SICCI Building
31 Stanley Street
Singapore 068740

Mainline: +65 6222 2855
Email: sicci@sicci.com
Website: www.sicci.com

Embargoed till delivery – Check against delivery

MR SPEAKER SIR,

I thank you for allowing me to join this debate on a topic which is of utmost importance to each one of us and especially the business and financial fraternity where I come from.

In March this year, the Singapore Indian Chamber of Commerce and Industry held a fireside chat with a leading expert on cyber security who summarized the threats and challenges for cyber security with these words.

"THE BAD GUYS ARE HERE TO STAY"

Simple words, but scary and that is why this Bill before the House is most timely as not a day passes by in Singapore or any part of the world without a cyber security related incident takes place. Recently, we were told that even a well-known Singapore law firm paid a ransom of $1.89mn in bitcoin to threat actors to regain access to data.

Honorable members who spoke before me discussed the need for the various amendments which have been proposed in this amended legislation.

The proposed Cybersecurity (Amendment) Bill represents a significant step forward in enhancing Singapore's digital resilience. Among its key features, the bill empowers the Commissioner of Cybersecurity with the authority to conduct on-site inspections and broadens the scope of incidents that must be reported. Importantly, it extends the definition of Critical Information Infrastructure (CII) to include "non-provider-owned CII," thereby holding third-party vendors accountable when they manage essential services.

Additionally, the bill introduces new regulated categories, such as Systems of Temporary Cybersecurity Concern and Entities of Special Cybersecurity Interest, to

SICCI Building
31 Stanley Street
Singapore 068740

Mainline: +65 6222 2855
Email: sicci@sicci.com
Website: www.sicci.com

Embargoed till delivery – Check against delivery

address emerging threats and evolving operational risks. Through these measures, the bill seeks to bolster our cybersecurity framework, ensuring that we stay ahead of sophisticated and rapidly evolving digital threats.

With a focus on opportunities for businesses, the amendments provide for market expansion in cybersecurity services, where businesses in the cybersecurity sector can expand their offerings to include services tailored to the new categories like "foundational digital infrastructure" and "digital service providers".

There are also avenues for innovation and product development, leading to new patents, intellectual property, and leadership in niche markets.

The increased demand for skilled cybersecurity professionals, will provide more avenues for training and workforce development.

This amendment also creates an opportunity for the insurance industry to develop new products and services around cybersecurity insurance, which could become more prevalent and necessary as businesses seek to mitigate the increased risks associated with stringent compliance requirements.

I also believe the amendments will also result in challenges for the companies in this sector.

The expanded definitions and updated requirements are likely to increase the regulatory burden on businesses and require Companies to invest in new technologies,

For smaller businesses, these increased costs may be prohibitive, potentially leading to competitive disadvantages or even business closures if they cannot afford to

SICCI Building
31 Stanley Street
Singapore 068740

Mainline: +65 6222 2855
Email: sicci@sicci.com
Website: www.sicci.com

Embargoed till delivery – Check against delivery

comply.

There are also Data Privacy Concerns.

With the broadened scope of what constitutes sensitive digital infrastructure, businesses must handle an increased volume of sensitive data, raising data privacy and security concerns.

Mismanagement of data, or failures to adequately protect data, can lead to breaches, legal penalties, and loss of consumer trust, all of which can have significant financial repercussions. capital, towards cybersecurity efforts.

Sir, I am particularly concerned about the impact of the legislative changes on small and medium enterprises as they make up the backbone of our economy, more than ninety percent. Regulatory compliance can unfairly favour established companies.

SMEs may find it particularly challenging to meet the new requirements due to limited budgets and cybersecurity expertise.

If they fail to comply, SMEs might face penalties or be forced out of certain markets, reducing the diversity of the business ecosystem and possibly leading to consolidation in certain industries, which could stifle innovation and competition.

Also, the stringent requirements for entities of special cybersecurity interest could act as a barrier to entry for new startups in critical sectors.

Meeting these high standards from the outset could be daunting and financially taxing for new market entrants.

Amidst these upsides of the legislative challenges and emerging challenges to face to make the law work and be effective, I have a few clarifications which I wish to raise with the honourable Minister.

SICCI Building
31 Stanley Street
Singapore 068740

Mainline: +65 6222 2855
Email: sicci@sicci.com
Website: www.sicci.com

Embargoed till delivery – Check against delivery

1. Businesses seek clarity on the specific criteria used to designate entities as of special cybersecurity interest.

Knowing these criteria can help companies assess their status and understand whether they fall under this designation.

Organizations need to know exactly what security measures they must implement once designated as systems of temporary cybersecurity concern.

And they want more information on the types of penalties for non-compliance and the enforcement mechanisms that will be used.

2. Businesses want to understand both the financial and operational impacts of non-compliance.

Also are there any exemptions or exceptions, particularly for small and medium-sized enterprises (SMEs) or start-ups that might face significant challenges in meeting the stringent requirements?

In its publicly available closing note on the Bill's consultation process, CSA "has communicated that further industry consultations will be conducted on the development of reporting parameters and applicable cybersecurity codes or standards". I would like to ask the Minister in what ways chambers of commerce and trade associations can help and collaborate with the various training agencies to help prepare the workforce to meet these hidden compliance costs amidst growing manpower challenges.

SICCI Building
31 Stanley Street
Singapore 068740

Mainline: +65 6222 2855
Email: sicci@sicci.com
Website: www.sicci.com

Embargoed till delivery – Check against delivery

Mr Speaker Sir,

Cybersecurity is a serious matter for Singapore, and it impacts our reputation as a global smart city.

To ensure the proposed Cybersecurity (Amendment) Bill is effective and equitable, it is crucial to consider international best practices in its formulation. We can draw valuable lessons from the United States, where a recent Executive Order focuses on harnessing AI for advanced cybersecurity, and from the European Union's Network and Information Systems (NIS) Directive, which emphasizes proactive risk assessment and public-private partnerships.

Additionally, countries like Estonia have demonstrated how continuous risk assessment and collaboration can enhance digital infrastructure protection. By aligning our roadmap with these global standards, we can develop a robust and forward-thinking cybersecurity framework that not only addresses emerging threats but also fosters innovation and industry collaboration.

Notwithstanding my clarifications and the assurances that the business community looks forward to on the concerns raised, this legislation has my fullest support.

Thank you, Mr Speaker.

Neil Parekh