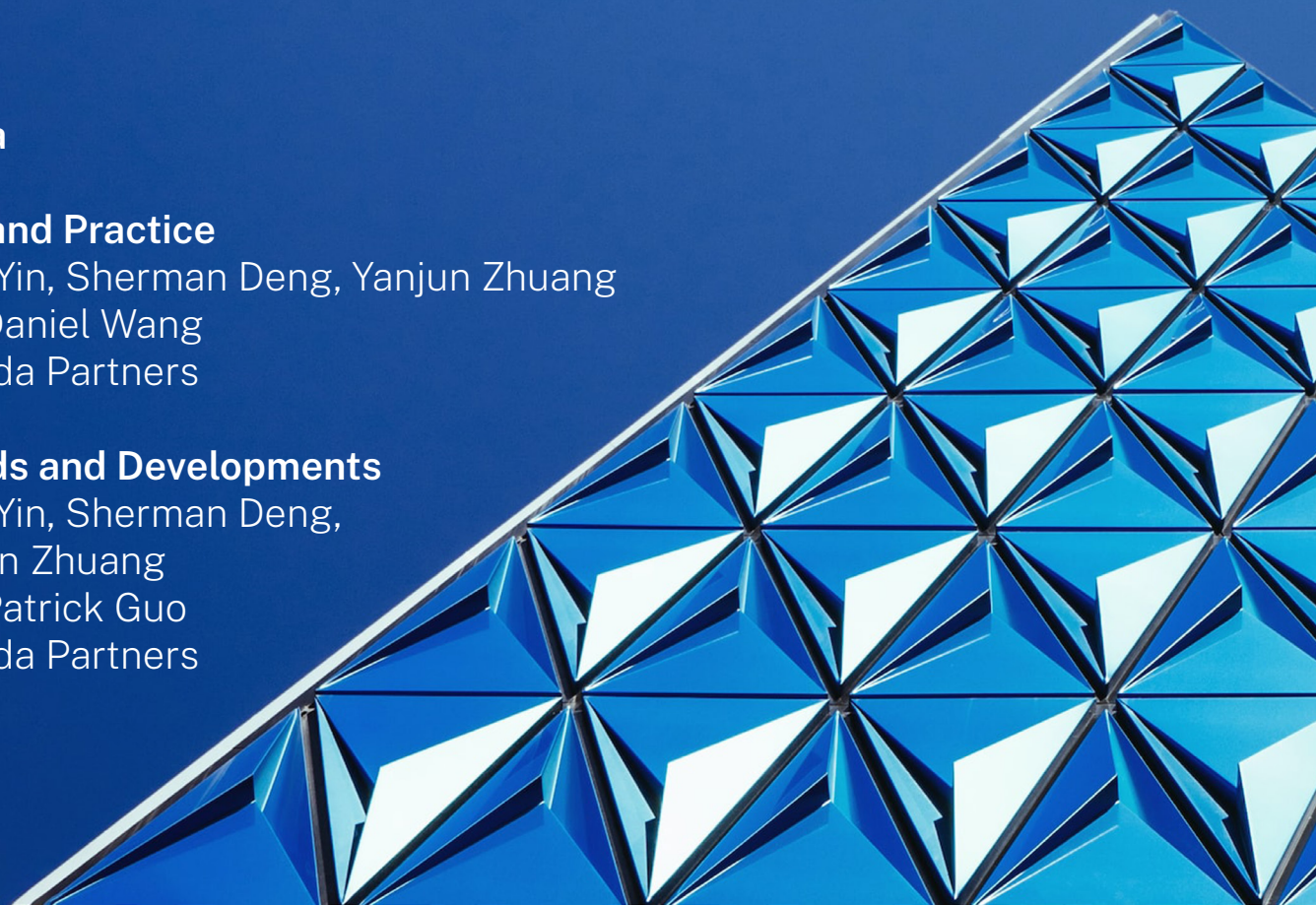
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers



China

Law and Practice
Kate Yin, Sherman Deng, Yanjun Zhuang and Daniel Wang
Fangda Partners

Trends and Developments
Kate Yin, Sherman Deng, Yanjun Zhuang and Patrick Guo
Fangda Partners

CHINA

Law and Practice

Contributed by:
Kate Yin, Sherman Deng, Yanjun Zhuang and Daniel Wang
Fangda Partners

Contents

Fangda Partners (FD) was founded in 1993 and stands as a pre-eminent, full-service law firm focused on the Greater China market, with its expertise in local regulatory frameworks highly recognised by both clients and regulators. FD has a team of over 800 lawyers across seven offices in Beijing, Guangzhou, Hong Kong, Nanjing, Shanghai, Shenzhen and Singapore. It has long been the adviser of choice for numerous clients seeking sophisticated counsel on complex legal matters. When embarking on major transactions, a multitude of leading Chinese and global enterprises, as well as financial institutions, engage its services to obtain expert advice and tailored solutions for their most intricate, challenging legal issues. Over the past three decades, FD has remained at the forefront of commercial legal services. It has successfully assisted clients in executing a host of landmark transactions and cases and secured favourable outcomes in a wide array of groundbreaking, complex and precedent-setting disputes.

Authors

Kate Yin is a recognised leader in compliance and government enforcement, boasting extensive experience in complex multi-jurisdictional and multi-agency cases, and successfully helping clients reduce or avoid penalties. Prior to joining Fangda Partners, she spent a decade in the US. founded Ropes & Gray's Asia compliance team, and is a Chambers Asia-Pacific Leading Lawyer. She has advised numerous multinational and domestic enterprises in responding to law enforcement actions by US, Chinese, and other overseas governments, conducting internal investigations that resulted in clients being exempted from penalties and recovering substantial losses.

Sherman Deng practises in the field of data privacy and cybersecurity compliance, representing both domestic and multinational clients in bank finance, tourism, internet, manufacture industries on data governance, incident response and cross-border data transfer matters. Before joining Fangda Partners, Mr Deng was a VP and senior counsel of Marriott International. In his seven years at the company, Mr Deng handled several high-profile data and cybersecurity incidents. He played a leadership role in implementing the company's cybersecurity-related compliance playbooks and policies, incident response plans, advising internal clients on MLPS, data localisation and cross-border data transfer projects, and setting up cross-functional cybersecurity teams.

Yanjun Zhuang has extensive experience in criminal defence and government enforcement, as well as in anti-fraud internal investigations for both multinational companies and domestic Chinese companies. Mr Zhuang has served clients in a broad range of industries, such as life sciences, TMT, manufacturing, real estate, automobile and finance. He excels in uncovering sophisticated fraud schemes and recovering millions of dollars for clients in criminal and civil matters and investigations. Before joining Fangda, Mr Zhuang worked for 15 years in the procuratorial department.

Daniel Wang is highly experienced in criminal defence, criminal reporting and representation, law enforcement response, internal investigations and integrated resolution for civil and commercial disputes. Dr Wang has provided legal services to numerous well-known domestic and international businesses and government agencies in cases involving white collar crimes, financial crimes, infringement of corporate rights, crime of infringing upon trade secrets, crimes disrupting the market economy, and crimes against personal and property rights. He excels in identifying and mitigating criminal risks in complex cross-border transactions, ensuring the smooth execution of commercial investment.

Fangda Partners

24/F, HKRI Centre Two
HKRI Taikoo Hui
288 Shi Men Yi Road
Shanghai 200041
China

Tel: +8621 2208 1166
Fax: +8621 5298 5599
Email: email@fangdalaw.com
Web: www.fangdalaw.com

FANGDA PARTNERS
方達律師事務所

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

China's cybersecurity regulation strategy is anchored in a state-led model that treats cybersecurity as a foundational element of national security and economic governance. A key recent development is that the amendment to the Cybersecurity Law (CSL, in Chinese 网络安全法), was adopted on 28 October 2025 and the new law came into force on 1 January 2026. The revision reinforces legal liability and enhances coordination with the broader data and cybersecurity law framework. For details, see **1.2 Cybersecurity Laws**.

Building on this strategy, China's legislative framework pursues three core, hierarchical purposes:

- safeguarding cybersecurity to uphold cyberspace sovereignty, national security and public interest;
- protecting the legitimate rights and interests of citizens, legal persons and other organisations; and
- advancing informatisation and the digital economy.

To achieve these objectives, China's cybersecurity framework sets out multiple regulatory priorities. In practice, enhanced obligations are imposed on critical information infrastructure (CII) (Note: although the name is CII, the substance is similar to critical infrastructure in other jurisdictions) and important data (which refers to data involving specific fields, groups, regions or meeting certain accuracy and scale requirements that could directly jeopardise national security, economic operation, social stability, and public health and safety if compromised, with specific scopes catalogued by respective industry regulators), supported by China's Multi-Level Protection Scheme (MLPS).

The framework also emphasises prevention and resilience, which are guaranteed through requirements for monitoring, early warning and incident response. Within this regulatory approach, the Data Security Law (DSL, in Chinese 数据安全法), promulgated on 10 June 2021 and effective from 1 September 2021, treats data as a strategic and economic resource subject to risk-based regulation, while the Personal Information Protection Law (PIPL, in Chinese 个人信息保护法), promulgated on 20 August 2021 and effective from 1 November 2021, focuses on safeguarding individual rights in personal information processing.

1.2 Cybersecurity Laws

China's cybersecurity regime is structured around a combination of general legislation, sector-specialised laws and regulations, and national and industry standards.

The overarching structure at the top is known as "Three laws plus two regulations", as summarised below:

The "Three Laws"

At the general level, the CSL applies to the construction, operation, maintenance and use of a network, as well as the supervision and administration of cybersecurity within the territory of China (note: Hong Kong Special Administrative Region, Macau Special Administrative Region and Taiwan China are separate juris-

dictions from mainland China where Chinese cybersecurity laws do not apply. For the purpose of this article only, China refers to mainland China), and sets out stringent requirements for the protection of network information and the security of network operations. The recent amendment to the CSL significantly increases the severity of penalties for network operators and CII operators (CIIOs) that breach cybersecurity obligations, reflecting a strengthened enforcement framework. The revised CSL explicitly supports the research on artificial intelligence and R&D of key technologies such as algorithms, advances construction of infrastructure such as training data resources and computing power, improves ethical norms for artificial intelligence, and strengthens risk monitoring, assessment and security supervision.

The DSL applies to any individual or organisation engaged in data processing activities in China. These activities include collecting, storing, processing, using, providing, trading, and publicly disclosing data, whether conducted online or offline. The DSL also has extraterritorial application effect – ie, if any data processing activities carried out outside of the territory of China harms the national security, public interests, or legitimate rights and interests of citizens or organisations of China, legal liability shall be investigated in accordance with the DSL.

At a general level, the DSL imposes comprehensive data safeguarding obligations on data handlers (which are, conceptually, similar to data controllers under GDPR) encompassing organisational governance and technical safeguards, including the establishment of internal data security management mechanisms, the provision of security awareness training, the implementation of data classification and grading, and the conduct of periodic data security risk assessments.

The PIPL applies to any activity of processing of personal information of a natural person that is carried out within China. The PIPL also has clear extraterritorial application effect – ie, it applies to any data processing activities carried on outside of China if it covers the personal information of a natural person in China and the purpose is to provide a product or service to that natural person, or to analyse or assess the behaviour of that natural person. The PIPL establishes principles for personal information processing such as transparency, fairness, purpose limitation, data minimisation, limited retention, accuracy and accountability. While many provisions echo the EU's GDPR, including fines of up to 5% of prior-year revenue for serious breaches, the PIPL differs in the sense that consent is the default lawful basis for data processing activities, and it does not recognise the "legitimate interest" lawful basis widely used in EU.

The "Two Regulations"

The Regulation on Network Data Security Management ("Network Data Management Regulation", in Chinese 网络数据安全管理条例), promulgated by China's State Council on 30 September 2024 and effective from 1 January 2025, sets out detailed obligations for data handlers in China, with a particular focus on the protection of important data, for instance, regularly conducting network data security risk monitoring, risk assessments and emergency drills. The regulation also restates requirements for security assessments of cross-border data transfer (CBDTs) that were set out in previous rules and clarifies the responsibilities of internet platform service providers, specifying the obligations of third-party service and product providers. As an implementing regulation of the CSL, DSL and PIPL, the Network Data Management Regulation has a substantially unified scope of application, applying to network data processing activities and related security supervision conducted within the territory of China, and, where applicable, extending extraterritorially to overseas activities that process personal information of individuals located within China or that harm China's national security, public interests or the lawful rights and interests of its citizens or organisations.

The other regulation is known as the Regulation on Protecting the Security of Critical Information Infrastructure ("CIIO Regulation", in Chinese 关键信息基础设施安全保护条例). Compared to the Network Data Management Regulation which applies to all data handlers, the scope of application for the CIIO is much narrower, as it applies only to CIIOs. It sets out detailed obligations for any CIIO, including risk assessment, security management, incident response and reporting requirements.

In addition to the "three laws plus two regulations", there are other cross-sector regulations and rules with "dense" or "spotty" cybersecurity requirements. For example, the MLPS requirements were updated in 2025 through the Notice on Further Strengthening Cybersecurity Tiered-Protection Work (Gongwang'an [2025] No 1001) on 8 March 2025, and the Notice on Further Specifying Matters Related to Cybersecurity Tiered-Protection Work (Gongwang'an [2025] No 1846) on 27 April 2025. The updated basic requirements specify data inventory survey, MLPS filing, identification and handling of potential risks and vulnerabilities and formulation of a protection workplan and corresponding filing.

There are also sectoral rules applicable to specific industries. For example, the Administrative Measures on Data Security for Banking and Insurance Institutions (effective from 27 December 2024) and the Administrative Measures on Data Security in the Business Scope of the People's Bank of China (effective from 30 June 2025) provide the relevant requirements on cybersecurity specifically applicable in the financial services sector.

To complement these laws and regulations, a series of national and industry standards, including those applicable in the financial services sector, have been promulgated. For example, Data Security Technology-Guidelines on Social Responsibility for Data Security and Personal Information Protection (GB/T 46071-2025), Data Security Technology-Security Certification Requirements for Cross-Border Processing of Personal Information (GB/T 46068-2025), Financial Data Security-Data Lifecycle Security Specification (JR/T 0223-2021), Financial Data Security-Data Security Classification and Grading Guidelines (JR/T 0197-2020) and Technical Specifications for Personal Financial Information Protection (JR/T 0171-2020). Even though such national and industry standards are in general not mandatory, they are a good reference point to companies when implementing the requirements under the various laws and regulations.

1.3 Cybersecurity Regulators

In China, the enforcement of cybersecurity-related laws is jointly undertaken by multiple competent authorities with overlapping powers.

The Cyberspace Administration of China (CAC) is primarily the regulatory authority responsible for formulating cybersecurity and data protection rules, co-ordinating network data security and building awareness with the general public. CAC is also in charge of law enforcement, but it usually takes a "soft" approach to this, for example, informal inquiries, invitation for a private talk, onsite inspections and orders for rectification of breaches of the regulations. Occasionally, CAC may also launch an investigation and hand out penalties. The cybersecurity division of the Public Security Bureau (PSB) or "cyber police" is the law enforcement agency responsible for enforcing cybersecurity laws and regulations, conducting inspections and ensuring that businesses comply with local data protection requirements. It has broad enforcement powers to inspect and monitor internet service providers and other businesses processing personal information. It also has the power to detain bad actors if any criminal activities are suspected.

The Ministry of Industry and Information Technology (MIIT) supervises data security in the IT, industrial and telecommunications sectors. It enforces filing requirements and classification standards, conducts inspections and imposes penalties.

The State Administration for Market Regulation oversees data security in market activities and investigates unfair competition and consumer rights violations. These authorities co-ordinate to form a comprehensive supervision and incident response system, ensuring effective law enforcement.

Moreover, the National Data Bureau (NDB), which is under the administration of National Development and Reform Commission, was officially established on 25 October 2023. The NDB is tasked with advancing the development of basic data institutions, co-ordinating the integration, sharing, development and application of data resources, as well as promoting the planning and construction of a Digital China, the digital economy and a digital society.

In specific industries, sectoral regulators are also responsible for data security management. For example, in the financial services sector, such regulators mainly include the National Financial Regulatory

Administration (NFRA), regulating banks and insurance companies, the People's Bank of China (PBOC) regulating banks and payment agencies, and China Securities Regulatory Commission (CSRC), regulating security brokers and mutual funds. They have formulated appropriate sectoral rules on cybersecurity and data protection, such as the Administrative Measures on Data Security in the Business Scope of the People's Bank of China, the Administrative Measures on Data Security for Banking and Insurance Institutions, and the Measures for the Administration of Cybersecurity and Information Security in the Securities and Futures Industry.

2. Critical Infrastructure Cybersecurity Regulation

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

In China, the framework of CII is primarily built upon a hierarchical structure of the CSL, CIIO Regulation and related national standards.

The CSL stipulates operational security responsibilities and network information security responsibilities regarding CII. The CIIO Regulation stipulates the identification for CII, the responsibilities of the CIIO, and how state organs safeguard and promote the operation of CII.

According to Article 33 of the CSL, CII refers to the important network facilities and information systems in important industries and fields such as public telecommunications, information services, energy, transportation, water conservancy, finance, public services, e-government and national defence science, technology and industry, as well as other important network facilities and information systems which, in case of destruction, loss of function or leak of data, may result in serious damage to national security, the national economy, people's livelihood and public interests. Legal entities that operate CIIs are CIIOs. Articles 8 and 10 of the CIIO Regulations further clarify that the specific identification of CII is not self-assessed by the operators but is designated by the Protection Authorities.

National standards include: the Information Security Technology – Guide to Security Inspection and Evaluation of Critical Information Infrastructure; the Information Security Technology – Indicator System of Critical Information Infrastructure Security Assurance; and the Information Security Technology – Cybersecurity Requirements for Critical Information Infrastructure Protection.

2.2 Critical Infrastructure Cybersecurity Requirements

Articles 23 and 27 of the CSL set the "floor" of cybersecurity requirements for all network operators, including implementing the MLPS and formulating contingency plans for cybersecurity incidents, as well as responsibilities related to network information security, such as log retention and audit, and the installation of firewalls, anti-virus software and intrusion detection systems.

For CIIOs, on top of the "floor" requirements, they must fulfill the following "stretched" cybersecurity obligations, as detailed below:

- implement the following enhanced safeguarding obligations compared with network operators other than the CIIO:
  - (a) setting up a dedicated security management body and appointing a person in charge of security management;
  - (b) conducting regular cybersecurity education, technical training and skills assessment for employees;
  - (c) performing disaster recovery backups for important systems and databases; and
  - (d) formulating contingency plans for cybersecurity incidents and conducting regular drills. (Note: the stretched cybersecurity requirements described above were originally imposed only on CIIOs under the CSL. However, subsequent legislation, including the DSL and the PIPL, has broadened the scope of regulated entities to include network operators acting as data handlers);
- when procuring network products and services, sign security and confidentiality agreements with providers, for the purpose of safeguarding important data against vulnerabilities;

- store personal information and important data within the territory of China, and where it is strictly necessary to provide such data overseas due to business needs, complete a security assessment, as required; and
- conduct an inspection and assessment of the security of their networks and potential risks at least once a year and report the assessment outcome and any rectification measures to the relevant departments responsible for the security protection of CII.

2.3 Incident Response and Notification Obligations

CAC issued the Administrative Measures for the Reporting of National Cybersecurity Incidents ("Cybersecurity Incident Reporting Measures", in Chinese 国家网络安全事件报告管理办法) that provide the harmonised rules and guidance for cybersecurity incident reporting. The Cybersecurity Incident Reporting Measures came into force on 1 November 2025. Under the Measures, network operators operating in China shall report cybersecurity incidents that are classified as "Relatively Severe or above".

According to the appendix of the Cybersecurity Incident Reporting Measures, the Cybersecurity Incident Classification Guidelines ("Classification Guidelines", in Chinese 网络安全事件分级指南), cybersecurity incidents are categorised from low to high as: "General", "Relatively Severe", "Severe" and "Significantly Severe". The Classification Guidelines specify different thresholds for key entities, including CIIOs, government agencies and other network operators, to assess the level of severity of their cybersecurity incidents. Typically, if a CII experiences either a total outage lasting not less than ten minutes or a disruption of its primary functions lasting not less than 30 minutes, it will be constituted as "Relatively Severe". From a practical perspective, most companies including CIIOs should focus on the core assessment criteria – ie, the volume of impacted individuals. The bulk thresholds for the three levels of incident categories are relatively straightforward – ie, one million for Relatively Severe, 10 million for Severe and 100 million for Significantly Severe. China takes a broad-based approach (similar to GDPR) instead of a narrow-based one (for example, CCPA) when it comes to data breach notice-and-report. The covered data compromised under a data breach that triggers notice-and-report is not limited to personally identifiable information but any personal information. Also, if a cybersecurity incident concerns the breach of national core data or important data under Chinese laws, regardless of volume, such incident will reach "Relatively Severe or Above". (Note: "national core data" refers to the most critical category of data under the data classification and grading regime, characterised by relatively high coverage of specific fields, groups or regions, or meeting the thresholds of high accuracy, large scale and a certain depth of information, the illegal use or sharing of which may directly jeopardise political security).

Upon the detection of an incident, CIIOs must immediately report it to the CII protection department (ie, the sectoral regulator with oversight responsibilities on the CII. For example, in case of a telecom carrier, it will be MIIT) and PSB within one hour, and other network operators shall immediately report it to local CAC within four hours.

The following information shall be included in a cybersecurity incident report to be submitted to the CAC:

- basic information – organisation name, responsible personnel, contact details;
- incident description – basic information about the affected systems or facilities, time, location, type and level of the cybersecurity incident, as well as the impacts and harms already caused, the measures taken, and their effectiveness; in the case of a ransomware attack, the report shall also include the ransom amount demanded, the payment method and the deadline; and
- further assessment of cybersecurity incidents – how the incident has developed and the potential further impacts and harms, leads for tracing and investigation, root cause analysis, planned further response measures and requests for support, status of preservation of the incident scene, and so on. For further assessment, network operators may submit additional information in the form of supplementary reports within 72 hours following the initial report. In addition, network operators are required to submit a summary report on the cybersecurity incident handling within 30 days after the comple-

tion of cybersecurity incident handling through the original reporting channel.

With respect to reporting channels, CAC has established multiple channels for receiving cybersecurity incident reports, including a dedicated cybersecurity incident reporting hotline (12387), an online reporting platform, email (12387@cert.org.cn), facsimile (010-82992387), the "12387" WeChat Mini Programme, and the official WeChat public account of the National Computer Network Emergency Response Technical Team/Coordination Center (CNCERT).

Notably, reporting an incident to CAC does not mean an organisation is exempt from reporting it to other relevant authorities who may have a need to know. In particular, where a cybersecurity incident is suspected to involve potential criminal offences, the operator must also promptly report the incident to the PSB as enforcement lead; and where there are specific industry requirements, the operator shall also report to the competent sectoral regulators. For example, under the Measures for the Administration of the Reporting of Cybersecurity Incidents in the Business Fields of the PBOC, upon the occurrence of a cybersecurity incident at or above the Relatively Severe level, financial institutions subject to the PBOC supervision shall submit a brief report within one hour and then a detailed report within 24 hours, and within ten working days of the incident disposition, submit a post-incident investigation and summary report. Further, for Severe and above-level incidents, financial institutions shall submit progress reports every two hours until the incident is resolved.

In addition to reporting the cybersecurity incident to competent authorities, network operators are also required to notify the affected individuals of the incident. Such notification may be exempted if the network operator concerned can demonstrate that it has adopted effective measures to prevent or mitigate the resulting harm. Having said that, if competent authorities believe that the harm may not be prevented or mitigated otherwise, they may still require the network operator concerned to notify the individual.

2.4 State Responsibilities and Obligations

The CSL and DSL comprehensively prescribe state obligations.

Under the CSL, the state is responsible for formulating the cybersecurity strategy, clarifying basic requirements and major objectives, and establishing a cybersecurity protection system to enhance protection capabilities. The state shall adopt measures to monitor, defend against and handle cybersecurity risks and threats, with particular focus on safeguarding CIIs.

Under the DSL, the state shall establish a data security governance system and integrate data security into the national security outlook. Specifically, it stipulates the establishment of a data classification and grading protection system, as well as a data security review system to conduct national security reviews of data processing activities that affect national security.

Regarding threat intelligence sharing, the CSL mandates state supervision and administration of network information security, and the establishment of a cybersecurity monitoring, early warning and information notification system. It also supports co-operation between network operators and requires the standardised release of cybersecurity-related information. Under the DSL, the state shall establish a data security emergency response process.

As for public-private co-operation, the CSL stipulates that the state shall support enterprises and educational institutions in conducting cybersecurity-related education and training, cultivate talent, and encourage enterprises to offer cybersecurity certification, testing and risk assessment services as part of procedural safe harbours. The DSL encourages relevant entities to formulate data security codes of conduct and group standards to guide their members in fulfilling data protection obligations.

3. Operational Resilience in the Financial Sector

3.1 Scope of Financial Sector Operational Resilience Regulation

Unlike the EU's Digital Operational Resilience Act (DORA) or the USA's Sound Practices to Strengthen Operational Resilience, China's framework adopts a layered, sector-specific approach. Its regulatory scope is defined by a combination of general cybersecurity and data security laws and industry-specific rules, which together establish the overarching compliance requirements for regulated financial institutions.

At the general level, cybersecurity and data security legislation applies to all financial institutions as network operators and data handlers. Because certain core financial systems may be designated as CIIs and their operators CIIOs, they are subject to enhanced obligations under the CIIO Regulation. These rules establish baseline requirements for risk monitoring, incident response, emergency handling and recovery capabilities.

At the sectoral level, sectoral rules refine operational resilience obligations across multiple dimensions. In terms of the data security regulations, there are the Measures for the Data Security Management of Banking and Insurance Institutions ("NFRA DSL", in Chinese 银行保险机构数据安全管理办法) and the Measures for the Administration of Data Security in the Business Fields of the People's Bank of China ("PBOC DSL", in Chinese 中国人民银行业务领域数据安全管理办法) focusing on data security risk monitoring, disposal and lifecycle management. As for IT outsourcing supervision, the Measures for the Supervision of Information Technology Outsourcing Risks of Banking and Insurance Institutions ("IT Outsourcing Risk Management Measures", in Chinese 银行保险机构信息科技外包风险监管办法) specifically regulate the information technology outsourcing risks of banking and insurance institutions, including subcontracting management and exit mechanisms. With respect to core business continuity, the Measures for the Administration of Emergency Response Financial Services of Banking and Insurance Institutions clarify requirements for emergency drills and disaster recovery support to ensure continuous financial services during incidents.

China's operational resilience-related rules do not establish a standalone, compliance-based extraterritorial regime comparable to DORA. However, Article 77 of the CSL explicitly recognises extraterritorial jurisdiction where overseas entities engage in activities that endanger China's cybersecurity, thereby producing functional extraterritorial effects for relevant foreign service providers.

3.2 ICT Service Provider Contractual Requirements

In the financial services sector, there is no special distinction for those who provide information and communication technology (ICT) or other third-party IT services. They are collectively known as "information technology outsourcing", which means that a banking or insurance institution engages service providers to conduct IT activities that would be otherwise undertaken by itself, including the entrusted processing of data. These outsourcings are subject to restrictions due to third-party risks associated with outsourcing.

Under Article 37 and 38 of the CSL, where ICT and other third-party service providers supply network products or services to CIIOs, they are required to cooperate with the applicable national security review if such products or services are critical to the operation of the CII, and to comply with statutory confidentiality and data security obligations. These security review and confidentiality requirements should be clearly stipulated in the vendor contracts.

In the financial services sector, according to Articles 6 and 7 of the IT Outsourcing Risk Management Measures, banking and insurance institutions are required to establish an IT outsourcing governance structure and decision-making/approval procedures (at the board and senior management levels) to ensure effective oversight and accountability. According to Article 21 of the IT Outsourcing Risk Management Measures, IT outsourcing contracts are required to include clauses covering: scope of service, regulatory compliance, service continuity, audit and supervisory rights of financial institutions, cybersecurity and data protection, incident reporting mechanisms, and dispute resolution, among others, and, to the extent a foreign vendor is engaged, the vendor contract should have Chinese law as governing law and Chinese dispute

resolution settlement institutions for dispute resolution. Furthermore, for the purpose of safeguarding service continuity in the event of termination of outsourcing arrangements, Article 14 of the IT Outsourcing Risk Management Measures requires banking and insurance institutions to put in place exit strategies and contingency arrangements.

Under Article 28 and Article 46 of PBOC DSL, where data processing is entrusted to third parties, the trustee's data security obligations must be clearly defined, enhanced due diligence is required before entrusting third parties to process important or core data, and the trustee should refrain from transferring any data restricted by PBOC from outsourcing to a third party.

Overall, legal restrictions for ICT and other third-party providers are "spotty" and scattered around different regulations.

It is worth noting that ICT service providers that service the government or state-owned enterprises (such as state-owned banks), will be subject to a *Xinchuang* (ie, trust and innovation) programme, which is essentially a localisation programme where only government-approved local ICT vendors can participate. The programme also calls for gradual phase-out and sometimes rip-and-replace of critical components in the IT system if they are sourced from outside of China or if the service provider is otherwise not on the *Xinchuang* list.

3.3 Key Operational Resilience Obligations

Under the CSL, financial institutions must comply with the MLPS and establish a sound operational resilience management system. Core obligations focus on establishing internal security management systems, designating cybersecurity-responsible persons, deploying technical measures to guard against cyber threats, implementing network monitoring and log retention for no less than six months, and carrying out data classification, backup and encryption. For CIIOs, additional obligations involve establishing specific security management institutions, providing cybersecurity training for employees, conducting security background checks on key personnel, setting up disaster recovery backups for critical systems and databases, developing cybersecurity incident response plans with regular drills and performing annual risk assessments.

The Measures for the Administration of the Reporting of Cybersecurity Incidents in the Business Fields of the PBOC further refine these requirements, such as clarifying emergency disposal responsibilities and requiring professional data security personnel and annual training. For incident reporting, financial institutions must submit: brief reports within one hour and detailed reports within 24 hours for Relatively Severe or above-level incidents; and progress reports every two hours for Severe or above-level incidents until disposal, with a post-incident summary within ten working days.

Under the Measures for the Reporting, Investigation and Handling of Cybersecurity Incidents in the Securities and Futures Industry, securities and futures institutions are required to promptly report any network or information system failures that may constitute cybersecurity incidents, irrespective of the incident classification level. Where an incident is assessed as potentially "Significantly Severe" or "Severe", institutions must provide ongoing progress updates at intervals of no less than every 30 minutes until normal system operations are fully restored, whereas for Relatively Severe or general incidents, continuous reporting is not required after the initial report unless material developments arise.

3.4 Operational Resilience Enforcement

In China, cybersecurity obligations applicable to critical ICT services providers are enforced under the CSL, under which providers may be subject to regulatory rectification orders, warnings and monetary penalties when they fail to timely address security defects or vulnerabilities, discontinue required security maintenance, or inadequately respond to cybersecurity incidents. Where a provider refuses to rectify or causes consequences endangering cybersecurity, administrative fines ranging from CNY50,000 to CNY500,000 may be imposed, together with personal fines of CNY10,000 to CNY100,000 on directly responsible personnel.

Regarding enforcement targeting critical ICT service providers, in 2024, the WIND system, a leading

financial terminal developed by a critical ICT service providers, suffered a service disruption that could have prevented financial institutions from accessing market data and analytical information in a timely manner, thereby undermining their trading decision-making and risk management practices. This incident exposed critical deficiencies on the part of the vendor, including an inadequate monitoring and detection mechanism, a poorly designed file backup and recovery plan, and weak network operation and management capabilities. For these failings, the vendor was issued a cautionary letter by the CSRC.

Additionally, regulators have issued a substantial number of enforcement actions against financial sector operators for failures to fulfill cybersecurity and data security obligations, including deficiencies in network security management, data security controls, customer identity verification and incident response. Such cases typically involve penalties imposed on both institutions and responsible individuals, with enforcement measures including warnings and fines ranging from several thousand yuan renminbi to several million yuan renminbi.

3.5 International Data Transfers

With respect to China's CBDT processes, relevant obligations currently focus primarily on personal information and important data. Under the current PRC regulatory framework, CBDT is primarily governed by three processes: CAC security assessment, standard contract filing (SCC Filing) and personal information protection certification. The Provisions on Promoting and Regulating Cross-Border Data Flows issued by CAC on 22 March 2024, introduced clear exemptions and bulk thresholds for these processes. Specifically, data handlers (other than CIIOs) are exempted from any CBDT process where they cumulatively transfer less than 100,000 individuals' non-sensitive personal information overseas within a calendar year, or where the transfer is necessary for specific business or public interest scenarios, including contractual necessity in cross-border transactions, lawful cross-border human resources management, or emergency situations to protect individuals' vital interests.

By contrast, data handlers must complete a security assessment with the CAC if they transfer data overseas and meet any of the following conditions/bulk thresholds:

- CIIOs transfer personal information or important data abroad; or
- non-CIIO data handlers transfer important data overseas, or have cumulatively transferred personal information of over one million individuals (excluding sensitive personal information) or sensitive personal information of over 10,000 individuals overseas since January 1 of the current year.

Regarding the identification of important data, if the data handler has not received a notification from relevant departments or regional government that the data is important data or that the data is designated as important data under rules and regulations, data handlers are not required to declare it as important data for the purpose of a security assessment. Transfers falling below the security assessment thresholds but above the exemption thresholds may be conducted through either SCC Filing or personal information protection certification.

In 2025, relevant competent authorities jointly issued the Guidelines on Promoting and Regulating Compliance in Cross-border Data Flows in the Financial Sector (the "Financial Data Cross-border Transfer Guidelines", in Chinese 促进和规范金融业数据跨境流动合规指南), which aim to clarify and facilitate cross-border data transfers in the financial services sector in coordination with existing data protection and cybersecurity rules. Please note that the Guidelines were issued privately to financial institutions and have not been made public. According to the Financial Data Cross-Border Transfer Guidelines, financial institutions may independently transfer data stored within China overseas without undergoing any regulatory procedures, provided that such data does not include personal information and important data under Chinese laws. For certain business scenarios providing personal financial services, financial institutions may transfer specific types of client data overseas without going through any of the three CBDT processes, if the transfer falls within the prescribed circumstances and data categories listed in Appendix I of the Financial Data Cross-Border Transfer Guidelines. For other financial business scenarios (including corporate

banking) or internal management activities, financial institutions are still required to follow one of the applicable CBDT processes. However, if the transfer falls within the specific scenarios and data categories of certain data subjects listed in Appendix II of the Financial Data Cross-Border Transfer Guidelines, regulators generally acknowledge the necessity of such transfers, meaning that the approval or filing process is expected to be smoother and more efficient. For example, for tax filing purposes under the compliance and internal control scenario, the cross-border transfer of corporate clients' name, internal ID, country/region, nationality, document issuing authority, document validity period, partially masked address, birth date, document type or contact details, are generally recognised as necessary.

3.6 Threat-Led Penetration Testing

China has not established a unified regime equivalent to the Threat-Led Penetration Testing (TLPT) frameworks adopted in the EU and USA; moreover, in certain scenarios, TLPT is expressly restricted. In particular, pursuant to Article 31 of the CIIO Regulation, active vulnerability scanning and penetration testing against CII are, in principle, prohibited unless prior approval or authorisation is obtained from competent authorities. Instead, a functionally comparable set of requirements has evolved out of China's financial regulatory and cybersecurity governance system, which collectively form a closed-loop mechanism covering threat detection, defensive controls, incident response, continuous testing and simulation exercises.

- Under Article 23 of the CSL and Article 5 of the NFRA DSL, financial institutions are required to establish threat detection, risk monitoring and early-warning processes, including continuous monitoring and risk analysis for cyber and data security threats. While under sectoral administration measures, sectoral regulators require timely escalation and reporting of identified risks.
- Under Article 23 of the CSL, institutions must implement preventive and defensive security controls. This is primarily achieved through MLPS, which network operators need to focus on the major risks and vulnerabilities identified through assessments, thoroughly investigate the root causes, comprehensively analyse security protection needs, propose rectification ideas, and finally formulate a protection work plan based on actual conditions. These controls aim to prevent, detect, and mitigate cyberattacks affecting critical business systems.
- Under Article 27 of the CSL, incident response and emergency handling are set as core compliance obligations. Financial institutions must establish incident response processes, activate incident response plans upon detection of security incidents, and report material incidents to competent authorities within prescribed timelines. Response measures are expected to balance containment, service recovery, evidence preservation and stakeholder communication.
- Under Article 23 of the CSL, regulators set forth continuous monitoring as a form of long-term and normalised safeguards. Institutions are required to maintain effective security protection through ongoing monitoring processes, including log retention, system filing and record-keeping, and incident account management. For network systems classified at third-level or above under MLPS, relevant protection work plans must be filed with local PSB and sectoral regulator (if applicable) on an annual basis.

Finally, under the Measures for the Administration of Emergency Response Financial Services of Banking and Insurance Institutions and CIIO Regulation, simulation exercises and drills play a role analogous to TLPT stress scenarios. A banking or insurance institution shall conduct an emergency response plan drill at least once every three years, and those designated as CIIO shall conduct at least one cybersecurity test and risk assessment annually.

Taken together, China's approach achieves TLPT-like objectives through a layered combination of statutory duties, sectoral supervision, baseline standards and recurring exercises.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

Constituents to China's statutory framework for cyber resilience include the CSL, DSL, CIIO Regulation,

Network Data Management Regulation, Administrative Provisions on Security Vulnerabilities of Cyber Products ("Cyber Product Vulnerability Provisions", in Chinese 网络产品安全漏洞管理规定) and MLPS.

- The CSL establishes foundational obligations for network operational security and mandates baseline requirements for critical equipment access and continuous security maintenance.
- The DSL institutionalises the data classification and hierarchical protection system, requiring risk monitoring and emergency response mechanisms throughout the data lifecycle.
- The CIIO Regulation emphasises special protection for core industries, mandating simultaneous plan, establishment and use of security measures to ensure business continuity.
- The Network Data Management Regulation strengthens systemic robustness obligations for large-scale platforms and defines mandatory notice-and-report procedures for cyberattacks and supply chain disruptions.
- The Cyber Product Vulnerability Provisions mandate a two-day reporting window for vulnerabilities, establishing a closed-loop response resilience process from discovery to patching.
- The MLPS provides cross-sector technical benchmarks, requiring tiered defence and recovery capability building for cloud, IoT, and mobile architectures.

Regarding the scope of application, connected devices (IoT) are subject to specialised technical assessments focusing on the physical and perception layers; meanwhile, SaaS and cloud services must undergo cloud computing security evaluations to ensure multi-tenant isolation and business continuity. Furthermore, for digital services, the Network Data Management Regulation imposes heightened obligations on large-scale platform operators concerning systemic robustness and supply chain due diligence, reinforced by administrative sanctions calculated as a percentage of the entity's global annual turnover.

4.2 Key Obligations Under Legislation

According to the specific provisions of the CSL and Cyber Product Vulnerability Provisions, network operators are strictly responsible for vulnerability management and formulating emergency plans for cybersecurity incidents and conducting activities such as cybersecurity certification, testing and risk assessment.

Under Articles 27 and 28 of the CSL, upon discovering risks such as security defects or vulnerabilities in network products or services, network operators shall immediately take remedial measures, notify users in a timely manner, and report to the competent authorities. The Cyber Product Vulnerability Provisions further stipulate that network operators shall establish and improve channels for receiving information on network product security vulnerabilities and keep such channels open, and after discovering the vulnerability, report it to the cybersecurity threat and vulnerability information-sharing platform of MIIT within two days.

Regarding post-market surveillance of products, Article 24 of the CSL explicitly stipulates that providers of network products and services should provide continuous security maintenance for their products and services, and shall not terminate the provision of security maintenance within the prescribed period or the period agreed upon by the parties. The Network Data Management Regulation requires that when a network data security incident occurs, network data handlers shall activate incident response plans, take measures to prevent the expansion of harm, and report to competent authorities.

As for conformity assessment, marking and certifications, the CSL explicitly stipulates that equipment and products listed in the "Catalog of Critical Network Equipment and Specialized Cybersecurity Products" can only be sold or provided after being certified as qualified by a qualified institution or meeting the requirements of security testing. The CIIO Regulation stipulates that if the procurement of network products and services by CIIO may affect national security, it shall undergo a national security review organised by CAC in conjunction with relevant departments of the State Council. The DSL mentions that the state promotes the development of services such as data security testing, assessment and certification.

In terms of product recall or withdrawal duties, the CSL stipulates that if critical network equipment and

specialised cybersecurity products are sold or provided without security certification or security testing, or if the security certification is unqualified or the security testing does not meet the relevant requirements, the competent authority has the right to order the suspension of sales and confiscate illegal gains.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

The primary cybersecurity certification framework in China is the MLPS, which has been further developed and clarified by the Notice on Further Strengthening Cybersecurity Tiered Protection Work (Gongwang'an [2025] No 1001) and the Notice on Further Specifying Matters Related to Cybersecurity Tiered Protection Work (Gongwang'an [2025] No 1846) in 2025. The current regime mandates a comprehensive and dynamic update of system filings between 8 March and 30 November 2025, applicable to all information systems classified at second-level or above. A significant expansion in this iteration is the integration of data governance into the certification process and operators are now legally required to complete a data survey questionnaire as part of the filing to map data assets and cross-border flows, thereby linking cybersecurity directly with data security obligations.

The framework classifies systems into five levels based on their relative importance to national security and social order. Fifth-level systems, defined as those where a breach would cause particularly serious harm to national security, represent the highest assurance level and are subject to stringent oversight by provincial-level PSB. The certification assessment standards have shifted from static compliance to dynamic defence under the new Cybersecurity Level Evaluation Report Template (2025 Edition). A critical "Severe Risk Veto" process has been introduced: a system can only be deemed "Compliant" if it achieves a score of over 90% and contains no major risks or vulnerabilities. Conversely, systems with major risks cannot achieve full compliance status regardless of their numerical score, compelling operators to prioritise the rectification of substantive security gaps over paper compliance.

Furthermore, the certification process now requires the formulation of a protection work plan for systems at third-level and above. Operators must submit these plans, detailing asset conditions, rectification strategies and future security schedules, to both PSB and sectoral regulators annually. For the current cycle, the initial batch of work plans must be submitted by 30 June 2025. This certification is not only a regulatory requirement but effectively serves as a market access licence; failure to obtain MLPS certification can preclude entities from public procurement opportunities and sector-specific licensing in critical industries such as finance and energy.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

Under the PIPL, personal information handlers are required to take measures to ensure that their processing activities comply with laws and administrative regulations based on the purpose and means of processing, the categories of personal information to be processed, the impact on personal rights and interests, and the potential security risks. This compliance framework shall prevent unauthorised access to, as well as breach, tampering, or loss of any personal information. Specifically, handlers shall formulate an internal management system and operational procedures, implement classified management of personal information, adopt corresponding security technical measures such as encryption and de-identification, and reasonably determine the operational authority for processing.

For a handler that processes personal information of over one million individuals, it shall designate a person in charge of personal information protection to supervise the processing activities and complete the corresponding filing obligations with CAC. This person is known as PIPO, equivalent to DPO under GDPR.

To ensure proactive risk management, for processing activities that may have significant impacts on individuals, handlers shall conduct a personal information

protection impact assessment and keep the assessment report and records of processing for at least three years. Such processing activities mainly include processing sensitive personal information, using personal information to conduct automated decision-making, entrusting personal information processing to a third party, providing personal information to another handler, publicly disclosing personal information and transferring personal information overseas.

Regarding incident response, under Article 57 of the PIPL, where the breach, tampering or loss of personal information occurs or may occur, a handler shall immediately take remedial measures and notify the cyberspace administration department and relevant individuals. The notice shall include the types of personal information involved, the reason and possible harm, the remedial measures adopted and the contact information of the handler. While the handler is not required to notify individuals if the measures taken can effectively avoid harm, the cyberspace administration department has the authority to request the handler to notify individuals if they consider that harm may have materialised. For specific breach-notification obligations, including notification thresholds, timelines and required content, see **2.3 Incident Response and Notification Obligations**.

For a handler that provides important internet platform services involving a huge number of users and complicated business types, Article 58 of the PIPL establishes heightened obligations. These handlers shall establish and maintain a compliance system, set up an independent organisation mainly composed of external members to supervise protection efforts, formulate platform rules following the principles of openness, fairness and justice to clarify norms for providers within the platform, stop providing services to providers that seriously violate laws, and regularly publish social responsibility reports for public supervision.

6.2 Cybersecurity and AI

The cybersecurity landscape for AI in China operates under a layered framework where specific AI legislation functions as a specialised extension of the CSL, DSL and PIPL. A pivotal development is the 2025 Amendment to the CSL, which added a new Article 20. This article explicitly mandates that the state shall improve AI ethical norms and strengthen risk monitoring, assessment and security supervision, providing the statutory bedrock for the entire AI governance regime. Under this framework, AI service providers face strict "security-by-design" and supply chain obligations. Providers shall ensure the legality of foundation models and training data used in pre-training and optimisation, strictly utilising data from lawful sources that do not infringe on intellectual property rights. Furthermore, where data annotation is involved, providers should establish clear labelling rules and conduct accuracy verification to ensure the authenticity and objectivity of the data.

Chinese regulations impose different filing requirements on traditional AI algorithms and generative AI ("Gen AI") services. Under the Provisions on the Administration of Algorithm-Generated Recommendations for Internet Information Services, traditional AI algorithms, such as search and deep synthesis algorithms, are subject to the algorithm filing with the CAC (the "Algorithm Filing"). Separately, pursuant to the Interim Measures for the Administration of Generative Artificial Intelligence Services, providers of Gen AI services are subject to a filing requirement with the competent local CAC (the "Gen AI Filing").

Accordingly, for Gen AI products, the filing requirement follows a "dual filing" process. Specifically, traditional AI components are subject to the Algorithm Filing, while the Gen AI component is subject to the Gen AI Filing. By contrast, traditional AI products that do not involve generative functionalities are only required to complete the Algorithm Filing.

Beyond the above filing obligations, providers are also obligated to establish comprehensive management systems, including algorithmic mechanism reviews and technological ethics reviews, to regularly verify the security of models and data to prevent the generation of illegal content.

Regarding incident reporting, the statutory obligations are rigorous and quantifiable. Providers shall immediately suspend the generation of illegal content and take corrective measures such as model retraining. In practice, the Guidelines for Security Incident Emergency Response of Generative Artificial Intelligence

Services issued by the National Technical Committee 260 on Cybersecurity of SAC operationalise this. The guidelines classify incidents into information content, data security and network attack events. A critical threshold for immediate reporting to authorities includes scenarios where third-level (Severe) incidents occur cumulatively five times within 24 hours and affect over 10,000 users. Finally, it is crucial to note that these specific AI regulations interact directly with general laws; violations of AI-specific duties will trigger the severe penalty mechanisms prescribed in the CSL, DSL and PIPL, including potential business suspension or criminal liability.

6.3 Cybersecurity in the Healthcare Sector

Pursuant to the Administrative Measures for Cybersecurity of Medical and Health Institutions issued by the National Health Commission, healthcare institutions are mandated to establish a comprehensive cybersecurity governance structure where the institution assumes the primary responsibility. This includes, among others, the formation of a cybersecurity leadership group and strict adherence to the MLPS. Notably, for any newly constructed networks (including electronic health record systems), the security protection level shall be determined during the planning and declaration phase. Systems classified at third-level or above are subject to MLPS assessment at least once annually, while second-level systems processing personal information of over 100,000 individuals shall undergo assessment at least every three years.

In terms of procurement and supply chain security, healthcare institutions shall execute written agreements with IT contractors and medical device manufacturers, explicitly defining cybersecurity obligations and liability for any breach. A strict "security-by-design" and lifecycle management approach is required for medical devices, covering tendering, procurement, installation, maintenance and final disposal. A unique sector-specific requirement mandates that for all new informatisation projects, the budget allocated specifically for cybersecurity shall not be less than 5% of the total project budget.

Regarding data protection and incident reporting, under Articles 20 and 21, institutions shall conduct an annual inventory of data assets and establish a classification system based on the potential harm of a breach. An annual data security risk assessment is also mandatory. Data generated shall primarily be stored within China; cross-border transfers require a security assessment or review in accordance with relevant laws. In the event of a personal information leak or significant cybersecurity incident, the institution is obligated to immediately activate emergency plans, take remedial measures, and notify the affected individuals via telephone, SMS or mail, and report the incident to the supervisory authorities.

Trends and Developments

Contributed by:
Kate Yin, Sherman Deng, Yanjun Zhuang and Patrick Guo
Fangda Partners

Fangda Partners (FD) was founded in 1993 and stands as a pre-eminent, full-service law firm focused on the Greater China market, with its expertise in local regulatory frameworks highly recognised by both clients and regulators. FD has a team of over 800 lawyers across seven offices in Beijing, Guangzhou, Hong Kong, Nanjing, Shanghai, Shenzhen and Singapore. It has long been the adviser of choice for numerous clients seeking sophisticated counsel on complex legal matters. When embarking on major transactions, a multitude of leading Chinese and global enterprises, as well as financial institutions, engage its services to obtain expert advice and tailored solutions for their most intricate, challenging legal issues. Over the past three decades, FD has remained at the forefront of commercial legal services. It has successfully assisted clients in executing a host of landmark transactions and cases and secured favourable outcomes in a wide array of groundbreaking, complex and precedent-setting disputes.

Authors

Kate Yin is a recognised leader in compliance and government enforcement, boasting extensive experience in complex multi-jurisdictional and multi-agency cases, and successfully helping clients reduce or avoid penalties. Prior to joining Fangda Partners, she spent a decade in the US. founded Ropes & Gray's Asia compliance team, and is a Chambers Asia-Pacific Leading Lawyer. She has advised numerous multinational and domestic enterprises in responding to law enforcement actions by US, Chinese, and other overseas governments, conducting internal investigations that resulted in clients being exempted from penalties and recovering substantial losses.

Sherman Deng practises in the field of data privacy and cybersecurity compliance, representing both domestic and multinational clients in bank finance, tourism, internet, manufacture industries on data governance, incident response and cross-border data transfer matters. Before joining Fangda Partners, Mr Deng was a VP and senior counsel of Marriott International. In his seven years at the company, Mr Deng handled several high-profile data and cybersecurity incidents. He played a leadership role in implementing the company's cybersecurity-related compliance playbooks and policies, incident response plans, advising internal clients on MLPS, data localisation and cross-border data transfer projects, and setting up cross-functional cybersecurity teams.

Yanjun Zhuang has extensive experience in criminal defence and government enforcement, as well as in anti-fraud internal investigations for both multinational companies and domestic Chinese companies. Mr Zhuang has served clients in a broad range of industries, such as life sciences, TMT, manufacturing, real estate, automobile and finance. He excels in uncovering sophisticated fraud schemes and recovering millions of dollars for clients in criminal and civil matters and investigations. Before joining Fangda, Mr Zhuang worked for 15 years in the procuratorial department.

Patrick Guo has a practice at Fangda Partners, which focuses on privacy and data protection, cybersecurity, government enforcement and regulatory compliance. His clients operate in a wide range of industries and sectors such as finance, consulting, education, manufacturing, hospitality, luxury, retail, automotive, TMT, gaming, logistics, pharmaceuticals, artificial

intelligence and information technology. Mr Guo has been involved in many data protection and cybersecurity compliance projects, including establishing and implementing data protection and cybersecurity compliance systems, advising on cross-border data transfer compliance, and conducting data protection and cybersecurity compliance due diligence in IPOs and related transactions.

Fangda Partners

24/F, HKRI Centre Two, HKRI Taikoo Hui
288 Shi Men Yi Road
Shanghai 200041
China

Tel: +8621 2208 1166
Fax: +8621 2208 1166
Email: email@fangdalaw.com
Web: www.fangdalaw.com

Recap of Past Developments

At a high-level, the development of China's cybersecurity regime over the past decade can be summarised into three stages.

- Influence (2016–2021) – establishing the legal architecture through the Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL), while shaping the ecosystem via regulations, standards, name-and-shame campaigns targeting illegitimate mobile apps, pilot programmes and guidance. This stage aimed to raise public awareness of China's data sovereignty, the importance of cybersecurity and the obligations to safeguard personal information.
- Monitor (2021–2025) – building administrative procedures such as cross-border data transfer (CBDT) control (including negative lists in free trade zones (FTZs)), personal information audits, security assessments, algorithm/large-model filings, and frequent rectification campaigns (ie, requiring those in breach of regulations to put them right themselves). These measures have enabled regulators to better understand industry practices, recalibrate enforcement priorities and gather leads for supervision.
- Control (2025–) – entering a decisive enforcement phase by mandating the appointment of a personal information protection officer (PIPO), raising penalty ceilings, broadening extraterritorial reach, tightening incident reporting service level agreements and scaling sectoral inspections, while still attempting to preserve reasonable compliance burdens to allow the digital economy to function effectively.

The New Trends

2026 marks the first year of the new five-year plan of the Cyberspace Administration of China (CAC), signalling a transition in priority from monitoring to control.

The amendment to the CSL passed in October 2025 (effective 1 January 2026; amending the original 2016 law) provides the clearest signal of this shift. It materially increases penalty ceilings, introduces personal liability for "directly responsible persons" covering the PIPO, chief information security officer and other management personnel; and broadens extraterritorial

reach to overseas conduct that endangers China's cybersecurity, not just conduct harming critical information infrastructure.

At the same time, regulators continue to calibrate rules around CBDT and AI governance to maintain commercial activity. The CAC's 2025 Q&A on CBDT and FTZ negative lists confirms that ordinary data and limited personal information can flow freely while the exports of "important data" and sensitive personal information or bulk personal information remain gated by transfer mechanisms.

Theme for 2026: Enforcement will intensify, but the operative question remains "what is reasonable cybersecurity?" Regulators balance national security, crime prevention, personal information protection, economic development and technology growth when enforcing the law. Companies that can demonstrate proportionate technical and organisational controls, including permits, certifications, audits and structured processes, will have stronger affirmative defences in enforcement actions.

The remainder of this article unpacks three enforcement vectors foreign businesses should prepare for in 2026:

- enforcement against illegal CBDT;
- data breach compliance and response; and
- AI regulation.

Enforcement against illegal CBDT

CBDT of personal information

In 2025, CAC issued multiple interpretations of the CBDT mechanisms stipulated in the PIPL, reflecting China's emphasis on data sovereignty. These interpretations can be found in its Q&As dated April, May and October 2025, respectively. Additional interpretations can be found in the guidelines issued by the FTZs and the technical standards issued by the State Administration for Market Regulation. Together, they form a comprehensive set of implementing rules on CBDT, supplementing the otherwise high-level and general provisions of CBDT mechanisms under the PIPL and other CAC regulations.

In addition, CAC established a new Data Security Division, tasked with enforcement alongside the pre-existing Cybersecurity Division and Enforcement Division. With these developments, regulatory requirements and expectations are now clearly articulated, and heightened enforcement activity can be anticipated in 2026.

A case in point is international hotels. Through a CAC Q&A dated October 2025, CAC clarified that using a central reservation system to process bookings for Chinese domestic travellers does not satisfy the "necessity" requirement for CBDT.

Other potential triggers for CBDT enforcement would include international data breaches. Typically, these involve global notice-and-report obligations of multinational company (MNC) headquarters, which cover Chinese residents, if affected. Once notifications reach Chinese residents, they often circulate the information on social media, potentially drawing regulatory attention. Regulators may then query the China operation of the MNC to investigate the breach: why Chinese residents were affected, how their data ended up in a global database, and whether proper transfer mechanisms were followed. If the local management of the China operation cannot explain, or if it turns out that the transfer mechanism was not fulfilled, for instance, filing is not complete or there is evidence of "gun jumping", regulators may initiate a formal investigation and impose penalties as a result.

CBDT of important data

In addition to the enforcement against illegal CBDT of personal information, regulators are increasingly focused on the illegal CBDT of important data. In a US context, important data is similar to controlled unclassified information. In a nutshell, it refers to regulated, non-public data relating to the government regulators, state-owned enterprises, private-public projects or critical infrastructure operators that matter to national security. For example, in the electronic vehicle sector, large-scale data concerning vehicle traffic flows and logistics that reflect the macroeconomic operation of a municipality are designated by law as important data. This is because roadway networks constitute critical infrastructure, and operational data relating to such networks may have national security implications.

The status quo for important data in China is that there is no overarching, unified catalogue for important data with sufficient granularity to allow organisations to determine with certainty whether the data they hold qualifies as important data. Instead, catalogues for important data are "spotty", appearing in negative lists issued by FTZs, sector-specific regulatory specifications, technical standards, and, in some cases, through case-by-case designation by the regulators.

CBDT of important data is subject to approval by CAC. Under the existing CAC rules, before applying for such approval, the data exporter must already have knowledge that the data in question has been classified as important data by a sector regulator or relevant regulations. Given the "spotty" nature of the important data, organisations may inadvertently transfer potential important data out of China without seeking the requisite approval.

Against the backdrop of heightened geopolitical tensions, data related to high technology with national security relevance, especially data concerning critical minerals, manufacturing supply chain chokepoints, or key components in technology supply chain is highly likely to be deemed important data, if not classified as state secrets. Any cross-border transfer of such data, unless approved by regulators or certified through a prescribed risk assessment, is likely to trigger enforcement action from CAC or other law enforcement regulators such as public security bureau or national security bureau.

In addition, Article 36 of the DSL establishes a blocking statute that prohibits the provision of any data to foreign governments or foreign courts in connection with law enforcement or judicial proceedings without prior approval from the Chinese regulators. While the specific approval regulator has not been clearly identified, existing sectoral regulations endorsed by the CAC suggest that the approval process will, at a minimum, involve one or more of the following regulators: (i) the relevant sector-regulator; (i) the Ministry of Justice; and (iii) the CAC.

Data breach compliance and response

The volume, scale, sophistication and impacts of data breaches have drastically increased over the past few years. With assistance from AI technologies, it has become significantly easier for threat actors to impersonate employees, retrieve credentials and launch successful cyberattacks. Therefore, foreign businesses operating in China must remain highly vigilant with respect to data breach and their legal implications.

Following the rollout of China's CBDT regime, most MNCs' China-based entities, acting as data handlers, have entered into the standard contractual clauses (SCCs) with their global data recipients. All of these SCCs follow a government-mandated standard template, which imposes binding data breach notice and report obligations on the overseas data recipients, to the extent that the breach involves the personal information of individuals in China covered by the SCCs.

Notice-and-report

In this context, China must be considered as a significant jurisdiction in the event of a global data breach. The Measures for the Reporting of National Cybersecurity Incidents issued by CAC in 2025 requires a network operator to notify CAC within four hours after the discovery of a "relatively severe" data breach. Although this rule remains unclear whether the same reporting timelines apply uniformly to global data breaches, the requirement warrants close attention in practice.

Where a data breach is reportable, an organisation must fulfil its notice-and-report obligations. Here, "notice" refers to notice-to-individuals, requiring the organisation to inform the breach to the impacted individuals so that they may take precautions. "Report" refers to report-to-regulator, requiring the organisation to report the breach to regulators for them to take action, including investigation and law enforcement. China follows a "harm-based" approach to breach notification. Where the organisation discovers that no actual harm has occurred, for example, there has been no data exfiltration, then notice is not mandatory. In practice, Chinese regulators may also provide guidance on notice, particularly where public notification could raise national security concerns. By contrast, a report is generally required, and as already referred to above, the reporting timeline can be as short as four hours.

Risk assessment and audit

In addition to the core notice-and-report obligations, Chinese regulators are also calling on organizations to fulfil certain procedural compliance requirements, including data inventory/data mapping, scenario-based record of processing activities (RoPA), data risk assessments and personal information compliance audit (PI Audit).

On 6 December 2025, CAC issued the Measures for Network Data Security Risk Assessment (Draft for Public Consultation) (the "Draft Measures"), establishing a unified, cross-sectoral framework for assessing risks arising from network data processing. Extending requirements previously imposed on banking and insurance institutions stipulated in the Measures for the Data Security Management of Banking and Insurance Institutions, the Draft Measures apply to all network data processing activities within China and define risk assessment as a "structured process of identifying, analysing, and evaluating data security risks". Under the proposed regulatory architecture, CAC co-ordinates nationwide assessment work, while sectoral regulators organise and implement assessments based on the principle that business operators are responsible for their own data and data security.

The Draft Measures distinguish between important data handlers and general data handlers, echoing Article 30 of the DSL and Article 33 of the Regulation on Network Data Security Management. Important data handlers must conduct annual risk assessments, while general handlers are encouraged to conduct them at least once every three years. Assessments may be performed internally by designated personnel or externally by certified third-party institutions. When engaging third-party institutions, handlers must clearly define responsibilities and confidentiality obligations. Assessment institutions must maintain independence, objectivity and professional judgement, and are accountable for the authenticity and completeness of their reports. The same institution may not conduct more than three consecutive assessments for the same handler. Reports must be retained for at least three years, and important data handlers must file the reports with competent regulators within ten working days.

The Draft Measures further introduce a trigger-based mechanism. If CAC identifies significant risks, major data security incidents, or activities that may endanger national security or public interests, it may require the engagement of certified third-party institutions. Regulators may order rectification, restrict the important data processing, or pursue liability for non-compliance. Assessment institutions themselves may be subject to corrective measures or prohibitions in case of serious misconduct.

As a matter of best practice, organisations are expected to test the effectiveness of their cybersecurity and data protection control measures, and China is no exception. Under the current regulatory framework, there is a mandatory PI audit programme requirement where large companies need to complete an audit once every two years.

In parallel to the periodic audits, the regime also contemplates special audits targeting specific processing activities, for example, the processing of minors' personal information. In particular, CAC has been actively requiring organisations that process minors' personal information to submit the results of their annual PI audits, with recent practice indicating a submission deadline of the end of January each year.

AI regulation

In parallel, the CAC is continuing to draft and roll out a new generation of rules to regulate AI.

Recap of regulatory framework

In China, AI regulations distinguish between two categories of AI: traditional AI and Generative AI ("Gen AI"). Traditional AI refers to algorithms that have automated decision-making functions for non-generative tasks, such as search, ranking or recommendation. By contrast, Gen AI refers to models that perform a generative function such as text-to-text, text-to-graph or text-to-video generation function.

Chinese regulations impose different filing requirements for traditional AI algorithms and public-facing Gen AI services.

Under the Provisions on the Administration of Algorithm-generated Recommendations for Internet

Information Services, both traditional AI and Gen AI algorithms must be filed with central CAC ("Algorithm Filing"). Separately, pursuant to the Interim Measures for the Administration of Generative Artificial Intelligence Services, providers of Gen AI services must also file with provincial CAC ("Gen AI Filing"). Accordingly, Gen AI products follow a "dual filing" requirement. Traditional AI components are subject to Algorithm Filing, while the Gen AI component requires Gen AI Filing. In comparison, purely traditional AI products without generative functionality only require Algorithm Filing.

Take the example for interpretation, if an AI product consists of three components: (i) Gen AI; (ii) search algorithm; and (iii) ranking algorithm, Algorithm Filing is required for items (ii) and (iii), while Gen AI Filing applies to item (i).

Products that rely on foreign-based SaaS services or overseas infrastructure are generally considered regulatory "vulnerability" as such services fall outside Chinese jurisdiction and often lack mandatory Chinese requirements, such as MLPS certification, "positive energy" content mechanisms, and controls to prevent prohibited or sensitive content. Consequently, CAC tends to apply a more cautious review standard in practice.

The "dual filing" essentially mandates AI developers to disclose the core aspects of public-facing AI systems, including: (i) the developer's risk management system; (ii) data protection; (iii) technical documentation; (iv) record keeping; (v) transparency and explainability; (vi) human oversight; (vii) assessments for robustness, accuracy and cybersecurity; and (viii) content moderation.

Summary of new developments

The 2026 regulatory landscape introduces high-stakes enforcement for AI. First, public-facing AI services that have not completed the required filing may be subject to enforcement sweeps by CAC, including taking these services down, particularly if the service has a large user base or generates illegal content. For example, the founder of the AI service Alien Chat is under criminal prosecution for pornographic content generated by AI.

Second, AI Companion services featuring human emulation reaching specific thresholds, such as one million registered users, are now required to undergo mandatory security assessments by CAC. App stores are also deputised to verify compliance before listing services.

For businesses operating in China, 2026 marks a shift toward integrated governance and enforceable technical standards, requiring immediate gap assessments and governance upgrades to navigate heightened supervisory scrutiny and operational requirements.

Mitigation measures

We would recommend foreign businesses operating in China establish and continuously improve a cybersecurity compliance programme to keep pace with rapid legal and technological developments.

As Sun Tsu famously said in the Art of War, "Don't work on the assumptions that your opponents will not attack, but on the assumption that they will attack but you already have a contingency plan". Given the inevitability of cybersecurity incidents and the ensuing government inspection, companies should adopt a security by default and security by design strategy, continuously enhancing their compliance programmes so that, when regulators knock on the door, affirmative defences are already in place.

At its core, the programme can be summarised as "know it, do it, test it". A company will need to know its data and assets through proactive inventory and discovery process, and align them with applicable legal requirements via data mapping and RoPA. Once mapping is complete, companies must build control points, for example, completing MLPS for key assets, dual filing for Gen AI, and setting up multi-factor authentication for admin account holders. After the control points are set up, companies also need to test these control points through assessments and audits to ensure they are effective, resilient and robust. All of these efforts, if preserved through excellent "record keeping" in the form of audit reports, management communication and training records, will serve as exculpatory evidence or credits of the company, helping to mitigate liability in the event of regulatory enforcement.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com