新加坡中華總商會
Singapore Chinese Chamber of Commerce & Industry

ERC/PR/2017
EMBARGOED TILL DELIVERY – 致辞前禁止发表
PLEASE CHECK AGAINST DELIVERY – 以现场致辞内容为准

MR THOMAS CHUA, IMMEDIATE PAST PRESIDENT OF SCCCI,
NOMINATED MEMBER OF PARLIAMENT
AT PARLIAMENT SITTING ON 3 APRIL 2017

Computer Misuse and Cybersecurity (Amendment) Bill

Mdm Speaker, computers and websites bring us much convenience as well as elements of risk. The Government's amendment of the Computer Misuse and Cybersecurity Bill would increase cybersecurity, and is a very timely action.

In May this year, the newly set-up Smart Nation and Digital Government Office would strengthen cross-agency coordination and collaboration; National University of Singapore will also provide data science training for 10,000 public servants, helping them to apply technology with ease, and use data and digital tools more effectively.

In the area of cyber usage and security, government agencies have already accumulated a wealth of experience. In comparison, businesses' risk awareness and digital capability is obviously lacking. But in the cyber world, enterprises can also become the target of cyberattacks. Hence, I hope that the Government could transfer their wealth of experience to companies, and enable the professional digital training courses offered to public servants to be promoted and made available in the business community. We would urge companies to send their top management and core technical personnel to receive training, and enable the public and private sectors to build a safety net of cybersecurity at the same time.

At the same time, businesses which make use of digital technology must strengthen their cybersecurity awareness. For example, the National Trade Platform which is being set up and will be operational in 2018, would allow enterprises and the Government to exchange information, help enterprises to lower their costs, and simplify trade processes. In using this platform, companies' key digital data is also open to cyber risk. Hence, I hope that in designing the platform, the Government would place the priority on cybersecurity.

Amendments to the Bill involve sensitive information which needs protection such as essential services like energy, water supply, banking and finance and transportation. The National Trade Platform is one of Singapore's most important trade infrastructures in the cyber world, and ought to be in the scope of cyber protection.

I would also urge businesses to pay heed to the newly amended Bill, especially in the newly inserted section 8B on criminal offences: anyone who obtains, retains, sells, creates, supplies or uses

whichever method to commit computer related offences, or deliberately allows these products to be used, would be committing an offence. Hence, moving forward, businesses must be much more vigilant when they are buying or selling products, to avoid being made use of unwittingly. I would like to recommend more clarity during implementation. For instance, how can businesses prove that their actions are legal and aboveboard? Will there be a relevant agency to provide guidance to businesses and will we set up an enforcement agency to monitor the implementation of this clause?

As the amended Bill would strengthen the protection of national and individual interests, then digitalisation entails a large injection of capital, manpower and resources. The Government may feel that businesses should be responsible for their own cybersecurity. However, when cyberattacks cause a certain degree of harm to "enterprises engaged in non-essential services", it would also involve public interests, and deserve legal protection. Hence, businesses hope that the Government can expand the protection scope and protect companies in the "non-essential service" areas as well, so that they do not become the target or victim of cyberattacks or trans-boundary crimes. In this way, these amendments could benefit a broader base of the business community, and the interests of industry groups and economic entities.

New technologies produce new conveniences, as well as new risks and new loopholes. I support the Government's move to regularly amend related security regulations to ensure that national, individual and business interests are not compromised. Moving forward, safeguarding cybersecurity is everyone's responsibility, and is a topic everyone should be concerned about.