

Cybersecurity in Asia and the Pacific - State of play and key issues in the context of trade and e-commerce - Singapore Context

Roundtable on Cybersecurity, E-commerce and Trade Facilitation

Asia-Pacific Trade Facilitation Forum

Room Kasultanan 3, Royal Ambarrukmo Hotel, Yogyakarta
7 September, 13:30 - 15:30

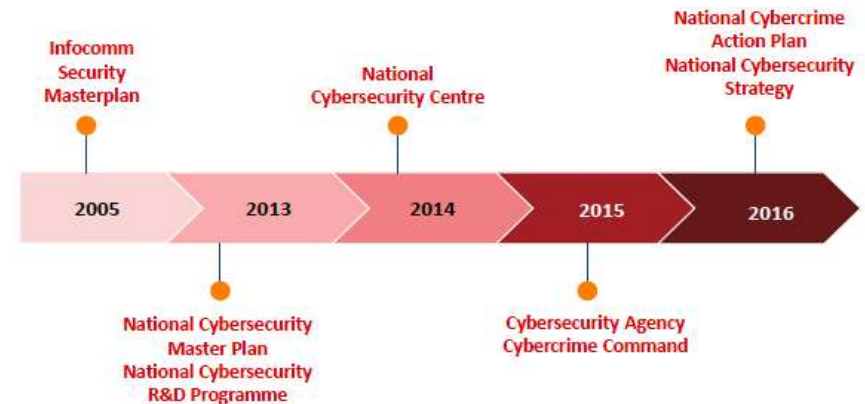
Jonathan Koh
Trade Facilitation Pte Ltd

Cybersecurity Legislation in Singapore

The need for new cybersecurity legislation

Singapore has one of the highest levels of digital connectivity in the world, a major cyber-attack, will have significant impact.

In April 2015, the Government set up the Cyber Security Agency of Singapore (CSA), as the central agency to oversee and coordinate all aspects of cybersecurity for the nation.

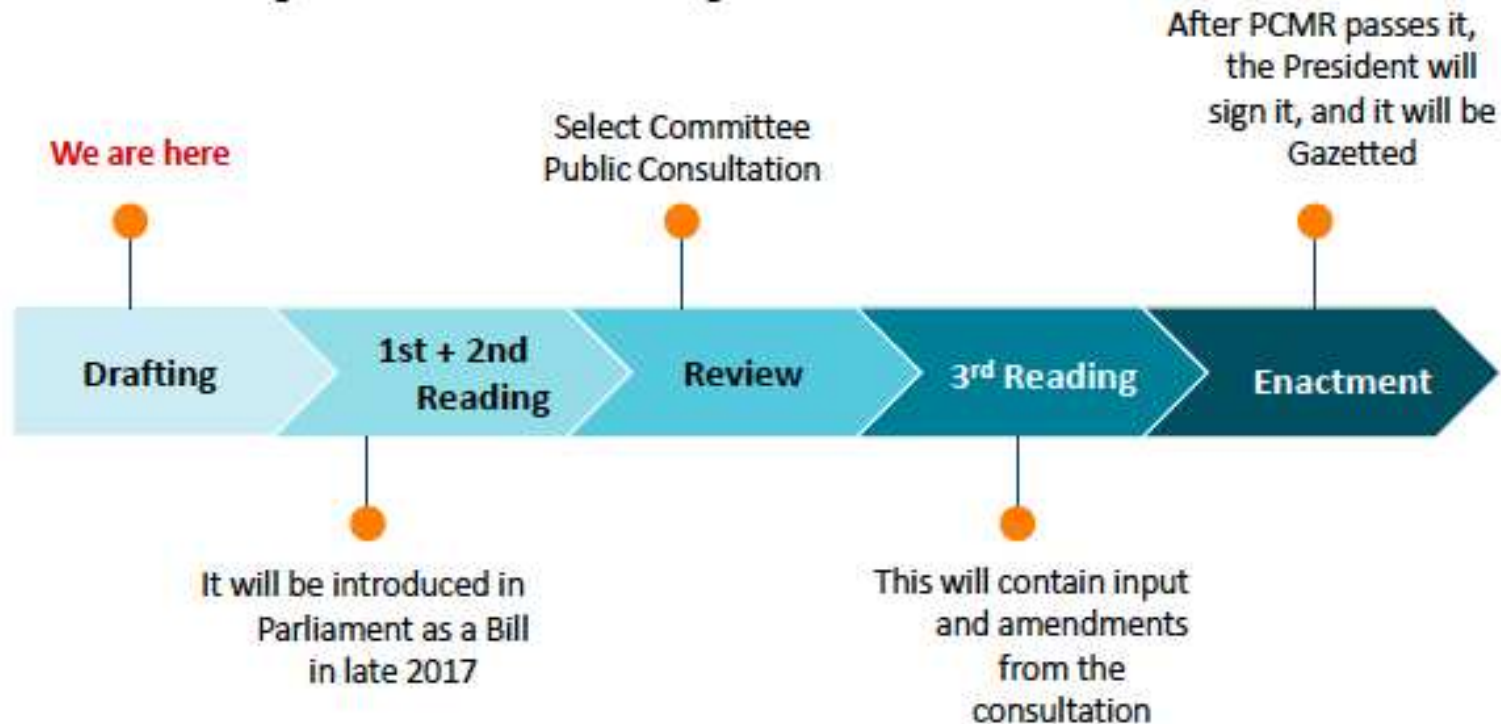


CSA's mandate is to

- (i) devise and coordinate **national cybersecurity strategy and policy development**,
- (ii) carry out both **cybersecurity capability development and crisis management** and
- (iii) adopt a holistic approach towards managing the cybersecurity of information infrastructure.

Singapore's Cybersecurity Act

The Cybersecurity Act



Singapore's National Cyber Security Strategy

4 Pillars of the Strategy

Building a Resilient Infrastructure



Creating a Safer Cyberspace



Developing a Vibrant Cybersecurity Ecosystem



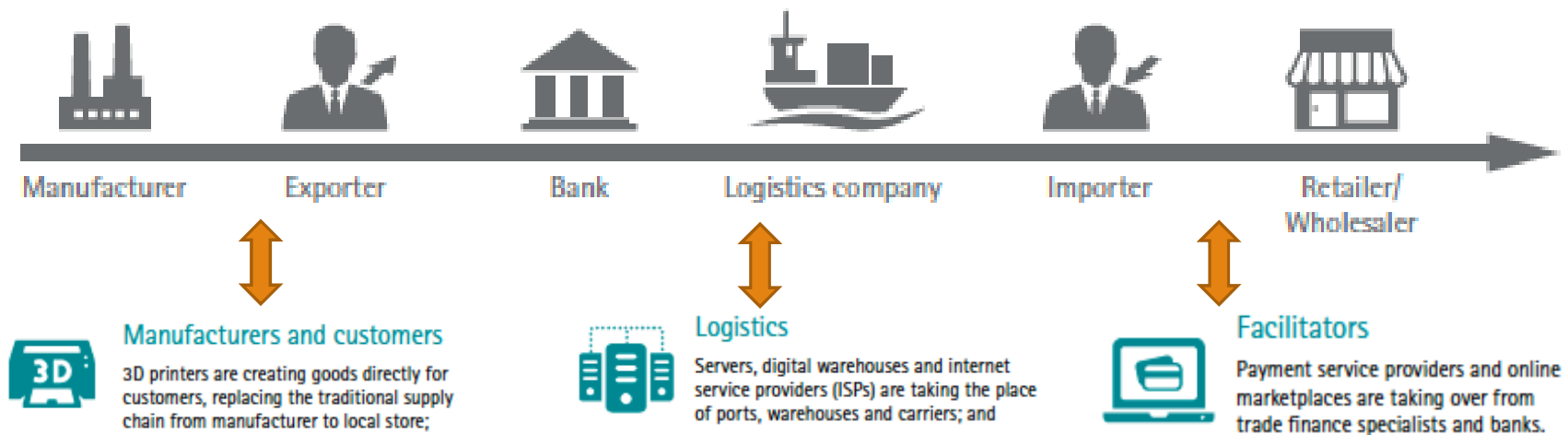
Strengthening International Partnerships



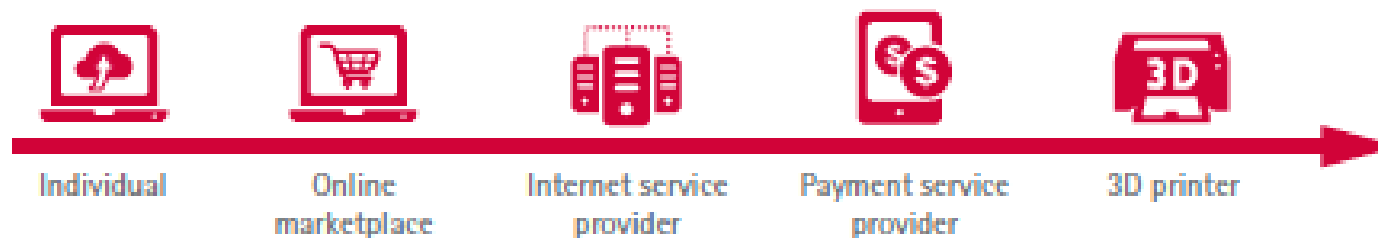
Source: "Singapore's National Cyber Security Strategy: Domestic, Regional and Global Impacts" - Benjamin Ang, Centre of Excellence for National Security, RSIS, Nanyang Technological University, Singapore.

Cybersecurity in the Digital Supply Chain / Cyber Trade

Physical supply chain



Digital supply chain



Issue 1 - Secure Data Exchange

1. Secure, Privacy-Preserving Data Exchange Platform for E-commerce and Trade

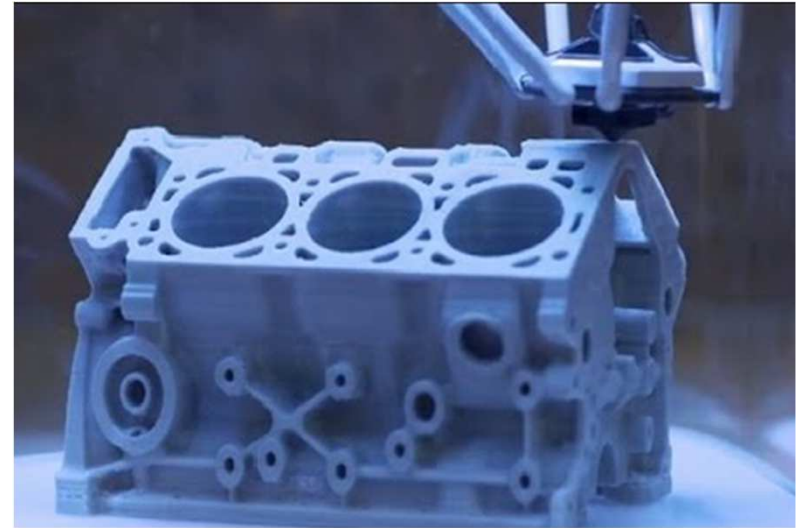
- The need for platforms providing secure data exchange and allowing multiple parties to share even sensitive data and perform analysis on it;
- Need for the different approaches to regulating cross-border data transfers, and that differing mechanisms can ensure a similar desired level of data protection;
- Need for strong, binding trade-agreement commitments that prohibit data localization requirements, support unimpeded data flows and encourage interoperability among regimes and systems

Issue 2 - Cross border E-Identification



Issue 3 - Cyber Trade

3. Fraud and Customs taxing the intangibles
(i.e., 3D Printing , IP, borderless cloud-based value chains and consumer electronic services



Thank you.

