COUNTRY: **MALAYSIA**

Legal Foundations: Malaysia does not have a single cybersecurity strategy, but refers to its collection of policies and strategies as Malaysia's Cyber Security Policy. The Malaysian Government has announced that this suite of policies will be completely revised and strengthened by 2017.

Operational Entities: CyberSecurity Malaysia runs the national cert — MyCert — as well as the reporting service Cyber999. It also acts as the chief authority on information security.

Public-Private Partnerships: CyberSecurity Malaysia organizes an awards event which doubles as an annual convention on cyber security in a public-private partnership model.

Sector-Specific Cybersecurity Plans: Public-private cooperation is a key principle of Malaysia's National Cyber Security Policy, which uses a sector-based approach to address security concerns and identifies 10 critical sectors for this purpose.

Education: The Cybersafe program provides a comprehensive suite of materials and activities relating to cybersecurity.

Additional Cyberlaw Indicators: Malaysia's government procurement regime includes certain restrictions on global cybersecurity providers, but the country otherwise avoids many undue legal and regulatory burdens.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	◑	Malaysia does not have a dedicated cybersecurity strategy in place. CyberSecurity Malaysia <www.cybersecurity.my> refers to the collation of publications and strategies associated with cybersecurity as Malaysia's Cyber Security Policy. The Malaysian government has announced that this suite of policies will be completely revised and strengthened by 2017.
2.	What year was the national cybersecurity strategy adopted?	–	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	◑	There is no comprehensive critical infrastructure protection (CIP) strategy or plan in place in Malaysia. However the Ministry of Science, Technology and Innovation runs the Critical National Information Infrastructure portal <cnii.cybersecurity.my>, which provides information on the scope of CIP policy in Malaysia and the CIP objectives of the ministry's working groups.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in Malaysia that requires the establishment of a written information security plan.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Official Secrets Act 1972 <www.agc.gov.my/Akta/Vol.%202/Act%2088.pdf> requires information whose disclosure may pose a risk to Malaysia to be classified a state secret, and be given a classification level, according to a four-tiered classification system.
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	◑	The Official Secrets Act 1972 <www.agc.gov.my/Akta/Vol.%202/Act%2088.pdf> requires information, of which disclosure may pose a risk to Malaysia to be classified a state secret. It details certain security requirements and practices that must be followed when handling state secrets, however these are not necessarily mapped to risk levels.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation or policy in Malaysia that requires an annual cybersecurity audit.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	There is no legislation or policy in Malaysia that requires a public report on cybersecurity capacity for the government. CyberSecurity Malaysia <www.cybersecurity.my> publishes regular reports — however, there are no legal requirements around the content or frequency of such publications.

COUNTRY: MALAYSIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	◑	While Malaysia does have ministerial level chief information officers, there is no legal requirement for each agency to have a chief information officer or chief security officer.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	There is no legislation or policy in Malaysia that requires the establishment of a written information security plan.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Ministry of Science, Technology and Innovation has published an appropriate definition for "critical infrastructure protection" through its Critical National Information Infrastructure portal <cnii.cybersecurity.my>.
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	There are no specific cybersecurity standards or certification requirements for procurement in Malaysia, as of May 2015. Malaysia is a Certificate Authorizing Member of the Common Criteria <www.commoncriteriaportal.org> and this indicates a commitment to recognize international standards.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	MyCERT <www.mycert.org.my> was established in 1997. It is responsible for the coordination and analysis of cyber incident responses across all Malaysian networks. MyCERT also conducts operational research in the area of emerging threats.
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)?	✔	CyberSecurity Malaysia <www.cybersecurity.my> acts as the national competent authority for network and information security in Malaysia. It is a government agency functioning under the Ministry of Science, Technology and Innovation.
4.	Is there an incident-reporting platform for collecting cybersecurity incident data?	✔	MyCERT <www.mycert.org.my> runs the Cyber999 Help Centre www.mycert.org.my/cyber999, a reporting platform through which all Malaysian internet users may log cyber incidents. It maintains multiple reporting channels including online forms, email, and telephone.
5.	Are national cybersecurity exercises conducted?	✔	Malaysia has conducted the national cyber exercise, X-Maya, yearly since 2008.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	The National Cyber Crisis Management Plan, as detailed in the National Security Council's Directive No. 24 <www.cybersecurity.my/data/content_files/44/1212.pdf?.diff=1385607561>, was launched in 2013. It is a systematic vertical notification and coordination system that is activated in the event of a cyber-incident.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership (PPP) for cybersecurity?	✔	The Cyber Security Malaysia - Awards, Conference & Exhibition (CSM-ACE) <www.csm-ace.my> is a public- private-partnership event, hosted by CyberSecurity Malaysia <www.cybersecurity.my> that provides a platform for information sharing and cybersecurity. It is attended by government representatives and professionals from the private and academic sectors.
2.	Is industry organized (i.e., business or industry cybersecurity councils)?	◑	The Information Security Professional Association of Malaysia (ISPA) <ispa.my> is a representative-body for information security professionals. It is not, however, a wider industry-led platform to facilitate cooperation on information security issues. The Malaysian National Computer Confederation (MNCC) <www.mncc.com.my> is a representative-body for organizations in the computer and software field. It is not a dedicated association for cybersecurity.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	–	Malaysia has a defined public-private partnership platform for cybersecurity in place.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✔	The National Cyber Security Policy (NCSP) <cnii.cybersecurity.org.my/main/ncsp/tncsp.html> is the policy framework that supports Malaysia's critical national information infrastructure. The NCSP, of which public-private cooperation is a key principle, uses a sector based approach to address security concerns and identifies ten critical sectors for this purpose.

COUNTRY: MALAYSIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
2.	Have sector-specific security priorities been defined?	✖	The National Cyber Security Policy (NCSP) <cnii.cybersecurity.org.my/main/ncsp/tncsp.html> uses a sector-based approach to address security concerns, however sector-specific security priorities for each of the ten identified critical sectors are not publicly available.
3.	Have any sector cybersecurity risk assessments been conducted?	✖	The National Cyber Security Policy (NCSP) <cnii.cybersecurity.org.my/main/ncsp/tncsp.html> provides a sector-based approach to cybersecurity process, however it is unclear whether cybersecurity risk assessments are part of that approach. As of May 2015, no sector or general risk assessments are 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 Cybersafe program <www.cybersafe.my> provides a comprehensive suite of materials and activities relating to cybersecurity, with special sections aimed at 'kids', 'youth,' and 'parents'.
	ADDITIONAL CYBERLAW INDICATORS		
1.	Are cybersecurity services able to operate free from laws that discriminate based on the nationality of the vendor?	◑	Preferential government procurement policy favors locally owned businesses in some sectors, including substantial price bonuses for domestic suppliers. International tenders are sometimes invited if goods and services are not available locally, but all foreign organizations must register with the Malaysian Department of Finance. Malaysia became an observer to the WTO plurilateral Agreement on Government Procurement in July 2012, but is not yet a full member.
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.
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 Malaysia that require service providers to locate their servers inside the country.
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 Malaysia. The privacy law does include some basic, light-touch, cross-border transfer rules.