Securing Asean's digital future

Member states are ramping up efforts to strengthen the region's cyber defence capabilities

Cyberthreats do not respect national boundaries and the repercussions and spill-over effects can spread far beyond our region, given the interconnectedness of our increasingly digitalised world.

With Asean touted as the world's fastest growing Internet region, it is worrying that there are glaring gaps in cyber security in this region. Consultancy firm AT Kearney recently reported that last year, Asean countries collectively spent just US$1.9 billion ($2.61 billion) or 0.06 per cent of their gross domestic product on cyber security—half the global average of 0.13 per cent.

Cyber terrorism, cyberfraud, and identity theft are among some of the biggest threats facing Asean's digital economy.

According to the Minister-in-charge of Cyber Security, Mr S Iswaran (below), there is a need for Singapore to foster close relationships with Asean counterparts to build up regional cyber capacity and cooperation in cyber security.

"The many conversations and discussions among Asean member states have given us much progress to strengthen our coordination on cyber policy, cyber security initiatives and capacity building efforts. This will enable us to project a unified Asean voice internationally and advance our regional perspectives," he says.

Professor Lam Kwook Yan, Professor of Computer Science, School of Computer Science and Engineering, and Programme Chair (Secure Community), Graduate College at Nanyang Technological University, shares the view that Asean countries need to boost their cyber security competencies, particularly in view of the diverse landscape which exists today.

He says: "In fact, even within the same country, different industry sectors adopt different risk appetites to cyber security.

"Thus, it is necessary that we deepen our efforts to develop a uniform level of cyber capacity across the different Asean countries, and to create a regional cyber security framework to achieve Security-by-Design, exchange of cyberthreat intelligence and enhanced collaborative efforts in responding to cyber attacks."

In addition to business as usual, Prof Lam says that it is important to look into research and development on strategic issues, for example, cyber resilience which develops techniques that allow information systems to work properly in the face of cyberthreats.

He says: "In cyber security, the technology lifecycle is very short, anything that can potentially be used to defend or attack will be exploited almost immediately."

Facilitating regional collaboration

Singapore has started the ball rolling. This year marks the 3rd Singapore International Cyber Week and Asean Ministerial Conference on Cybersecurity (AMCC), bringing together international policy makers, industry leaders and academics to discuss common issues aimed at raising the level of regional capacity and cooperation in cyber security.

In 2016, Singapore also announced the launch of the S10 million Asean Cyber Capacity Programme (ACCP). Comprising a series of events and initiatives, the ACCP seeks to develop technical, policy and strategy building capabilities with Asean member states through a modular, multi-disciplinary and multi-stakeholder approach.

To date, more than 140 director-level officials from Asean member states have already participated in the ACCP workshops.

Mr David Koh, Commissioner of Cybersecurity and chief executive of the Cyber Security Agency of Singapore (CSA), says: "Singapore has set aside $1.5 million to build technical capability among incident responders and operators in the Asean region and we will also partner the industry to run an Asean Cyber Security Industrial Attachment Programme (CS-IAP), to offer training opportunities in Singapore for candidates from Asean countries."

Singapore is also a sponsor of CyberGreen, a global initiative aimed at raising awareness of cybersecurity and potential vulnerabilities within countries' borders, as well as preventive actions countries can take to deal with potential risks and vulnerabilities.

Earlier this year, Asean leaders had issued a statement on cyber security cooperation during the 32nd Asean Summit in a bid to address the borderless threat. In the statement, they tasked Asean
member states to closely consider and submit recommendations on feasible options of coordinating cyber security policy, diplomacy, cooperation, technical and capacity building efforts so that Asean's efforts are focused, effective, and coordinated holistically on this important cross-cutting issue.

Mr Koh says: "This statement shows that despite the inherent differences, Asean member states recognise the need for greater cross-sectoral coordination of regional cyber security efforts and are committed to working together to address this."

H.E. Md Shah Nuri, chief executive of Malaysia's National Cyber Security Agency, says: "There is good collaboration in cyber security in various communities among the Asean member states, and we recognise that cyber security is a cross-border issue and that it must be tackled through concerted efforts."

Some of these efforts include the conduct of the annual Asean CERT (Computer Emergency Response Team) Incident Drill (ACID), which is aimed at strengthening coordination among CERTs in Asean and dialogue partners.

ACID tests the coordination among the incident response teams and their incident response procedures. Singapore has convened ACID since 2006.

"We can only grow stronger if we help each other in building capacity to support the domestic requirements for cyber security professionals, raising awareness among the domestic users on cyberthreats and the importance of practising cyber hygiene, as well as harmonising legal frameworks to expedite cooperation among the law enforcement agencies in resolving cybercrimes," he adds.

Countries outside of Asean have also leaned forward to collaborate with Asean partners to drive cyber security initiatives. Japan has been strengthening cooperation among Asean Regional Forum (ARF) member countries, through the ARF-ISIM (Inter-Sessional Meeting) on Security of and in the Use of Information and Communications Technologies (ICTs), which was jointly set up with Singapore and Malaysia in August last year.

The Ambassador in charge of Cyber Policy, Masato Otaka from the Ministry of Foreign Affairs, Japan, says the country has a decade-long history of cooperation with Asean nations under the framework of the Asean-Japan Cybersecurity Policy Meeting. Also noteworthy is its Asean-Japan Cybersecurity Capacity Building Centre in collaboration with the Thai government, as well as the training plan for ICS (Industrial Cyber Security) for Asia-Pacific Region by the US Department of Homeland Security and Japan's Ministry of Economy, Trade and Industry this year.

Dr Tobias Feakin, Ambassador for Cyber Affairs, Department of Foreign Affairs and Trade, Australia, says engaging with Asean and the broader international community to strengthen collective cyber security is a key objective for Australia.

To that end, Australia is working with its Asean partners to apply international law to cyber space, implement responsible state behaviour, develop confidence and coordinate initiatives.

Funding for Australia's Cyber Cooperation Program has been increased from AUD$4 million (S$5.93 million) to AUD$14 million over four years starting this year. It has co-hosted cyber workshops with partners including Asean, on risk reduction, cyber security and cybercrime, as well as international law and norms in cyberspace.

The first iteration of the Australia-Asean Cyber Policy Dialogue will be held during the Singapore International Cyber Week 2018. Says Dr Feakin: "The Dialogue will foster a stronger relationship with our Asean partners on cyber issues that are vital for our collective security and economic growth. It will build knowledge and capacity to manage cyber threats and harness opportunities for digital trade and e-governance."

The Dialogue will be supported by a one-off AUD$1 million grant to fund practical cyber capacity building.

These initiatives bode well for the region, yet much more needs to be done, given the sheer scale of cyber security threats and the significant challenges that states face including capacity constraints.

Mr Koh says: "Ensuring cyber security is an ongoing battle. The perpetrators are constantly developing new techniques and are on a constant lookout for weaknesses. At the same time, growth in technology and e-commerce has made tackling cyber issues more urgent. We need more stakeholders to come on board to take the battle forward."

Above: Dr Feakin and Mr Koh signed a memorandum of understanding on strengthening cyber security cooperation at the Iatana as part of the 2nd Singapore-Australia Leaders' Summit in June 2017.

Above left: ACID tests the coordination among the incident response teams and their incident response procedures.

PHOTO: CYBER SECURITY AGENCY OF SINGAPORE

PROF LAM KWOK YAN, MINISTRY OF COMMUNICATIONS AND INFORMATION

PROF LAM KWOK YAN
Professor of Computer Science,
School of Computer Science and Engineering, and Programme Chair
(Secure Community). Graduate College
Nanyang Technological University