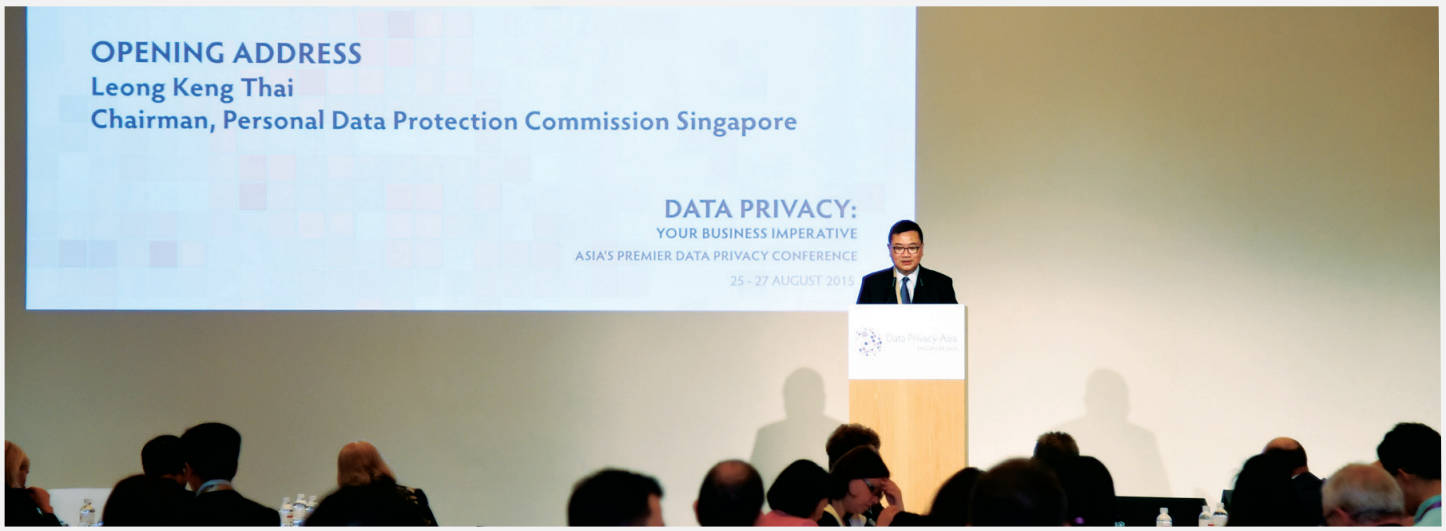

Photograph courtesy of Data Privacy Asia 2015.

Balancing Innovation and Personal Data Protection

It is important to strike a balance between innovation and personal data protection in building a Smart Nation.

Speaking at the Data Privacy Asia 2015 conference, Mr Leong Keng Thai, Chairman of the Personal Data Protection Commission (PDPC), noted that innovation has contributed significantly to the creative use of personal data and the advent of big data analytics.

Singapore's Smart Nation vision, which was announced by Prime Minister Lee Hsien Loong in November 2014, is driven by two data-related trends - Big Data, which provides useful insights for urban planning, and the Internet of Things (IoT), where everyday devices are web-connected to make business processes more efficient and lives better.

"The context of Smart Nation, Big Data and Internet of Things underlines the need for organisations and individuals to be pre-emptive in personal data governance and protection," said Mr Leong.

Data points relating to behaviours and preferences of individuals have become a competitive advantage for many organisations. However, without the assurance that such information is protected, individuals will not have confidence and trust in the organisations' use of their personal information.

"The key challenge lies in enabling the use and disclosure of data to support the progress of technology and innovation, whilst protecting personally identifiable information, to allay privacy concerns."

Cybersecurity is integral to ensuring data privacy.

Mr Leong cited a survey conducted by the Information Systems Audit and Control Association (ISACA) in 2015, in which 83 per cent of organisations surveyed listed cyber attacks as one of the top three threats they face.

Cybersecurity and Data Privacy

"Organisations need to understand the kind of threats they face, evaluate resources in coping with incidents, and strengthen protection of critical assets. In this regard, firm data protection laws can influence the incorporation of personal data governance in organisations' risk management practices," said Mr Leong.

"Data breaches should also be managed and reported immediately depending on their severity, so that relevant authorities can address the incident appropriately."

Presenting on "The Cyber Security Imperative" at the same event, Mr Wong Yu Han, Director (Strategy), Cyber Security Agency of Singapore

"The context of Smart Nation, Big Data and Internet of Things underlines the need for organisations and individuals to be pre-emptive in personal data governance and protection."

- Mr Leong Keng Thai,
Chairman of PDPC

(CSA), said the vision of a Smart Nation can succeed only if it is designed with cybersecurity in mind.

"Without cybersecurity, data privacy cannot be achieved," he said, as he highlighted the importance of building safe and trusted systems to deal with data.

The reality is that there is a black market where stolen personal data is being traded, and a dark web where all kinds of hacking tools can be bought and paid for, even using bitcoin. "All these occur in the dark web outside of Singapore's jurisdiction, which means that international engagement is key," said Mr Wong.

Formed in April 2015, CSA provides dedicated and centralised oversight of Singapore's national cyber security functions, including strategy and policy development, cyber security operations, industry development and outreach. It also works closely with educational institutions and the private sector to develop Singapore's cyber security eco-system.

In May, CSA signed a Memorandum of Understanding (MOU) with its French counterpart, Agence Nationale de la Sécurité des Systèmes d'Information to strengthen national cybersecurity capabilities through more regular bilateral exchanges, sharing of best practices and efforts to develop cyber security expertise.
An MOU on Cyber Security Cooperation was established with the Cabinet Office of the United Kingdom in July, covering areas such as cyber security incident response and cyber security talent development.

The development of world-class cybersecurity capabilities is also a very important aspect of Singapore's cybersecurity efforts, said Mr Wong. "Cybersecurity is a global game. To win it, we have to play at an international level."

Singapore has to build up a strong cybersecurity ecosystem by linking up educational institutions, industry and professional associations in a virtuous cycle to create a highly-skilled cybersecurity work force, he said.

The agency's key focus is on critical information infrastructure – infrastructure which, if damaged or compromised, will have a large impact on national security, the economy, public health and safety.

It has identified key sectors ranging from government to banking, energy and water, and is working with the respective sector leads to improve cybersecurity within and across these sectors. The agency is also studying how legislation can be strengthened.

"There is no such thing as perfect security because systems are interlinked," said Mr Wong. "We cannot do this alone."

"Individuals need to practise good cyber hygiene at work and at home, and organisations need to take ownership of their systems' cyber security. Everyone has a role to play to enable the creation of a resilient cyber security ecosystem."

This article was first published by IDA Singapore in Tech News, on 1 September 2015.

"Cybersecurity is a global game. To win it, we have to play at an international level."

- Mr Wong Yu Han,
CSA