COUNTRY: **SINGAPORE**

Legal Foundations: Singapore adopted a five-year National Cyber Security Masterplan in 2013, and also is continuing to develop its critical infrastructure protection regime. Singapore has some broad legal infrastructure in place for cybersecurity. The new Singapore Cybersecurity Agency will begin operations in April 2015.

Operational Entities: SingCERT was established as the national computer emergency response team in 1997, and the Infocomm Development Authority (IDA) acts as a high-profile coordinating agency for all aspects of information communications policy, including cybersecurity.

Public-Private Partnerships: Singapore's government agencies work closely with the private sector in the field of cybersecurity, and there is a formal commitment to the development of public-private partnerships.

Sector-Specific Cybersecurity Plans: The Infocomm Security Masterplan 2 (MP2), launched in 2008, stated the Singapore government would work to develop sector-specific security programs, particular with regard to owners of critical infrastructure. MP2 has been subsequently succeeded by a plan that, although building on MP2, does not include a direct commitment to the sector-based programs.

Education: The National Cyber Security Masterplan 2018, published in 2013, includes a strong commitment to cybersecurity education.

Additional Cyberlaw Indicators: Singapore avoids undue legal and regulatory restrictions on cybersecurity service providers.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The National Cyber Security Masterplan 2018 was adopted in 2013. It outlines a strategic direction for the enhancement of cybersecurity in Singapore across a five-year timeframe.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	Critical information infrastructure, referred to in Singapore as "Infocomm Infrastructure", was the focus of both the Infocomm Security Masterplan 2005 and the second Masterplan 2008. As part of the National Cyber Security Masterplan 2018, Singapore aims to complete the Critical Infocomm Infrastructure Protection Assessment programme which will identify and assess the information communications systems that are critical to the operation of critical infrastructures.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	◑	While there is no legislation in place in Singapore that requires the establishment of a written information security plan, information security has been addressed in each of Singapore's "infocomm" Masterplans since 2005.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Official Secrets Act 1935 <statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A3bc8b443-65c7-4c42-a4c3-49b650267c16%20Depth%3A0%20Status%3Ainforce;rec=0> provides a definition for official information but does not provide a system of classification or classification levels. In practice, Singapore uses a four-tiered system of classification for sensitive government information.
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	The Official Secrets Act 1935 <statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A3bc8b443-65c7-4c42-a4c3-49b650267c16%20Depth%3A0%20Status%3Ainforce;rec=0> details security practices and requirements for official information in general, but does not map these to specific risk levels.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	◑	There is no legislation in place in Singapore that requires an annual cybersecurity audit. The National Cyber Security Masterplan 2018 calls for an enhanced Cyber Watch Centre whose new capabilities will aim to improve the overall security monitoring effectiveness for the public sector.

COUNTRY: SINGAPORE

	QUESTION	RESPONSE	EXPLANATORY TEXT
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✖	There is no legislation or policy in Singapore that requires a public report on cybersecurity capacity for the government.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	◑	Chief information officers are assigned to ministries, however there is no legislation or policy in place requiring each ministry to have a chief information officer. In August 2014 the Infocomm Development Authority of Singapore (IDA) announced their intention to appoint Chief Information Security Officers to agencies <events.futuregov.asia/articles/2014/aug/28/singapore-agencies-appoint-chief-information-secur/>.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	There no legislation or policy in place in Singapore that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	Singapore's information security Masterplans, including the National Cyber Security Masterplan 2018, include an appropriate definition for "critical infocomm (information security) infrastructure".
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	Singapore's Cyber Security Masterplan 2018 promotes international engagement and cooperation. However, it does not include (public) details regarding the adoption or promotion of international standards. Singapore has a strong track record of applying international standards and recognizing international certification schemes in the broader ICT and telecommunications sector.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	SingCERT <www.singcert.org.sg> was established in 1997. It is responsible for coordinating incident response procedures for incidents that occur within .sg networks.
2.	What year was the computer emergency response team (CERT) established?	1997	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The Infocomm Development Authority of Singapore (IDA) <www.ida.gov.sg>, which operates under the Ministry of Communications and Information, is responsible for planning and developing information communications policy, and acts as the government's Chief Information Officer. In addition, the Singapore Infocomm Technology Security Authority (SITSA) has been active since 2009. It role is to oversee operational infocomm technology. In addition, the Cyber Security Agency (CSA) <www.csa.gov.sg> has been operational since April 2015. It is a high-level central agency with the task of coordinating public- and private-sector strategy and efforts to protect national systems from cyber threats.
4.	Is there an incident-reporting platform for collecting cybersecurity incident data?	✔	SingCERT <www.singcert.org.sg> is tasked with cyber incident data collection. It provides an email-based online reporting platform, through which incidents occurring on .sg networks may be logged.
5.	Are national cybersecurity exercises conducted?	◑	As of May 2015, only sector-specific exercises have been conducted. However, the National Cyber Security Masterplan 2018 outlines the National Cyber Security Exercise programme which will comprise national cross-sectorial cyber exercises.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	Singapore does not have a discrete national incident management structure for responding to cyber incidents.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership (PPP) for cybersecurity?	✔	The Cyber Security Awareness Alliance <gosafeonline.sg> is a collaborative bodies of public and private entities whose goal is to promote the awareness and adoption of cybersecurity practices. It is supported by the Infocomm Development Authority of Singapore (IDA) <www.ida.gov.sg>, the Chief Information Office of Singapore, and is addressed in the National Cyber Security Masterplan 2018. In addition, SingCERT <www.singcert.org.sg>, the national CERT, works closely with the private sector.

COUNTRY: SINGAPORE

	QUESTION	RESPONSE	EXPLANATORY TEXT
2.	Is industry organized (i.e., business or industry cybersecurity councils)?	◑	While there is not a specific industry-led association dedicated to cybersecurity, there are a few organizations operating in areas that are significantly engaged with cybersecurity issues, including: • Singapore Infocomm Technology Federation (SITF) <www.sitf.org.sg> — an industry association for companies in the information, communication and media sector; and • IT Management Association (ITMA) <www.itma.org.sg> — an association of managers working in the information technology field.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	✖	As of May 2015, there are no documented new public-private partnerships being planned in Singapore. The Assistant Chief Executive of the government's Chief Information Office, the Infocomm Development Authority of Singapore (IDA) <www.ida.gov.sg>, has indicated the government will be moving away from the public-private partnership model for addressing cybersecurity concerns, and towards the promotion of government-owned products <events.futuregov.asia/articles/2014/may/27/singapore-government-reveals-s12-billion-new-ict-t>.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	◑	The Infocomm Security Masterplan 2 (MP2) <www.ida.gov.sg/Programmes-Partnership/Store/Infocomm-Security-Masterplan-2>, launched in 2008, states that the Singapore government would work to develop sector-specific security programs, particular with regard to owners of critical infrastructure. MP2 has been subsequently succeeded by the National Cyber Security Masterplan 2018 (published 2013) that, although building on MP2, does not include a direct commitment to the sector-based programs.
2.	Have sector-specific security priorities been defined?	◑	The superseded Infocomm Security Masterplan 2 (MP2) <www.ida.gov.sg/Programmes-Partnership/Store/Infocomm-Security-Masterplan-2> proposed the development of sector-specific security programs. Such programs would define sector security priorities, however the programs themselves are not publicly available. While it identifies the benefit of cross-sector engagement, the current National Cyber Security Masterplan 2018 does not address sector-specific programs.
3.	Have any sector cybersecurity risk assessments been conducted?	◑	Infocomm Security Masterplan 2 (MP2) <www.ida.gov.sg/Programmes-Partnership/Store/Infocomm-Security-Masterplan-2> proposed developing sector-specific security programs — however, it is unclear whether such programs would specifically involve cybersecurity risk assessments. The programs are not publicly available.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	The National Cyber Security Masterplan 2018 (published 2013) <www.ida.gov.sg/Programmes-Partnership/Store/National-Cyber-Security-Masterplan-2018> includes a strong commitment to cybersecurity education. It states: "Current efforts will be reinforced to raise infocomm security awareness and adoption amongst users and businesses. This includes the Cyber Security Awareness and Outreach programme to augment existing outreach channels (e.g., via online and social media platforms, educational talks, road-shows, seminars, and print advertorials) and explore new avenues that offers wider coverage and reach to users, such as broadcast media."
	ADDITIONAL CYBERLAW INDICATORS		
1.	Are cybersecurity services able to operate free from laws that discriminate based on the nationality of the vendor?	✔	Singapore is a member of the WTO plurilateral Agreement on Government Procurement, which includes rules guaranteeing fair and non-discriminatory conditions of international competition. These rules cover most large contracts. In practice, many government procurement opportunities require a joint venture with a local firm or the establishment of a local agency arrangement. Singapore provides additional market access concessions to its trading partners under its bilateral free trade agreements.
2.	Are cybersecurity services able to operate free from laws or policies that mandate the use of specific technologies?	✔	There are no specific mandatory technology requirements in laws or policies.

COUNTRY: SINGAPORE

	QUESTION	RESPONSE	EXPLANATORY TEXT
3.	Are cybersecurity services able to operate free from additional local testing requirements that go beyond international testing requirements?	✔	There are no local testing requirements for cybersecurity services, as of May 2015.
4.	Are cybersecurity services able to operate free from laws or policies that mandate the submission of source code or other proprietary information?	✔	There are no requirements for cybersecurity services to submit source code, as of May 2015.
5.	Are cybersecurity services able to operate free from laws or policies that require service providers to locate their servers inside the subject country?	✔	There are no specific regulations in Singapore that require service providers to locate their servers inside the country. Some stricter rules apply to the location of financial service data.
6.	Are cybersecurity services able to operate free from unnecessary restrictions on cross-border data flows (such as registration requirements)?	✔	There are no registration requirements in Singapore. The privacy law does include some basic, light-touch, cross-border transfer rules.