out by amateurs for kicks, or small-time criminals looking to make a quick buck. Today, the adversary can be anything from a large syndicate to a state-sponsored organisation. Everyone can be implicated directly or as collateral victims. An example of that is the recent WannaCry ransomware outbreak, where the victim was any computing system that had not been patched.

To fight this war, Singapore needs a coordinated effort to build a strong defence. Thus it is logical that a single entity, the Cyber Security Agency, be appointed and granted appropriate powers and responsibilities to coordinate cyber security nationally. That will no doubt make Singapore more responsive and resilient to cyber attacks, thus helping it maintain its reputation as a cyber-safe city for business and investments.

As mentioned earlier, anything that is connected to cyberspace can be a target of cyber attacks. Given that resources are finite, it is impossible to protect everything completely. Priorities thus need to be established. The Bill identifies 11 sectors with Critical Information Infrastructure (CII) essential to Singapore's operations and survival. These include information infrastructure across key sectors such as utilities, finance, health and government. The Bill states the responsibilities of owners of CII and penalties for those who blatantly ignore those responsibilities.

As many of these CII are under the purview of different government ministries, statutory boards and organisations, it does appear that the public sector is keeping itself in check, ensuring that cyber security is taken seriously within its operations. From the viewpoint of a common citizen, I think that is good as it ensures CII are better secured and disruptions to residents' daily lives kept to a minimum.

One of the key provisions of the Bill is the requirement for organisations to disclose information so as to mitigate against the risk of cyber threats. Let me use an analogy to explain why such disclosure matters.

Let's say a burglar who is active in a neighbourhood manages to forge a master key that can open a particular brand of locks. If all victims in the neighbourhood keep silent about their properties having been broken into, more homes in the neighbourhood will become victims as there will be no general awareness of imminent danger. On the other hand, if the victims share information about their situation, not only will everyone be more vigilant, but it also becomes possible for the root vulnerability to be identified earlier. Thus, by simply changing the brand of locks, the burglar is rendered ineffective and the neighbourhood is once again safe.

Likewise in cyber security, information is key in determining the vulnerabilities and mitigating the risk. However, due to different considerations such as reputation risk and business impact, some companies and organisations may not be forthcoming in sharing information. A company whose system has been breached may not want to share data that can help its competitor avoid similar breaches. The mentality of "let's fall together to level the playing field" results in a vicious circle that can only cause all on the field to fall progressively silo by silo, instead of the players rising together to meet the challenge of evolving cyber threats.

In essence, the Bill seeks to break this vicious circle by ensuring that information is disclosed when required so that appropriate investigations can be carried out in the event of a breach. That will, hopefully, prevent other organisations from having their systems breached in similar ways.

SETTING PROFESSIONAL STANDARDS

As President of the Association of Information Security Professionals (AISP) and an academic at the Singapore Institute of Technology, I find the part of the Bill on regulating cyber-security service providers and professionals closest to my heart. That is also the part with the most potential benefit if done correctly.

Regulating cyber security services may allow better traceability should anything untoward happen, and that, in turn, provides better assurance to the end users.

Regulating the cyber-security industry allows the profession to be recognised formally, and for the formation of a community of practice to drive excellence in this field and celebrate achievements. Besides Singapore, countries such as Britain and the United States are embarking on cyber-security professionalisation. Thus, there will be a need for cyber-security professionals and services to be mutually recognised across borders – a far from simple feat.

A mutual understanding of terms and definitions, as well as the knowledge required in each discipline of cyber security, must first be established. That could be supported through a Body of Knowledge(BoK) which contains a complete set of concepts, terms, knowledge and activities that make up a professional domain. The BoK will also be essential in assisting the institutes of higher learning in crafting cyber-security curricula.

Singapore is fortunate to have already developed its own version of the BoK back in 2009. It is being updated by AISP and was the first of its kind in the region. Singapore should leverage on its BoK to foster greater collaboration with overseas counterparts. That will provide a platform for mutual recognition of licensed cyber-security professionals and services across borders. The city state may well be poised to lead this effort in the region, which will help our local professionals and service providers expand into the global cyber-security market.

Taken as a whole, the Cyber Security Bill is a bold and innovative move but questions remain as to how it will be operationalised, its impact on business costs and what needs to be done to prevent over-regulation that could put people off joining the sector. Questions have also been raised about how the Bill seems to be affecting a majority of the "good guys" instead of just penalising the "bad guys".

As with any pioneering piece of legislation, there will be kinks that need to be ironed out along the way. Implementation of the Bill will have to take place in phases. There should be ample opportunities for both experts in the field and members of the public to contribute their views and feedback along the way.

I encourage members of the public to take an interest in this Bill and to take part in the ongoing public consultation as cyber security affects everyone. What we do today will have an impact on future generations.

Members of the public are encouraged to take an interest in the Cyber Security Bill and to take part in the ongoing public consultation as cyber security affects everyone, and what is done today will have an impact on future generations. ST PHOTO: KEVIN LIM

stopinion@sph.com.sg

• Steven Wong is the President, Association of Information Security Professionals; and Deputy Cluster Director and Programme Director, Singapore Institute of Technology.