BSA | The Software Alliance

COUNTRY: **TAIWAN**

Legal Foundations: Taiwan's National Information and Communication Security Taskforce has developed several National Information Security Policy and Strategy documents. The current strategy covers the period from 2013 to 2016.

Operational Entities: Taiwan has two computer emergency response teams in place and collectively they cover cybersecurity incidents across the Taiwanese network. Government responsibility for network information and security rests within the Ministry for National Defense.

Public-Private Partnerships: While there is no defined public-private partnership in Taiwan for cybersecurity, the CERT does closely liaise with the private sector.

Sector-Specific Cybersecurity Plans: There is no joint public-private sector plan in Taiwan that addresses cybersecurity.

Education: Cybersecurity education is coordinated by the National Information and Communication Security Taskforce. The Ministry of Education has also developed a cybersecurity education website.

Additional Cyberlaw Indicators: Taiwan avoids most undue restrictions on cybersecurity service providers, but it does allow for the restriction of certain cross-border data flows.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	Taiwan's National Information and Communication Security Taskforce has developed several National Information Security Policy and Strategy documents. The current strategy covers the period from 2013 to 2016 <www.nicst.ey.gov.tw/News3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF>. The national strategy is a comprehensive and detailed document including timelines, budget commitments, and implementation plans.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The National Information and Communication Security Taskforce has developed several relevant plans, including the National Information Infrastructure Security Mechanism Building Plan (2005–2008) and the National Information and Communication Development Plan (2009–2012) <www.nicst.ey.gov.tw>. Critical infrastructure protection is also addressed briefly in the National Information Security Policy and Strategy 2013–2016 <www.nicst.ey.gov.tw/News3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF>.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	No	Taiwan does not have legislation or policy in place that requires the establishment of a written information security plan. Regular national information security plans have been published since 2005.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Classified National Security Information Protection Act 2003 <law.moj.gov.tw/eng/LawClass/LawAll.aspx?PCode=I0060003> details a three-tiered classification system, with each classification level being assigned according to level of risk to national security unauthorized disclosure would cause. Notably, the Act includes discrete restrictions on what can be classified. Article 5 requires that the amount of classified information be the absolute minimum, and that information shall not be classified in order to conceal violations of law or administrative error, restrain competition, prevent embarrassment to a person or entity, or prevent or delay the public release of information that does not require protection in the interest of national security.

COUNTRY: TAIWAN

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✓	The Classified National Security Information Protection Act 2003 details information security practices for classified government information. These include both general practices, and practices mapped to the classification level assigned to the information. Those classification levels are assigned according to the amount of damage to national security their unauthorized disclosure would cause. Elaboration on the meaning of the terms used in the act, including definitions of what is considered "damaged," is included in the Enforcement Rules of the Classified National Security Information Protection Act 2003.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✓	Taiwan's National Information Security Policy and Strategy (2013 to 2016) includes a commitment to annual security audits in key risk areas <www.nicst.ey.gov.tw/News3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF>. Approximately 20–30 audits are undertaken each year.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◐	Taiwan does not have legislation or policy in place that requires a public report on cybersecurity capacity for the government. However, they do have other commitments in place requiring cybersecurity case studies to be undertaken and published.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✓	In Taiwan, the deputy head of each agency has been appointed as the chief security officer, in accordance with the National Information Security Policy and Strategy (2013 to 2016) <www.nicst.ey.gov.tw/News3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF>.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✗	Taiwan does not have legislation or policy in place that requires mandatory reporting of cybersecurity incidents in the private sector.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✓	Taiwan's National Information Security Policy and Strategy (2013 to 2016) includes an appropriate definition for "critical infrastructure protection" <www.nicst.ey.gov.tw/News3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF>.
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	Not applicable	There are no specific cybersecurity standards or certification requirements for procurement in Taiwan, as of May 2015.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✓	TWCERT/CC <www.cert.org.tw> was established in 1998. It is responsible for incidents occurring across all .tw networks and Taiwanese IP addresses. TWNCERT <www.twncert.org.tw> is responsible for incidents occurring in Taiwanese government or military networks.
2.	What year was the computer emergency response team (CERT) established?	1998	
3.	Is there a national competent authority for network and information security (NIS)?	✓	There are multiple government agencies in charge of national network and information security in Taiwan. The National Information and Communication Security Taskforce, which reports to the government executive, addresses general cybersecurity security issues. The National Security Bureau, which reports to the President of Taiwan, is responsible for national information security issues that relate to homeland security and the military. The Office of the Deputy Chief of the General Staff for Communication, Electronics and Information has responsibility for ensuring the integrity of Taiwan's information infrastructure. It reports to the National Security Bureau.
4.	Is there an incident-reporting platform for collecting cybersecurity incident data?	✓	Both TWCERT/CC <www.cert.org.tw> and TWNCERT <www.twncert.org.tw> provide online incident-reporting services through which cyber incidents may be logged.
5.	Are national cybersecurity exercises conducted?	✓	The Office of the Deputy Chief of the General Staff for Communication, Electronics and Information has conducted cyber exercises in conjunction with the Taiwanese military.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✓	The National Information and Communication Security Taskforce is responsible for Taiwan's national incident management structure.

COUNTRY: TAIWAN

	QUESTION	RESPONSE	EXPLANATORY TEXT
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership (PPP) for cybersecurity?	◑	While there is no defined public-private partnership in Taiwan for cybersecurity, TWCERT/CC <www.cert.org.tw> liaises with the private sector in order to implement and coordinate incident response procedures. Private sector experts also participate as special committee members to contribute and provide their expertise to both the National Information and Communication Security Taskforce and the National Security Bureau.
2.	Is industry organized (i.e., business or industry cybersecurity councils)?	◑	While there is no industry association dedicated to cybersecurity in Taiwan, the Information Service Industry Association of ROC (CISA) <www.cisanet.org.tw> is composed of domestic and international companies and institutes that operate in the information services industry.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	◑	As of May 2015, there are no documented specific public-private partnerships being planned in Taiwan. However, Taiwan's National Information Security Policy and Strategy (2013 to 2016) includes a workplan to explore public-private partnerships during the period 2013–2016 <www.nicst.ey.gov.tw/News3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF>.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	There is no joint public-private sector plan in Taiwan that addresses cybersecurity.
2.	Have sector-specific security priorities been defined?	◑	Sector-specific security priorities have not been publicly defined, nor has there been a proposal to define sector security priorities in legislation or policy, as of May 2015. However, Taiwan's National Information Security Policy and Strategy (2013 to 2016) includes a discussion of potential sector-specific approaches in areas like health, finance, transport, and energy <www.nicst.ey.gov.tw/News3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF>.
3.	Have any sector cybersecurity risk assessments been conducted?	✖	Sector cybersecurity risk assessments have not been conducted in Taiwan.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	Cybersecurity education is coordinated by the National Information and Communication Security Taskforce. The Ministry of Education has also developed a cybersecurity education website <https://isafe.moe.edu.tw/>. Schools at all levels can acquire cybersecurity education materials and the latest information from the campus information security service website <cissnet.edu.tw>.
	ADDITIONAL CYBERLAW INDICATORS		
1.	Are cybersecurity services able to operate free from laws that discriminate based on the nationality of the vendor?	✔	Taiwan 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.
2.	Are cybersecurity services able to operate free from laws or policies that mandate the use of specific technologies?	✔	There are no mandatory requirements to use specific technologies in Taiwan, as of May 2015.
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.

COUNTRY: TAIWAN

QUESTION	RESPONSE	EXPLANATORY TEXT
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 requirements to locate servers within Taiwan, as of May 2015.
6. Are cybersecurity services able to operate free from unnecessary restrictions on cross-border data flows (such as registration requirements)?	◑	The Taiwanese government can restrict the transfer of personal data to specific countries on the grounds of 'national interest' or where the target country does not provide sufficient privacy protection. This approach is more restrictive than other countries in the region, and in 2012 all transfers to mainland China were banned.