BSA | The Software Alliance

# COUNTRY: **CHINA**

**Legal Foundations:** China does not currently have a national cybersecurity strategy in place, although several government policies include advice on cybersecurity. There is no one specific law that focuses on cybersecurity in China, but there are many provisions under different laws that cover cybersecurity, such as the State Secrets Law 2010.

**Operational Entities:** China's national CERT, CNCERT/CC. was established in 2002. National information security is handled by a range of different government bodies and there is sometimes very little public information about their operations and objectives.

**Public-Private Partnerships:** There is little activity regarding public-private partnerships in China in the field of cybersecurity.

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

**Education:** There is no national cybersecurity education strategy in place in China, but some ad hoc education initiatives have been undertaken by the CERT and the Ministry of Industry and Information Technology.

**Additional Cyberlaw Indicators:** China imposes a range of legal and policy restrictions on cybersecurity service providers.

| | QUESTION | RESPONSE | EXPLANATORY TEXT |
|---|---|---|---|
| | **LEGAL FOUNDATIONS** | | |
| 1. | Is there a national cybersecurity strategy in place? | ◑ | China does not currently have a national cybersecurity strategy in place.<br>The Chinese government has issued two decisions on information security, one in 2003 and another in 2012 <politics.gmw.cn/2012-07/17/content_4571519.htm>. Both highlight areas of concern and areas of focus for the government and issue advice on matters of security.<br>In addition to this, cybersecurity was featured as an important element of a draft national security law, released in May 2015 <reuters.com/article/2015/05/08/us-china-security-idUSKBN0NT0E620150508?feedType=RSS&feedName=technologyNews>. |
| 2. | What year was the national cybersecurity strategy adopted? | – | |
| 3. | Is there a critical infrastructure protection (CIP) strategy or plan in place? | ✔ | The Regulations on Classified Protection of Information Security, commonly referred to as the Multi-Level Protection Scheme, function as China's critical information infrastructure policy. |
| 4. | Is there legislation/policy that requires the establishment of a written information security plan? | ✖ | There is no legislation or policy in place in China that requires the establishment of a written information security plan.<br>Information security documents have been published at the discretion of the Chinese executive and other relevant bodies. |
| 5. | Is there legislation/policy that requires an inventory of "systems" and the classification of data? | ✔ | The Law on the Protection of State Secrets 2010 <lawinfochina.com/display.aspx?lib=law&id=1191> requires information that, if disclosed, could endanger China's national interests of being classified. Such information is assigned a classification level based on a three-tiered classification system, which represents the level of harm that unauthorized disclosure of the information would cause. |
| 6. | Is there legislation/policy that requires security practices/requirements to be mapped to risk levels? | ✔ | The security practices and requirements for classified information is outlined in the Law on the Protection of State Secrets 2010 <lawinfochina.com/display.aspx?lib=law&id=1191>. Certain practices are mapped to the classification level assigned to the information, and these levels are assigned according to the level of harm unauthorized disclosure of the information would cause.<br>A suite of laws covering personal information also have basic security requirements — however, these are not mapped to particular risk levels. |

## COUNTRY: CHINA

| | QUESTION | RESPONSE | EXPLANATORY TEXT |
|---|---|---|---|
| 7. | Is there legislation/policy that requires (at least) an annual cybersecurity audit? | ✖ | There is no legislation or policy in place in China that requires an annual cybersecurity audit.<br>The Ministry for Public Security <www.mps.gov.cn> is responsible for the operation of cybersecurity measures, however its monitoring and review processes are not publicly available. |
| 8. | Is there legislation/policy that requires a public report on cybersecurity capacity for the government? | ◑ | There is no legislation or policy in place in China that requires a public report on cybersecurity capacity for the government.<br>The National Computer Network Emergency Response Technical Team/Coordination Center of China (CNERT/CC) <www.cert.org.cn> does release periodic public reports on information security vulnerabilities and China's capabilities in responding to cyber threats. The most recent report is China's Internet Security Report 2013 <www.cert.org.cn/publish/main/46/2014/20140603151551324380013/20140603151551324380013_.html>. |
| 9. | Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)? | ✖ | There is no legislation or policy in place in China that requires 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 place in China that requires mandatory reporting of cybersecurity incidents.<br>The National Computer Network Emergency Response Technical Team/Coordination Center of China (CNERT/CC) <www.cert.org.cn> is tasked with providing a reporting platform for the government sector, as well as private entities and individuals. |
| 11. | Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)? | ✖ | While China publicly recognizes the role of critical infrastructure protection in its information security decisions <politics.gmw.cn/2012-07/17/content_4571519.htm>, there is no publicly available legislation or policy in place in China that includes a clear 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? | ✖ | China imposes a range of onerous local certification and accreditation requirements that are in addition to (and often inconsistent with) international cybersecurity standards and general ICT standards. The Chinese government regularly publishes lists of approved products for cybersecurity, including encryption products, anti-virus software, and even basic operating systems. These lists exclude some organizations and products that have met international standards. China also imposes local testing requirements for telecommunications and ICT products that include cybersecurity products. |
| | **OPERATIONAL ENTITIES** | | |
| 1. | Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)? | ✔ | The National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) <www.cert.org.cn> was established in 2002. It is tasked with incident protection and the coordination of incident response procedures across all internet systems, critical information systems, and industry control systems in China. |
| 2. | What year was the computer emergency response team (CERT) established? | 2002 | |
| 3. | Is there a national competent authority for network and information security (NIS)? | ◑ | The responsibility for network and information security in China is spread across different government departments, agencies, and working groups, the operational status of which is often unclear.<br>The Ministry for Public Security <www.mps.gov.cn> and the Ministry of Industry and Information Technology <www.miit.gov.cn> notionally share the responsibility of cyber and network security and critical infrastructure protection. In addition, the People's Liberation Army carries out operational measures related to cybersecurity, including engaging with the civilian sphere.<br>The National Administration for the Protection of State Secrets (State Secrets Bureau), a government agency, and the Central Committee for the Protection of State Secrets, an organization of the Communist Party of China, are both responsible for the protection of classified information in China.<br>Chinese state intelligence agencies and high-level working groups also act in developing and implementing information and network security policies, however details of their roles and functions are not publicly available. |

COUNTRY: CHINA

| QUESTION | RESPONSE | EXPLANATORY TEXT |
|---|---|---|
| 4. Is there an incident-reporting platform for collecting cybersecurity incident data? | ✔ | The National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) <www.cert.org.cn> is responsible for the collection of incident data and provides an online reporting platform for handling incident reporting. |
| 5. Are national cybersecurity exercises conducted? | ✔ | China has conducted several cyber exercises, mainly involving the People's Liberation Army in a mock-cyberwarfare scenario. |
| 6. Is there a national incident management structure (NIMS) for responding to cybersecurity incidents? | ✖ | There is no clear national incident management structure to respond to cybersecurity incidents. |
| **PUBLIC-PRIVATE PARTNERSHIPS** | | |
| 1. Is there a defined public-private partnership (PPP) for cybersecurity? | ✖ | China does not have a defined public-private partnership for cybersecurity.<br>The China Software Industry Association (CSIA) <www.csia.org.cn> is a representative agency for Chinese software organizations and professionals. The agency is registered by the Ministry of Civil Affairs <www.mca.gov.cn> and has been nominated directly by the Chinese government as a beneficiary of the Chinese government's support of the software industry. The nature of the relationship between member organizations of CSIA and representatives from the government is not one that reflects a typical public-private partnership. |
| 2. Is industry organized (i.e., business or industry cybersecurity councils)? | ◑ | There is no industry-led platform dedicated to cybersecurity issues in China.<br>The China Software Industry Association (CSIA) <www.csia.org.cn> is a representative agency for Chinese software organizations and professionals. The agency is registered by the Ministry of Civil Affairs <www.mca.gov.cn> and has been nominated directly by the Chinese government as a beneficiary of the Chinese government's support of the software industry, however CSIA acts as an independent agency. CSIA engages with aspects of cybersecurity as they relate to the software industry in the course of its duties.<br>Furthermore, the China Association for Science and Technology (CAST) <english.cast.org.cn>, a non-governmental organization of scientific and technological workers in China, may engage with aspects of cybersecurity in the course of its duties. |
| 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 China. |
| **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 China 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-specific security priorities in legislation or policy, as of May 2015. |
| 3. Have any sector cybersecurity risk assessments been conducted? | ✖ | Sector cybersecurity risk assessments have not been conducted in China. |
| **EDUCATION** | | |
| 1. Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age? | ◑ | There is no national cybersecurity education strategy in place in China.<br>Some ad hoc education initiatives have been undertaken by the CERT and the Ministry of Industry and Information Technology (MIIT). For example, in 2013 the Ministry released a plan to 'Prevent and Combat the Hacker Underground Supply Chain' which included an objective of educating the public regarding internet safety and ethics <www.miit.gov.cn/n11293472/n11293832/n12843926/n13917072/15567197.html>. |

COUNTRY: CHINA

| | 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? | ✖ | China is an observer, but not a full member, of the WTO plurilateral Agreement on Government Procurement.<br>Under Article 10 of the Law on Government Procurement 2003, goods may only be purchased from foreigners under exceptional circumstances — although, in practice, procurement from foreign suppliers appears to occur routinely for some products. The law does not cover purchasing by state-owned enterprises.<br>ICT security products in information systems classified at level three and above in the Multi-Level Protection of Information Security (MLPS) are required to undergo a national information assurance certification, and the product developers and manufacturers must be invested or owned by Chinese citizens or local companies.<br>Requirements for local ownership are particularly onerous in the field of encryption, which is subject to the Regulation on Commercial Encryption Codes by the Office of State Commercial Cryptography Administration (OSCCA) <www.oscca.gov.cn>. In 2014 the European Union concluded:<br>"In practice today, only Chinese or Chinese-owned companies are eligible for OSCCA certification to sell, produce and to carry out R&D for encryption technology in China, as well as to gain product licensing, and foreign or foreign-owned companies, even if based in China, are excluded." [European Union Trade Directorate, IT Security — Chinese licensing practices and approaches to information deviating from the international standards and global practices, February 2014, <madb.europa.eu/madb/barriers_details.htm?barrier_id=085196&version=4>] |
| 2. | Are cybersecurity services able to operate free from laws or policies that mandate the use of specific technologies? | ◑ | China procurement opportunities in both the public and private sectors will often include a requirement for products to be subject to China Compulsory Certification (CCC). While this scheme is supposed to deliver a generic level of quality assurance, in practice it leads to a small number of specific ICT security technologies and products being selected from the CCC Catalogue.<br>Local software certification requirements are also imposed by the China Information Security Certification Center (ISCCC) <www.isccc.gov.cn/zxjs/zxjs>. |
| 3. | Are cybersecurity services able to operate free from additional local testing requirements that go beyond international testing requirements? | ✖ | Expensive and burdensome local testing requirements are in place in China for ICT security services and products that concern information categorized as level 3 or higher in the Multi-Level Protection of Information Security (MLPS). In addition, the OSCCA <www.oscca.gov.cn> certification process requires all conformity assessments to be undertaken by Chinese government-accredited test laboratories. |
| 4. | Are cybersecurity services able to operate free from laws or policies that mandate the submission of source code or other proprietary information? | ✖ | China's Administrative Measures for the Multi-Level Protection of Information Security establish mandatory requirements that include the provision of source code for some ICT security services, including encryption services. |
| 5. | Are cybersecurity services able to operate free from laws or policies that require service providers to locate their servers inside the subject country? | ◑ | Some cybersecurity services are likely to be caught by specific (often regional) Chinese requirements to establish joint ventures with local firms in order to provide their services within China. China's control over internet access points and their censorship/firewall regime may also present practical challenges for organizations providing services without establishing a data center or mirror sites and services in China. |
| 6. | Are cybersecurity services able to operate free from unnecessary restrictions on cross-border data flows (such as registration requirements)? | ◑ | There are no mandatory registration requirements or other unnecessary restrictions on cross-border data flows in China.<br>However, many Chinese government agencies and companies follow the voluntary standards issued by the Standardisation Administration and the General Administration of Quality Supervision, Inspection, and Quarantine. These standards prohibit overseas transfers of data to an entity without the express consent of users, unless specific government permission or explicit legal or regulatory permission has been obtained. The result is that a de facto restriction applies to most cross-border data transfers in China. |