COUNTRY: **JAPAN**

Legal Foundations: Japan's Cybersecurity Strategy, adopted in 2013, is a comprehensive document that identifies not only proposed measures, but also address the roles of various stakeholders with regard to Japanese cybersecurity. The legal framework supporting cybersecurity is one of the strongest in the region, following the recent passage of the Basic Law on Cybersecurity 2014. Japan also passed a new state secrets law in December 2013 that imposes much stronger security practices on the handling of sensitive information and stronger penalties in cases of unauthorised access.

Operational Entities: The operational entities in Japan that relate to cybersecurity are all mature. The national cert, JCERT/CC, was established in 1996 and maintains a strong web presence. The Cyber Security Strategy Headquarters has also been established under the Basic Law on Cybersecurity 2014.

Public-Private Partnerships: Japan has a mature public-private partnership structure for cybersecurity, including J-CSIP, whose members include representatives from government and private entities involved with critical national infrastructure.

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

Education: Japan's Cybersecurity Strategy 2013 contains a detailed and comprehensive commitment to educating young people about cybersecurity.

Additional Cyberlaw Indicators: Japan 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?	✔	Japan's Cybersecurity Strategy <www.nisc.go.jp/eng> was adopted by the Japanese Government in 2013. It is a comprehensive document that includes key principles and targeted measures. It identifies and outlines the roles of the various stakeholders in Japanese cybersecurity across both the government and private sectors. In light of the passing of the Basic Law on Cybersecurity 2014 and the subsequent restructuring of Japan's cybersecurity policy and strategy bodies, as of May 2015, the Japanese government is drafting a new cybersecurity strategy <japan.kantei.go.jp/97_abe/actions/201502/10article4.html>.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The Basic Policy of Critical Information Infrastructure Protection <www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf> was released by the Information Security Policy Council (now the Cybersecurity Strategy Headquarters) in 2014. Under the Basic Law on Cybersecurity 2014, critical infrastructure companies are legally obligated to cooperate with national and local governments on cybersecurity and cyberdefense.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✔	Basic Law on Cybersecurity 2014 requires a cybersecurity basic plan to be drafted and approved by the cabinet. In addition, the Basic Law on Cybersecurity 2014 <www.nisc.go.jp/conference/seisaku/dai40/pdf/40shiryou0102.pdf> established the Cybersecurity Strategy Headquarters. The new body is responsible for coordinating cybersecurity strategy across government and the private sector.

COUNTRY: JAPAN

	QUESTION	RESPONSE	EXPLANATORY TEXT
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	Japan has enacted a new classified information law, Act 108 on the Protection of State Secrets 2013 <www.japaneselawtranslation.go.jp/law/detail/?id=2231&vm=04&re=01>, which implements stringent security practices for handling any information deemed by the Japanese Government to be a state secret. The act includes a definition for "specially designated secrets," but does not detail an inventory of systems. Additional legislation covers particular systems for classifying information. These include: • Act 120 on the National Public Service 1947 <law.e-gov.go.jp/cgi-bin/idxselect.cgi?IDX_OPT=1&H_NAME=%8d%91%89%c6%8c%f6%96%b1%88%f5%96%40&H_NAME_YOMI=%82%a0&H_NO_GENGO=H&H_NO_YEAR=&H_NO_TYPE=2&H_NO_NO=&H_FILE_NAME=S22HO120&H_RYAKU=1&H_CTG=1&H_YOMI_GUN=1&H_CTG_GUN=1>; and • Act 261 on Local Public Service 1950 <law.e-gov.go.jp/cgi-bin/idxselect.cgi?IDX_OPT=1&H_NAME=%92%6e%95%fb%8c%f6%96%b1%88%f5%96%40&H_NAME_YOMI=%82%a0&H_NO_GENGO=H&H_NO_YEAR=&H_NO_TYPE=2&H_NO_NO=&H_FILE_NAME=S25HO261&H_RYAKU=1&H_CTG=1&H_YOMI_GUN=1&H_CTG_GUN=1> and the suite of national security laws which include: • Act 165 on the Self-Defense Forces <law.e-gov.go.jp/htmldata/S29/S29SE179.html>; and • Act 166 on the Protection of Secrets Due to the Japan-US Mutual Defense Agreement.
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✔	Japan has enacted a new classified information law, Act 108 on the Protection of State Secrets 2013 <www.japaneselawtranslation.go.jp/law/detail/?id=2231&vm=04&re=01>, which implements stringent security practices on any information deemed by the Japanese government to be a state secret. For information to be deemed a "specially designated secret," as per the definition in the act, its unintended disclosure must be of a risk to Japan's national security interests. The act then maps detailed security practices to information thus deemed a state secret. Additional security practices are required by the following acts: • Act 120 on the National Public Service 1947 <law.e-gov.go.jp/cgi-bin/idxselect.cgi?IDX_OPT=1&H_NAME=%8d%91%89%c6%8c%f6%96%b1%88%f5%96%40&H_NAME_YOMI=%82%a0&H_NO_GENGO=H&H_NO_YEAR=&H_NO_TYPE=2&H_NO_NO=&H_FILE_NAME=S22HO120&H_RYAKU=1&H_CTG=1&H_YOMI_GUN=1&H_CTG_GUN=1>; and • Act 261 on Local Public Service 1950 <law.e-gov.go.jp/cgi-bin/idxselect.cgi?IDX_OPT=1&H_NAME=%92%6e%95%fb%8c%f6%96%b1%88%f5%96%40&H_NAME_YOMI=%82%a0&H_NO_GENGO=H&H_NO_YEAR=&H_NO_TYPE=2&H_NO_NO=&H_FILE_NAME=S25HO261&H_RYAKU=1&H_CTG=1&H_YOMI_GUN=1&H_CTG_GUN=1> and the suite of national security laws which include: • Act 165 on the Self-Defense Forces <law.e-gov.go.jp/htmldata/S29/S29SE179.html>; and • Act 166 on the Protection of Secrets Due to the Japan-US Mutual Defense Agreement.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation or policy in place in Japan that requires an annual cybersecurity audit. Pursuant to Article 25 of the Basic Law on Cybersecurity 2014, a review and audit of Japan's cybersecurity will be carried out.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	No	There is no legislation or policy in place in Japan that requires a public report on cybersecurity capacity. Japan's Cybersecurity Strategy <www.nisc.go.jp/eng> contains an assessment of the country's cybersecurity capacity as of 2013 and requires annuals plans from 2013 on the implementation of the strategy's goals — however, they are not strictly reports on cybersecurity capacity, nor is there a requirement for them to be made public.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	◑	While Japan has chief information officers appointed to various ministries, as well as a senior government chief information officer, there is no legislation or policy that requires each government agency to have a chief information officer or chief security officer.

COUNTRY: JAPAN

	QUESTION	RESPONSE	EXPLANATORY TEXT
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	◑	Article 30 of the Basic Law on Cybersecurity 2014 requires each head of agency submit relevant information and materials in timely manner so that Cybersecurity Strategy Headquarters can conduct its affairs assigned by the Basic Law. Since the Cybersecurity Strategy Headquarters is responsible for the evaluation of cybersecurity measures and investigation of cause with regard to serious cybersecurity incidents at national agencies, each government agency is legally obliged to provide such information.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	Both the Basic Law on Cybersecurity 2014 and the Basic Policy of Critical Information Infrastructure Protection 2014 <www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf> include an appropriate definition for "critical infrastructure protection".
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	Japan's Cybersecurity Strategy <www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf> includes a commitment to revise the "Groups of Standards for Information Security Measures for Central Government Computer Systems" to promote international cooperation, including international standardization and sharing of best practices. Specifically, the Strategy states that government procurement should include certification. "within the scope of approved in international agreements for the conditions of government procurement including utilization of conformity assessment systems based on international standards and application of required measures for assuring national security in the Agreement on Government Procurement."
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	JPCERT Coordination Center (JPCERT/CC) <www.jpcert.or.jp> was established in 1996. It is responsible for early warning systems and coordinating incident response for administrators and users of Japanese networks.
2.	What year was the computer emergency response team (CERT) established?	1996	
3.	Is there a national competent authority for network and information security (NIS)?	✔	Japan has three authorities with responsibility for network and information security: • The Cybersecurity Strategy Headquarters is a cabinet-level group of senior government figures who are responsible for formulating Japan's cybersecurity strategy, and coordinating overall government cybersecurity policy. In doing so, it works closely with the National Security Council and the IT Strategy Headquarters. The group first sat in February 2015, and will be part of a review and drafting of a new cybersecurity strategy in 2015 <japan.kantei.go.jp/97_abe/actions/201502/10article4.html>. • The National Information Security Centre (NISC) <www.nisc.go.jp>, sitting within the cabinet secretariat, is the executing command post for information security policy. Its functions cover the planning and coordination of the information security strategy. The Basic Law on Cybersecurity2014 <www.nisc.go.jp/conference/seisaku/dai40/pdf/40shiryou0102.pdf> requires that the NISC be reorganized into a dedicated cybersecurity center with expanded functions. This reorganization process commenced in January 2015. Additionally, the Information-Technology Promotion Agency (IPA) <www.ipa.go.jp> is a government agency dedicated to the development of information technology (IT) policy and the promotion of Japan's IT sector. It engages with cybersecurity issues in the course of its duties, including organizing and participating in the Cybersecurity Information Sharing Partnership of Japan (J-CSIP) <www.ipa.go.jp/security/J-CSIP>, Japan's dedicated public-private partnership for the protection of critical infrastructure against cybersecurity incidents.
4.	Is there an incident-reporting platform for collecting cybersecurity incident data?	✔	JPCERT Coordination Center (JPCERT/CC) <www.jpcert.or.jp> is tasked with collecting information about cybersecurity incidents. It has a fax and email-based reporting structure to log cybersecurity incidents. JPCERT/CC regularly publishes the information gathered by this reporting process in various forms, including studies, technical notes, and press releases. In addition, the National Information Security Centre (NISC) <www.nisc.go.jp> is responsible for incident data collection within government.
5.	Are national cybersecurity exercises conducted?	✔	Japan conducted a cyber exercise in March 2014, specifically in preparation for the 2020 Tokyo Olympic games. It involved all relevant ministries and the national police agency, and was the first such exercise to be conducted by Japan.

COUNTRY: JAPAN

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	◑	There is no clear high-level national incident management structure for responding to cyber incidents in Japan, however there are teams engaged in the event of a cyber incident. These are the: • Cyber Incident Mobile Assistant Team (CYMAT), which provides technical support and advice to prevent further damage and aid recovery, and the • Government Security Operations Coordination (GSOC) team, which analyses the incident and shares the findings with relevant government departments and agencies. The roles of the two agencies are outlines in Japan's Cybersecurity Strategy <www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf>. The strategy highlights the need for these teams, as well as relevant CERTs, to better collaborate and for a system to be established that ensures the sharing of incident information between these teams, government institutions and entities engaged with critical infrastructure. A special process is followed in the event of a cyber-attack carried out as part of an armed attack, in which case the Ministry of Defense <www.mod.go.jp> and the Self-Defense Forces are tasked response and handling.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership (PPP) for cybersecurity?	✔	The Cybersecurity Information Sharing Partnership of Japan (J-CSIP) <www.ipa.go.jp/security/J-CSIP> is a defined public-private partnership for cybersecurity, organized by the Ministry of Economy Trade and Industry (METI) <www.meti.go.jp> and the Information-Technology Promotion Agency (IPA) <www.ipa.go.jp>. Members include companies and industry organizations that are engaged with critical infrastructure. J-CSIP's focus is to provide a continuous information sharing platform as well to provide network-wide responses to cybersecurity incidents that affect critical infrastructure. J-CISP publishes regular reports on its activities.
2.	Is industry organized (i.e., business or industry cybersecurity councils)?	✔	The Japan Network Security Association (JNSA) <www.jnsa.org> is an association of companies whose goal is to promote network security standardization and contribute raising public awareness of network security issues. Their membership includes both Japanese and international companies working in Japan.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	✔	Japan has a defined public-private partnership for cybersecurity in place. Japan's Cybersecurity Strategy <www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf> adopts a "New Public-Private Partnership Model" which is a framework that identifies the different sectors who would be involved in any new cybersecurity partnership.
	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 Japan that addresses cybersecurity.
2.	Have sector-specific security priorities been defined?	✖	As of May 2015, sector-specific security priorities have not been publicly defined, nor has there been a proposal to define sector-specific security priorities in legislation or policy.
3.	Have any sector cybersecurity risk assessments been conducted?	✖	Sector cybersecurity risk assessments have not been conducted in Japan.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	Japan's Cybersecurity Strategy 2013 <www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf> contains a detailed and comprehensive commitment to educating young people about cybersecurity. It states: "It is necessary to plan awareness raising activities starting from the elementary and middle school education stages, and implement participatory awareness raising projects such as motto and poster contests. At the elementary and middle school education stages, depending upon the development stages of the student children, learning activities have be enhanced so that computers and information communications networks and other information tools can be used for instruction in each subject, positive promotion has be carried out for education on information morals, including information security. Hereafter, practical measures united with the utilization of information communication technologies in various fields of education, such as use of digital textbooks for students and education on software programming, will be promoted."

COUNTRY: JAPAN

	QUESTION	RESPONSE	EXPLANATORY TEXT
	ADDITIONAL CYBERLAW INDICATORS		
1.	Are cybersecurity services able to operate free from laws that discriminate based on the nationality of the vendor?	✔	Japan 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. No preferences are granted to domestic suppliers.
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 requirements in legislation or policy that require servers to be located in Japan.
6.	Are cybersecurity services able to operate free from unnecessary restrictions on cross-border data flows (such as registration requirements)?	✔	There are no requirements for registration for overseas transfer of data. However, a range of rules apply to data transfers to both domestic and global third party service providers, including a requirement to supervise sub-contractors when data is transferred to a third party.