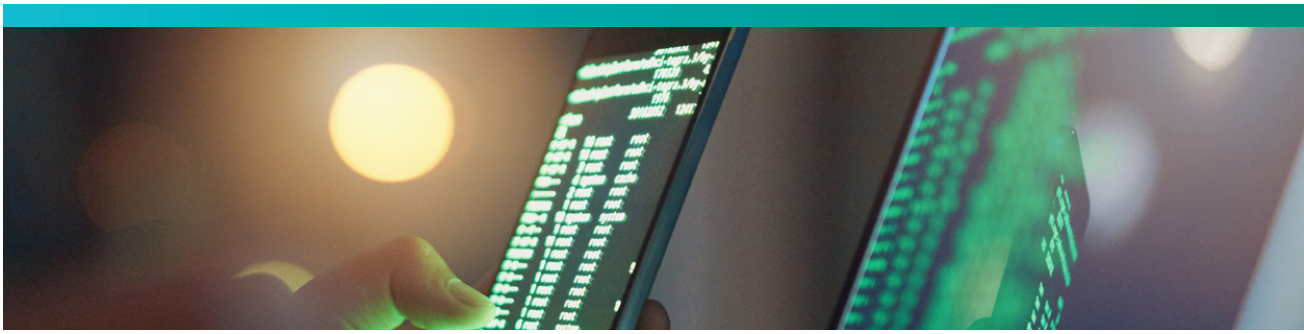
protiviti®
Face the Future with Confidence



Interpretations of the updates to China's Cyber Security Law

All companies[1] incorporated within Mainland China are required to abide by the Cybersecurity Law of The People's Republic of China (PRC), which went into effect 1 June 2017. Given the complex business relationships within the international market, the Cybersecurity Law will continue to have important political, economic, and technical implications for both domestic and multinational corporations (MNC). As updated regulations and interpretations to the Law have been released since 2017, this Point of View (POV) aims to provide further insight to the Law and expand on our July 2017 white paper, *China's Cybersecurity Law and Its Impacts: Key requirements businesses need to understand to ensure compliance.* [2]

Technically speaking, the Cybersecurity Law is an "umbrella law" that encompasses a structured suite of security and privacy laws that are enforced by official sources of law[3] . To be in compliance, companies must understand not only the Cybersecurity Law but also these supportive regulations, rules, and interpretations. This POV offers an overview of recent updates to the Law and addresses the compliance challenges that they may pose.

Overview of the Cybersecurity Law

The Cybersecurity Law integrates preexisting regulations and rules of the PRC to create a structured and statutory law addressing the following legislative objectives:

[1] As defined by the Cybersecurity Law, a company is the network operator or critical information infrastructure operator.

[2] *China's Cybersecurity Law and Its Impacts: Key requirements businesses need to understand to ensure compliance*, Protiviti, 2017: www.protiviti.com/HK-en/insights/china-cybersecurity-law-and-impacts.

[3] Retrieved 9, April 2020 from Legal Research Guide, China: www.loc.gov/law/help/legal-research-guide/china.php.

- Define the principle of cyberspace sovereignty
- Define the cybersecurity obligations of internet products and services providers
- Formulate the rules of personal information protection
- Establish a security baseline for critical information infrastructure
- Institute rules for cross-border transmission of data

The Cybersecurity Law also provides detailed articles and provisions on legal liability, prescribing a variety of penalties that include fines, certificate suspension, and revocation of permits and/or business licenses. Where criminal acts are involved, offenders will be punishable according to the Criminal Law of the People's Republic of China[4]. The Cybersecurity Law grants the Cyber Security Administrative Authorities (CSAA) with rights and guidelines to carry out legal enforcement on illegal acts.

Affected Organizations and Updated Compliance Requirements

The Cybersecurity Law expressly applies to network operators and critical information infrastructure (CII) operators within mainland China. Since the release of its updated guidelines, more details have become available regarding compliance requirements for network operators and CIIs.

"Network operator," as defined in the appendix to the Cybersecurity Law, could be applicable to almost all businesses in mainland China that own or administer their networks. The Cybersecurity Law may also be interpreted to encompass a wide set of industries apart from traditional information technology, internet service providers, and telecommunications companies. Therefore it is safe to assume that any company operating its network – including websites, as well as internal and external networks – to conduct business, provide a service, or collect data in mainland China falls within the scope of "Network operator."

Although the Cyberspace Administration of China (CAC) has yet to issue further guidance on CIIs, it has incorporated a wide range of industries, including but not limited to communications, information services, energy, transportation, utility, financial services, public services, and government services. In general, the requirements for network operators and CIIs are similar in terms of their objectives, but the requirements for CIIs are more stringent. The differences in obligations between network operators and CIIs are detailed below and organizations should take note of where they fall.

[4] For more information on the Criminal Law of the People's Republic of China, please refer to www.ceolaws.net/Info/View.Asp?id=4156

Network Operator Obligations

Article	Legal Requirements *
No. 8	The State Council departments for telecommunications, public security, and other relevant organizations are responsible for cybersecurity protection, supervision, and management efforts within the scope of their respective jurisdictions.
No. 21	Perform security protection duties according to the requirements of the cybersecurity multi-level protection schema (MLS).
No. 21, Sec. 3	Adopt technical measures for monitoring and recording network operational statuses and cybersecurity incidents, and store these network logs for at least six months.
No. 21, Sec. 4	Adopt additional measures such as data classification, backup of important data, and encryption.
No. 24	Users are required to provide real identity information when signing agreements for services. Failure to do so will result in network services being terminated or withheld.
No. 25	Network operators must develop a cybersecurity incident response plan that promptly addresses system vulnerability, computer viruses, network attack, network intrusion, and other cybersecurity risks, and report all incidents to the relevant departments.
No. 47	Strengthen the management of information published by users, immediately terminating the transmission of illegal information and preventing the spread of disinformation.

* This is not an exhaustive list

Critical Information Infrastructure Security

Article	Legal Requirements *
No. 34, Sec. 1	Set up a dedicated security management body with a designated security management leader; conduct security background checks on personnel in key positions.
No. 34, Sec. 2	Periodically conduct cybersecurity education, technical training, and skills evaluations for employees.
No. 34, Sec. 3	Conduct disaster-recovery backups of critical systems and databases.
No. 34, Sec. 4	Formulate emergency response plans for cybersecurity incidents and regularly organize drills.
No. 38	Conduct annual inspection and assessment of network security. Submit a cybersecurity report as well as proposed improvement measures to the departments responsible.

* This is not an exhaustive list

Cross-Border Data Transmission

Organizations that transmit data to overseas affiliates or headquarters must abide by data localization requirements. To avoid violation, they should either restructure their system architecture around cross-border data transfer, or conduct assessments for approval by regulatory authorities.

While Article 37 of the Cybersecurity Law originally outlined the legal requirements on cross-border data transmission for CIIs, selected requirements under this article have now been extended to network operators.

Article	Legal Requirements *
No. 37	Store all collected personal information and important data within mainland China, and prior to a cross-border data transfer, conduct a security assessment for approval by the relevant departments.

* This is not an exhaustive list

Personal Information Protection

Chapter Four of the Cybersecurity Law focuses on the protection of personal information, which is defined within the appendix as "information recorded by electronic or other means that can be used alone or in combination with other information to identify a person, including name, date of birth, identity document number, biometrics, address details or other similar personal details." With the release of updated guidelines in May 2019[5], organizations should take into account the following articles to ensure compliance with related regulations:

Article	Legal Requirements *
No. 40	Network operators must keep user information strictly confidential and maintain a private information protection system.
No. 41	Collection and usage of personal information shall be in compliance with all laws and regulations and with the user's consent, and only for purposes related to the service being provided.
No. 42	Personal information shall not be disclosed, tampered with or shared with others, and security measure should be put in place to protect personal information.
No. 49	Network operators shall establish network information security complaint and reporting policies, publicly disclose said policies and promptly handle complaints and reports relevant to network information security.

* This is not an exhaustive list

[5] China issues final guideline for Internet personal information protection, ReedSmith, May 2019: www.reedsmith.com/en/perspectives/2019/05/china-issues-final-guideline-for-internet-personal-information-protection

Compliance Challenges and Impacts

Cyber Security Law (CSL) Challenges

Given the broad scope of the law and China's growing prominence as the world's second largest economy, the Cybersecurity Law presents various challenges – not only for multinational companies operating in mainland China, but also for domestic companies looking to grow their business internationally.

AMBIGUITY

Overall, the biggest challenge of the Cybersecurity Law is its ambiguous language and general vagueness, which make it difficult for organizations to fully understand whether or not they are in compliance. This issue becomes even more pronounced as companies work towards compliance by attempting to define work scopes, initiate remediation plans, adjust corporate processes, select technical solutions, and prepare budgets.

For example, Article 37, in reference to cross-border data transfers, states that personal and other important business data produced in mainland China shall be stored within mainland China. However, neither the Cybersecurity Law nor its supportive rules and regulations actually define the criteria of cross-border data transfers, which would affect an organization's strategy for compliance, from implementing technical solutions to budget planning.

What's more, even though the Cybersecurity Law has been in effect since 2017, many of its supportive regulations and rules are still in development or draft from.

COMPLEXITY OF CHINA'S LEGAL SYSTEM

Another challenge comes from the complicated legal system and regulatory framework in mainland China. Besides judicial interpretation, the various sources of statutory law on cybersecurity create a complex environment for organizations pursuing compliance. For example, with the Basic Requirement for Multi-Layer Protection Schema of Cybersecurity coming into effect on 1 December 2019, business and IT operations now have to respond to various assessments, interviews, and remediation from different departments like legal counsel, compliance, audit, and IT security, in order to fulfil their compliance requirements.

Without providing all the details needed to comply with its broad scope of legal requirements, the Cybersecurity Law makes it necessary for organizations to navigate and understand all supportive regulations and rules. With more than 300 laws, regulations, rules and other legal documents, a great burden is put on an organization's legal counsel and compliance officers, especially since different legislative authorities, laws, regulations and rules may conflict with one another. When two laws govern the same factual situation, a law governing a specific subject matter (special laws) can override a law governing only general matters (general laws). An example of this is the cybersecurity regulation of the financial industry. The legal implications require cybersecurity personnel to have professional knowledge not only in legal affairs, but in the industry.

COST

The last, and possibly the most immediate challenge, is the cost of compliance. Costs related to compliance assessments, as well as remediation and mitigation actions after assessments, can discourage some organizations from operating in mainland China or cooperating with local business partners. Compliance, especially from a technical perspective, extends beyond the purchasing of devices and equipment or migration of systems from one place to another. There is a great deal of time and effort involved in its maintenance, not to mention resources needed to implement new procedures and systems to meet compliance requirements. All these add to the burden of cost for organizations wishing to operate in mainland China, and for some companies, this is simply not affordable. Officers in charge of Cybersecurity Law compliance inevitably face challenges in balancing compliance with business operations, especially with regards to budget.

Cybersecurity Law and its impact

Even before the Cybersecurity Law was enacted, legal requirements related to cybersecurity have already had an impact on companies operating in mainland China, especially within the IT and cybersecurity industry.

One such impact is the increased prevalence of companies and individuals claiming to be security specialists. On the one hand, the recent growth of the IT and cybersecurity industry as a whole has led to the emergence of specialized companies, new products, and subject matter experts, bringing more choices and support for achieving compliance with the Cybersecurity Law. On the other, organizations need to be vigilant and properly vet these new service providers, ensuring that they have the appropriate qualifications. Otherwise, companies risk receiving subpar service, feeling a dangerous false sense of security and compliance where critical vulnerabilities still exist, and worse, subjecting themselves to additional costs of remediating inadequate security services or defective systems.

Another direct impact on organizations is the cost of non-compliance. The Cybersecurity Law provides elaborate regulations and definitions on legal liability, setting a variety of punishments, including monetary fines, suspension or removal of business licenses, revocation of permits, and criminal prosecution.

Protiviti Cybersecurity and Privacy Protection Services

IT Specialized Audit	• Often included in the overall audit co-sourcing or outsourcing program • More in-depth and technical than Information Technology General Control (ITGC) audit • Often focused on a specific part of IT operations such as Cybersecurity or Disaster Recovery
Security Risk and Compliance Assessment	• International Security Standards: ISO/IEC 2700x, NIST Cybersecurity Framework, CSA Cloud Control Matrix • Payment Card Security Standards: PCI DSS 3.x • Other Regulations/Standards: China Cybersecurity Law, HKMA, SFC, MAS, COSO SOX, ISO/IEC 27701
Data Privacy Services	• Compliance assessment against privacy regulations: Hong Kong PDPO Cap.486, China Personal Information Protection, EU GDPR, US CCPA • Managed privacy services: Privacy-as-a-service • Personal data inventory advisory
Attack and Penetration Service	• Vulnerability scan and penetration test • Source code review • Red team test • Phishing and social engineering test
Security Program and Strategy Design	• Design and revision of cybersecurity strategy and program • Design and revision of security policies, such as data and information classification • Design, revision, and implementation of security procedures
Security Architecture and Control Design	• System hardening review and enhancement • Security architecture design: on-premise, cloud platform • Security control design and review: firewall, data loss prevention, privileged access management, event log analyzer
Security Implementation Services	• Security tools design and selection • Project management and support for security tools implementation • Leverage Protiviti global partnerships with OneTrust, SailPoint, CyberArk, Palo Alto, ServiceNow, Carbon Black, Splunk, LogRhythm, etc.
Managed Security Services	• Security resource augmentation • Managed security operations • Third-party risk outsourcing
Incident Response and Forensics	• Security incident response advisory and support • Security incident investigation and root-cause analysis • Compromise assessment
Security Awareness and Capability Advisory	• Blueteam security assessment and advisory (e.g. SOC, MSSP) • Cyber incident handling and mitigation review • Security awareness assessment and support

How Protiviti Can Help

In response to an increase in IT security breaches and potential uncertainties in geopolitical affairs, the Chinese government is increasingly involved in safeguarding cybersecurity regulations and protecting personal information. Companies can expect to encounter heightened audit and security compliance measures and further demands on their already over-burdened IT and cybersecurity divisions.

Protiviti works with legal counsels, compliance officers, audit executives, IT professionals and top management at companies of all sizes, public or private, to assist them with their cybersecurity needs –from strategic advice around structure and objectives, to the development and implementation of tools and processes with subject matter expertise.

Contacts

Michael Pang
Managing Director, Technology Consulting
Mobile (HK): +852 9211 9853
Mobile (PRC): +86 131 4399 6166
michael.pang@protiviti.com

Jonathan Hsieh
Associate Director, Technology Consulting
Office: +86 21 5153 6900
Mobile: +86 138 1745 5636
jonathan.hsieh@protiviti.com