SingHealth cyber attackers not named as it would not make system ‘more secure’: Balakrishnan

Kenneth Cheng
TODAY, 28 January 2019

SINGAPORE — The culprits behind Singapore’s worst cyber breach last year have not been named publicly as the authorities decided that doing so would not make “our system more secure or be helpful to us”, said Foreign Minister Vivian Balakrishnan on Monday (Jan 28).

He also added that the potential gains to the attackers outweighed the risk of them being identified.

Dr Balakrishnan was responding to a question by researcher Gillian Koh at a dialogue session of the Singapore Perspectives conference at the Sands Expo and Convention Centre. The annual conference is organised by the Institute of Policy Studies (IPS), a local think-tank.

The authorities had previously said that sophisticated cyber attackers who are “typically state-linked” were behind the unprecedented attack on SingHealth, Singapore’s largest public healthcare group, although they stopped short of specifying who the culprits were.

Reiterating that it is not in the public’s interest for the authorities to specify the group responsible, Dr Balakrishnan noted that there were parties attacking Singapore for commercial and state advantage.

He said it was “arguable” to think that it was down to “naming names” and banking on name-and-shame as a deterrent to these cyber attackers.

In the SingHealth attack, a party with “deep resources and technical skills” pulled it off. Dr Balakrishnan said that, as foreign minister, he has a say on whether Singapore should attribute an attack to a specific state because it has implications for foreign policy.

That was not the “decisive determinant”, as the Government decided that “simply naming names” was not going to help or make the system more secure, said the minister.

Dr Koh, who is IPS’ deputy director for research, noted that the parliamentary frontbench had been worried about the authorities disclosing the state actor behind the SingHealth attack. She asked Dr Balakrishnan where citizens fit in the broader foreign and defence strategy and maintaining sovereignty, and whether there were occasions where they should be taken into confidence and told who Singapore’s adversaries are.

Dr Balakrishnan replied that other issues have to be resolved before asking if an attack should be attributed.

Singapore has decided against returning to the days of “paper and pen” and electronic records will stay, he said.

To protect these files, it is not only a matter of having safeguards such as encryption, firewalls or Internet separation. Humans remain the “weakest link” and “you cannot take humans out of human systems”, said Dr Balakrishnan.

There is a need for surveillance systems, audits, checks and balances, and these have been rolled out in Singapore.

Singapore also has to keep abreast of technology as it “is also changing even under your feet and what works today may not work tomorrow”, he added.

Describing responses to cyber attacks as a “never-ending challenge”, the foreign minister noted the importance of awareness, taking basic precautions and public participation in formulating legislation as it evolves, so that they can be “part of the solution and not just a passive victim of the problem”.

About the SingHealth cyber attack

Between June 27 and July 4 last year, a foreign, persistent and sophisticated threat group broke into SingHealth’s systems and gained access to Sunrise Clinical Manager, a database holding electronic medical records.

The attackers stole the personal data of 1.5 million patients and the outpatient medication records of 160,000 among them — including Prime Minister Lee Hsien Loong’s.

A Committee of Inquiry formed to investigate the cyber attack found that employee lapses and vulnerabilities with the system led to the attack, which was ultimately preventable even though the attackers were skilled.