Singapore's Approach to Cyber Security

Cyber Security is the Flip Side of the Coin of Being a Smart Nation

"Cyber security is absolutely essential if we are to become a smart nation. You can't have electronic medical records, you can't have financial technology, you can't have large databases with information that could be abused or misused, you can't afford a breach of privacy. So the way I look at it, cyber security is the flip side of the coin of being a smart nation."

— Vivian Balakrishnan

Foreign Affairs Minister and Minister-In-Charge of the Smart Nation Initiative

When announcing the Smart Nation initiative last September, Singapore Prime Minister Lee Hsien Loong stressed the importance of cyber security being a central part of Singapore's smart nation ecosystem which incorporates cyber security into nascent areas such as the Internet of Things ("IoT") underpinning Singapore's Smart Nation ambition. The fact that the Singapore government is taking cyber security seriously shows in their recent move to stop all civil/government computers (about 100,000) from having Internet access in order to keep work e-mail and shared documents safe (Web surfing will still be allowed but only on employees' personal mobile devices and dedicated Internet terminals) .

Key government cyber security efforts that impact industries and companies active in Singapore include:

- Singapore's investment in cyber security as part of SG$ 2.82 billion worth of ICT tenders
- New cyber security bill to be tabled in 2017 as part of the updated national cyber security strategy stakeholder consultation which is expected to be released in the second half of 2016
- PM Lee Hsien Loong launching the National Cybersecurity Strategy document in October 2016
- Publication of the MAS Outsourcing Guidelines with a guiding principle for banks to manage outsourcing arrangements as if the services were conducted in-house

Strategy: National Cyber Security Masterplan 2018

In 2013, Singapore launched the five-year National Cyber Security Masterplan 2018 to further secure Singapore's cyber environment. The Masterplan was developed through a multi-agency effort led by the Infocomm Development Authority of Singapore ("IDA") under the guidance of the National Infocomm Security Committee.

In April 2015, the Cyber Security Agency ("CSA") was formed to develop a national strategy to tackle cyber threats. The strategy is aimed at coordinating public and private sector efforts to protect national systems in 10 critical sectors including power, transport, telecommunications and banking from increasing cyber threats.

Singapore has been partnering with like-minded nations to spur international collaboration on this front. Last year, the CSA signed a number of bilateral Memos of Understanding ("MoUs") with France, the U.K. and India. Singapore will support the regional Computer Emergency Response Team or CERT cooperation through the annual ASEAN CERT Incident Drill exercises. Furthermore, the Monetary Authority of Singapore ("MAS") co-chairs the CPMI-IOSCO Working Group, which works on strengthening the cyber resilience of financial market infrastructures.

With the regulatory, commercial and reputation risk of cyber security issues in Singapore continuing to grow, organisations must implement a robust cyber security framework consisting of policies, procedures and practices to ensure identification, protection and detection of cyber security threats and adequately respond and recover from cyber security incidents.

New Cyber Security Bill

On 21 January 2016, the Minister for Communications and Information ("MCI") and Minister-in-charge of cyber security Dr. Yaacob Ibrahim announced that a new cyber security bill would be introduced as part of Singapore's national cyber security strategy.[1] The bill is scheduled to be tabled in Parliament at the beginning of 2017. The CSA is expected to consult with stakeholders on the scope of the new law in the second half of 2016. The establishment of the CSA and the upcoming cyber security bill are part of the National Cyber Security Masterplan 2018.[2]

In regards to the new bill, Dr. Yaacob said the MCI will review the policy and legislative framework for cyber security and "broadly speaking, the bill will ensure that operators take proactive steps to secure our critical information infrastructure and report incidents." It will empower the CSA to manage cyber incidents and raise the standards of cyber security providers in Singapore. Minister Balakrishnan recently added that a "significant part of the legislation really is to just make sure providers of essential services at least take basic precautions to protect the data, protect the privacy and do not abuse the access to the information. The legislation would ensure that the data companies collect was safe from hackers."

Furthermore, the bill will:

- **Strengthen CSA's power:** It is understood that according to the new cyber security law, CSA's mandate is to assess the adequacy of Singapore's current cyber security laws and add "greater powers to secure our critical information infrastructure ("CII")" to prevent and cope with cyber security threats. The new bill is expected to include a mandatory requirement to report cyber security breaches, currently not required under CMCA. The requirement is likely to include a stipulated time frame;
- **Identify critical sectors:** Priority will be given to Singapore's critical sectors of energy, water, transport, health, government, infocomm, media, security and emergency services, and banking and finance (this largely mirrors the present scope of the CMCA, although it remains to be seen what these wider powers will entail);
- **Grow talent and manpower:** There will be a strong focus on growing cyber security talent and manpower. Singapore is seeking international cooperation and is currently working with the private sector to raise public awareness of the importance of cyber security.

What is Expected from the Financial Sector?

Within the financial sector, MAS has set minimum expectations and guidance for financial institutions to manage technology and cyber risks in the Technology Risk Management Guidelines[3] as well as through circulars and advisories issued to financial institutions. The MAS exercises its supervisory oversight of cyber security risks through onsite inspections and offsite supervision of financial institutions.

In his speech at the Asia Cyber Risk Summit on 16 May 2016[4], Mr. Bernard Wee, Executive Director, MAS, stated that the MAS expects financial institutions to implement strong controls in their IT systems, as set out in the MAS Technology Risk Management Guidelines. Furthermore, MAS Deputy Chairman and Minister for Trade and Industry, Mr. Lim Hng Kiang recently stated that banks need to take a holistic approach to address cyber risk given cyber criminals and hackers often probe for and target the weakest links in the system. A system of cyber intelligence exchange to identify potential vulnerabilities and frequent testing of the robustness of cyber defences are key to this effort.[5]

Cyber Risk Management Project

At the Asia Cyber Risk Summit, the MAS also announced the Cyber Risk Management Project ("CRMP"). The CRMP facilitates the systematic collection and modelling of cyber risks data, bringing together government bodies (in the form of the MAS and the Singapore Cyber Security Agency), public institutions (including the Nanyang Technological University) and a number of private organisations. The focus of the initiative is on fostering research and development into cyber threat assessment tools and encouraging the uptake of cyber risk insurance.

[1] MCI addendum to President Tan's annual address
[2] https://www.ida.gov.sg/Programmes-Partnership/Store/National-Cyber-Security-Masterplan-2018
[3] MAS Technology Risk Management Guidelines - June 2013 - http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2016/A-Bold-Approach-to-Cyber-Risk-Management.aspx
[4] http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2016/A-Bold-Approach-to-Cyber-Risk-Management.aspx
[5] http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2016/Sharpening-Risk-Management-Capabilities.aspx

The MAS' CRMP does not include any call for specific new cyber security compliance measures. However, at the time of the announcement MAS officials responded to questions about the recent cyber-attacks directed at banks in the region using the SWIFT financial messaging system, reportedly causing losses of US$ 81 million to a Bangladesh bank. MAS spokespeople explained that they would continue to monitor the landscape of cyber security threats and provide additional guidance where necessary.

MAS Outsourcing Guidelines

A concrete step in securing sound cyber management for financial institutions in Singapore will be through transparent management of outsourced services, with a guiding principle for banks to manage outsourcing arrangements as if the services were conducted in-house. This follows last year's MAS review on guidelines associated with cloud services, customer information and risk management frameworks.

The MAS Outsourcing Guidelines, expected to be published shortly, will include MAS' expectations on the use of cloud computing services by financial institutions and a greater emphasis on safeguarding customer information. Also, the revised guidelines will no longer require financial institutions to pre-notify MAS of any outsourcing arrangements on a case-by-case basis. Instead, they are expected to be responsible for ensuring the safety of all of their outsourcing arrangements on an ongoing basis.

Minister Lim said the guidelines were not intended to be exhaustive, with MAS recognising that the diverse range of outsourcing arrangements and rapid pace of progress in digital technology preclude a prescriptive approach to risk management practices for outsourcing, or a one-size-fits-all set of rules. MAS will adopt a risk-based approach in implementing the guidelines.

New Government Technology Organisation

The MCI will restructure the Infocomm Development Authority of Singapore ("IDA") and the Media Development Authority of Singapore ("MDA") to form the Government Technology Organisation ("GTO") and the Info-Communications Media Development Authority of Singapore ("IMDA").[6]

While IMDA's main focus will be to implement Singapore's Infocomm Media Masterplan, the GTO will continue to prioritise the cyber security needs of Singapore's government infrastructure and help government agencies capitalise on innovation through new technology trends such as robotics, artificial intelligence, IoT and Big Data. The new organisation will also play a central role in supporting Singapore's Smart Nation vision, especially in delivering the Smart Nation Platform and Smart Nation application.

Singapore International Cyber Week

On 10-12 October 2016, the CSA will hold the inaugural Singapore International Cyber Week ("SICW"), where Prime Minister Lee will launch the National Cybersecurity Strategy document. During the SICW, the annual GovernmentWare ("GovWare") Cyber Security conference will take place, as well as the inaugural ASEAN Ministerial Conference on Cybersecurity ("AMCC") and ASEAN Cybercrime Prosecutors' Roundtable meeting ("CPRM") hosted by CSA in collaboration with Attorney General's Chambers, Ministry of Foreign Affairs and Ministry of Home Affairs.[7]

GovWare regularly attracts top level representation from government, industry, thought leaders and C-level executives from the user community for in-depth discussions on technology, applications and user perspectives.

ASEAN Cooperation

During the SICW, ASEAN ministers will meet to discuss the various cyber security cooperation initiatives by the various ASEAN countries and dialogue partners, and provide a platform for discussion on what could be done to strengthen cyber security in the region.

SICW will also host the ASEAN Cybercrime Prosecutors' Roundtable Meeting which will serve as a platform for the sharing of knowledge and expertise between prosecutors on fighting cybercrime regionally. It also aims to promote the development of effective legislative frameworks within ASEAN for combating cybercrime.

> "Notification of, and engagement with, consumers, employees, affected parties and regulators are also critical factors in mitigating commercial, legal and reputational risk from cyber breaches. It is also critical that organisations prepare a cyber security breach response and have a communications program in place to ensure that both regulatory requirements and stakeholder expectations are met."

[6] Formation of Infocomm Media Development Authority and Government Technology Organisation

[7] Singapore International Cyber Week official webpage

Conclusion

The recent initiatives to strengthen cyber security are part of the government's ongoing efforts to reach out to individuals, the private sector and universities to raise security awareness and create the right skills and mindset to become a Smart Nation. With the regulatory, commercial and reputation risk of cyber security issues in Singapore continuing to grow, organisations must implement a robust cyber security framework consisting of policies, procedures and practices to ensure identification, protection and detection of cyber security threats and adequately respond and recover from cyber security incidents.

Notification of, and engagement with, consumers, employees, affected parties and regulators are also critical factors in mitigating commercial, legal and reputational risk from cyber breaches. It is also critical that organisations prepare a cyber security breach response and have a communications program in place to ensure that both regulatory requirements and stakeholder expectations are met.

Kees Jan Boonen
Director
+65 6831 7854
keesjan.boonen@fticonsulting.com