

# Boosting Singapore's online defences

The Cyber Security Agency (CSA) yesterday launched Singapore's cyber security strategy, which spells out four broad areas to deal with the threats and opportunities presented as the country becomes more connected, and it becomes essential to safeguard systems ranging from banking software to transport to utilities services.



## 1 HARDENING SECURITY

- New cyber security Bill next year will give CSA more powers
- Bill will also require owners of critical infrastructure such as telcos and power and gas companies to strengthen their systems
- Government will roll out plan to better protect agencies and critical infrastructure operators
- More multi-sector cyber exercises to test protections and defences



## 2 EDUCATING PEOPLE

- Greater public outreach to make people aware of cyberscams and good Internet-use practices
- Cybercrime fighting capabilities of police and testing of coordination with other government agencies to be boosted
- Personal Data Protection Commission will create programme to help organisations make data protection a priority



## 3 CREATING JOBS

- More priority on developing local companies with home-grown cyber security capabilities and intellectual property
- Clearer career pathways for cyber security professionals, such as a public sector scheme of service, and support for certification and skills upgrading
- Government will step up partnerships with tertiary institutions so curriculum meets industry needs
- Heavy investment in research and development to continue



## 4 WORKING WITH FRIENDS

- Singapore will seek closer cooperation within Asean and globally to fight cyberthreats and cybercrime
- Greater discussion on policymaking and cooperation, through events like Singapore International Cyber Week
- Help to build Asean and international cyber security capabilities through capacity building and training