



# China's Cybersecurity Law and Its Impacts

*Key requirements businesses need to  
understand to ensure compliance.*



# Introduction

On June 1, 2017, China's Cybersecurity Law went into effect, marking an important milestone in China's efforts to create strict guidelines on cyber governance.

Long before the Cybersecurity Law took effect, China had already made some efforts to strengthen information security. For example, a white paper titled *The Internet in China*, published in 2010, served as an early guide to China's policy on internet usage.<sup>1</sup> But the Cybersecurity Law marks a significant milestone in China's efforts to combat cybercrime.

Despite the Cybersecurity Law's passage and enactment, uncertainties still plague its introduction. Because of ambiguous requirements and broadly defined terminology, some enterprises are concerned about the law's potential impact on their operations in China, while others worry that it will create trade barriers to foreign companies in the Chinese market.

Adding to the confusion, the public is still anticipating the release by the Cyberspace Administration

of China (CAC) of official guidelines to enhance the interpretation of the Cybersecurity Law. For example, on April 11, the CAC released for public comment the Draft Security Assessment Measures for Cross-Border Transfer of Private Information and Important Data.<sup>2</sup> The Draft Measures provide important supplementary information to article No. 37 of the Cybersecurity Law, which offers insight into how the Chinese government plans to manage the flow of private information and important data across borders.

## Overview of the Cybersecurity Law

Consisting of 79 articles in seven chapters, the Cybersecurity Law is exceptionally wide in scope, containing an overarching framework targeting the regulation of internet security, protection of private and sensitive information, and safeguards for national cyberspace sovereignty and security. Similar to some of the most commonly used cybersecurity standards, such as the Cybersecurity Framework of the National Institute of Standards and Technology (NIST) and ISO 27000-27001,

the Cybersecurity Law emphasises requirements for network products, services, operations and information security, as well as monitoring, early detection, emergency response and reporting. On the topic of protection of data privacy, the Cybersecurity Law is similar to data-privacy laws and regulations in other jurisdictions. However, the requirements related to national cyberspace sovereignty and security are more distinct.

<sup>1</sup> *The Internet in China*, People's Daily Online, June 2010, <http://en.people.cn/90001/90776/90785/7017177.html>.

<sup>2</sup> Cyberspace Administration of China, "Draft Security Assessment Measures for Cross-Border Transfer of Private Information and Important Data" (in Chinese): [www.cac.gov.cn/2017-04/11/c\\_1120785691.htm](http://www.cac.gov.cn/2017-04/11/c_1120785691.htm).





# Affected Organisations and Key Requirements

The Cybersecurity Law expressly applies to network operators and critical information infrastructure (CII) operators, as the terms for these entities are repeatedly mentioned in the law. “Network operator,” as defined in the appendix to the Cybersecurity Law, could be applicable to almost all businesses in China that own or administer their networks. Due to the loosely defined terms, however, the Cybersecurity Law may 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 (regardless of size and domestic or multinational

extent) operating its network — including websites and internal and external networks — to conduct business, provide a service or collect data in China could very likely be in scope.

Although the 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 details of the differences are outlined below.

- • • **Four out of the seven chapters in the Cybersecurity Law outline its major requirements:**

			
<b>Network</b>	<b>Information Security</b>	<b>Monitor and Response</b>	<b>Regulatory Penalties</b>
Policies and procedures, network products and services, security assessment and information storage	Protection of private information and collection, usage and distribution of information	Live monitoring, comprehensive incident response, incident drill and risk assessment	Removal from office and maximum fine ≤ RMB 1 million, plus suspension of business and revocation of licenses

## Network Operation

This chapter of the Cybersecurity Law has been divided into two subsections: those pertaining to ordinary provisions, which are applicable to network operators,

and those pertaining to operations security for CIIs. Notable requirements of each section include the following:

- • • **Section 1: Ordinary Provisions**

Article	Key Requirements*
No. 21	The following must be established: security policy and operation procedures, designated network security personnel, utilisation of network protection technologies, monitoring and tracing of network activities and incidents, retention of network operation log for no less than six months, data classification, critical data backup, and encryption.
No. 22 & No. 23	<ul style="list-style-type: none"><li>• Internet product and service providers must obtain authorisation before collecting customer information.</li><li>• Network equipment and internet service providers must meet government requirements and be certified by an authorised agent before they can be sold to the public.</li></ul>
No. 24	Verification of a client's true identity must be obtained before providing services.
No. 25	Network operators must develop a cybersecurity incident response plan that promptly addresses the risks of system vulnerability, virus infection, network attack and intrusion.
No. 26	Execution of cybersecurity authentication, risk assessments and testing shall comply with relevant national provisions.
No. 29	Network operators are encouraged to establish industrywide cybersecurity standards, enhancement of cybersecurity assessment and periodic reporting.

\* This is not an exhaustive list.

Compared to other security standards, article No. 24 is unique. It requires network operators to validate a user's true identity before signing service agreements. Services might include but are not limited to network access, landline services, mobile services, instant messaging and other internet services.

• • • **Section 2: Operations Security for CIIs**

Article	Key Requirements*
No. 31	Impose emphasis on cyber-security protection in the areas of public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, and other important industries and fields. Encourage non-CIIs to participate as well.
No. 32	Define clear roles and responsibilities for those responsible for planning, guiding and monitoring the security operation of a CII.
No. 33	Ensure stability and continuity in the operations of a CII.
No. 34	In addition to meeting the requirements specified in article No. 21, CIIs should also meet the following requirements: <ul style="list-style-type: none"> <li>• Set up a dedicated security management body and security management leader and conduct security background checks on those responsible personnel in key positions.</li> <li>• Periodically conduct network security, as well as technical training and skills evaluations for employees.</li> <li>• Conduct disaster-recovery backups of critical systems and data.</li> <li>• Formulate emergency response plans for cyber security incidents and periodically perform drills.</li> </ul>
No. 37	<ul style="list-style-type: none"> <li>• CIIs should retain private information and key data collected or produced while operating in China.</li> <li>• Security assessments must be conducted by the state network information departments and relevant departments of the State Council if the data needs to be transmitted outside of China.</li> </ul>
No. 38	<ul style="list-style-type: none"> <li>• A cybersecurity risk assessment should be conducted annually, at minimum, by CIIs internally or by third-party vendors.</li> <li>• The assessment report, along with remediation plans, should be provided to departments responsible for security protection of CIIs.</li> </ul>
No. 39	State network information departments will coordinate the following for CII security protection: <ul style="list-style-type: none"> <li>• Carry out reviews on the cybersecurity risks of CIIs.</li> <li>• Regularly coordinate CIIs in conducting network-safety emergency drills.</li> <li>• Promote network information security sharing among relevant departments.</li> <li>• Provide technical support and assistance for network security emergency management and recovery.</li> </ul>

\* This is not an exhaustive list.

Even though article No. 37 is specific to CIIs under the Cybersecurity Law, the requirement has been extended to individuals and other organisations per the Draft Measures. The Draft Measures provide more details in terms of what is to be expected; these details include but are not limited to the following:

- Network operators are asked to perform self-security assessments before transmitting data across borders.
- Assessments should be conducted based on data quantity, type, scope and sensitivity level.
- An annual assessment on security measures related to data transmission must be conducted. In some cases, the data recipient must conduct a security assessment as well.
- In cases where certain conditions are met, the network operator must request external authorisation to perform a security assessment before transmission.

## Information Security

Chapter four of the Cybersecurity Law pertains to information security, with a focus on the protection of private information. Private information, as defined in the appendix of the Cybersecurity Law, is applicable to 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, personal biometric information (such as fingerprints, facial recognition and retina scans), address, telephone number and similar personal details. Some selected articles from this chapter are:

Article	Key Requirements*
No. 40	Network operators must maintain a private information protection mechanism to keep user information strictly confidential.
No. 41	Collection and usage of private information shall be in compliance with laws and regulations made available to the public and under users' consent. Furthermore, network operators must not collect data unrelated to the service they provide.
No. 42	<ul style="list-style-type: none"><li>• Private information collected shall not be disclosed, damaged, tampered with or shared with others without the user's consent.</li><li>• Security measures should be taken to ensure the safety of private information. Emergency security measures shall be taken in the event of private information loss; notification shall be sent to the relevant authority and users.</li></ul>
No. 43	In the event a user discovers that network operators have violated the provisions of law, the user has the right to request that private information be removed. Furthermore, when errors are discovered, users can request that their information be updated.
No. 47	Network operators will strengthen the management of the information published by its users. Immediate security measures are required to prohibit the publication or transmission of inappropriate information.

\* This is not an exhaustive list.

The Cybersecurity Law's requirements on data privacy are very similar to data-privacy regulations in other jurisdictions, including Hong Kong's Personal Data (Privacy) Ordinance.<sup>3</sup>

<sup>3</sup> Hong Kong's Personal Data (Privacy) Ordinance: [www.blis.gov.hk/blis\\_pdf.nsf/CurAllEngDoc/B4DF8B4125C4214D482575EF000EC5FF/\\$FILE/CAP\\_486\\_e\\_b5.pdf](http://www.blis.gov.hk/blis_pdf.nsf/CurAllEngDoc/B4DF8B4125C4214D482575EF000EC5FF/$FILE/CAP_486_e_b5.pdf).

## Monitor and Response

This chapter highlights the importance of having an appropriate cybersecurity governance body to monitor, detect and respond to security incidents. In addition,

security assessments are to be conducted immediately following the event to determine impact and damage. Articles of note from this chapter include:

Article	Key Requirements*
No. 52	CIIIs are required to develop cybersecurity systems to monitor, detect and report security events.
No. 53	<ul style="list-style-type: none"><li>• CIIIs are required to develop a cybersecurity incident response plan and conduct drills periodically.</li><li>• Classification of cybersecurity incidents are required based on impact and risk level, and an appropriate cybersecurity incident response plan must be developed based on classification.</li></ul>
No. 55	Immediate activation of a cybersecurity incident response plan upon identification of an incident is required. Investigation and impact assessment must be followed, along with publication of a warning relevant to the public.

\* This is not an exhaustive list.

This section is very similar to those requirements as specified in the NIST Cybersecurity Framework and ISO 2700x, except that both of these standards are more descriptive in regard to their specific requirements.

## Regulatory Penalties

Chapter six of the Cybersecurity Law outlines the regulatory penalties associated with violation of the law. Penalties include monetary fines and legal liabilities to individuals and enterprises. Examples of monetary fines range from RMB 5,000 to RMB 1,000,000, while potential legal liabilities include suspension of an enterprise's business license,

removal of its business license, removal of individuals from office or responsible parties being held criminally responsible. For instance, violation of article No. 26 or article 37, mentioned previously, could lead to the suspension of a business license or termination of the business.



# Immediate Impact on Regulatory Compliance Activities

Shortly after the Cybersecurity Law went into effect, regulators leveraged the new law in their investigations across various industries and enterprises. Among those under current investigation according to the Cybersecurity Law are some of China's biggest social media platforms: Tencent, Baidu and Sina Weibo. The three internet giants are under investigation for potential violations of the Cybersecurity Law — specifically, their potential failure to control users who have posted inappropriate content. Such investigations appear to be related to national cyberspace sovereignty and security. Other reported cases for different causes (e.g., articles 21, 24 and 47) have resulted in monetary penalties or warnings to remediate those violations within a given period.

Overall, organisations that operate in China, either domestically or internationally, should take a closer look at the Cybersecurity Law to ensure that the company's current practise is in line with the regulatory requirements. Among the actions that companies should consider taking as they determine how to comply with the Cybersecurity Law include the following:

- Take stock of how information is collected, processed and stored, including private sensitive information (in the area of national cyberspace sovereignty).
- Assess cybersecurity and privacy risks and threats in order to focus cybersecurity efforts on the most critical risks and threats.
- Strengthen overall security governance, especially security policies and procedures.
- Evaluate business processes to ensure that proper controls are in place for the collection, use and storage of private information.

- Develop clear roles and responsibilities for cybersecurity and privacy management.
- Set up a security and privacy incident monitoring system and appropriate reporting mechanisms.
- Execute periodic cybersecurity assessments.
- Ensure proper safeguards of private and important information transmitted outside of China's borders (including security assessment).
- Design a proper security incident response plan and perform periodic drills.

For those companies already in compliance with international cybersecurity standards (such as ISO 2700x and NIST's Cybersecurity Framework) and data-privacy regulations, the good news is that much less work will be required to adhere to the Cybersecurity Law. However, these companies will still need to attend to requirements related to national cyberspace sovereignty and security. Furthermore, for Chinese subsidiaries of multinational enterprises, the data residency requirements might require redesign of certain application systems and infrastructure.







Even many well-established multinational enterprises face the same challenge when operating abroad, where they don't know what data is being collected, how the data is being used or where the data is located, restraining them from developing a solid baseline for their cybersecurity efforts. With the Cybersecurity Law, it becomes even more critical for companies to review their current operations, especially pertaining to data, to ensure compliance with the local regulation. At the end of the day, one cannot follow the correct procedures if one is not educated on the latest regulations.

# How Protiviti Can Help

A recent *Forbes* article highlighted that the role of cybersecurity specialists constitutes “the fastest-growing job with a huge skills gap” and goes on to note that the “Information Systems Audit and Control Association (ISACA) foresees a global shortage of two million cybersecurity professionals by 2019.”<sup>4</sup>

Recognising that hiring a full-time chief information security officer and building up a security team can be difficult and costly, Protiviti works with audit executives 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.

## Protiviti China Cybersecurity Services

 <p>IT Specialised Audit</p>	<ul style="list-style-type: none"> <li>• Often part of the overall audit program</li> <li>• Often focused on a specific part of IT operations</li> </ul>	<ul style="list-style-type: none"> <li>• More in-depth and technical than Information Technology General Control (ITGC) audit</li> </ul>
 <p>Security Assessment and Compliance</p>	<ul style="list-style-type: none"> <li>• International Security Standard : ISO/IEC 2700x and NIST Cybersecurity Framework</li> <li>• Privacy Regulations : Hong Kong Personal Data (Privacy) Ordinance, European General Data Protection Regulation</li> </ul>	<ul style="list-style-type: none"> <li>• Payment Card Security Standard: PCI DSS 3.2</li> <li>• Other Regulations/Standards : China CyberSecurity Law, COSO SOX , COBIT 5, HKMA , HK SFC</li> </ul>
 <p>Technical Security Assessment</p>	<ul style="list-style-type: none"> <li>• Vulnerability scan and penetration test</li> <li>• Source code review</li> </ul>	<ul style="list-style-type: none"> <li>• Phishing and social engineering test</li> <li>• Red team simulation</li> </ul>
 <p>Security Framework Design</p>	<ul style="list-style-type: none"> <li>• Design and revision of cybersecurity strategy and program</li> <li>• Design and revision of security policies such as data and information classification</li> </ul>	<ul style="list-style-type: none"> <li>• Design, revision and implementation of security procedures</li> <li>• Design and rolling out of cybersecurity incident response plan</li> </ul>
 <p>Security Implementation</p>	<ul style="list-style-type: none"> <li>• Server and operating system (OS) hardening review and upgrade</li> <li>• Network security architecture design and review (including IDS/IPS, SIEM)</li> </ul>	<ul style="list-style-type: none"> <li>• Security tools design and implementation support</li> </ul>
 <p>Security Operation</p>	<ul style="list-style-type: none"> <li>• Security resource augmentation</li> <li>• Security operation outsourcing</li> </ul>	<ul style="list-style-type: none"> <li>• Security incident monitoring and response</li> </ul>

<sup>4</sup> “The Fast-Growing Job With A Huge Skills Gap: Cyber Security,” Jeff Kauflin, *Forbes*, March 16, 2017, [www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#423a2d6f5163\\_](http://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#423a2d6f5163_)

## Protiviti's Competitive Advantages

01

### Technical and Business Risk is in Protiviti's DNA

- Deep experience in understanding and assessing information, technical and business risk across diverse industries.
- Risk and control specialists can assist in assessing technical and business risk as well as in advising the appropriate controls.

02

### Deep Expertise in IT Security and Cybersecurity

- Protiviti has deep expertise and experience in IT security, cybersecurity privacy assessment and advisory.
- Our staff has strong credentials and qualifications in security assessment, implementation and operations.
- Our past experiences allow us to deliver strong advisory services along with strong security operations.

03

### Global Experts

- Protiviti has hundreds of experts worldwide in information security and privacy and industry expertise in various industries (such as financial services, manufacturing and consumer services).
- Protiviti project teams can and will leverage all experience and capability from experts around the world.

## ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

## CONTACTS

### Scott Laliberte

Managing Director, Global Information  
Security Practice Lead  
+1.267.256.8825  
scott.laliberte@protiviti.com

### Michael Pang

Managing Director, IT Consulting  
Practice Lead, Protiviti Greater China  
+852.2238.0499  
michael.pang@protiviti.com

### David Cheung

Managing Director, Country Market  
Lead, Protiviti Greater China  
+86.21.5153.6900  
david.cheung@protiviti.com









**THE AMERICAS**

**UNITED STATES**

Alexandria  
Atlanta  
Baltimore  
Boston  
Charlotte  
Chicago  
Cincinnati  
Cleveland  
Dallas  
Fort Lauderdale  
Houston

Indianapolis  
Kansas City  
Los Angeles  
Milwaukee  
Minneapolis  
New York  
Orlando  
Philadelphia  
Phoenix  
Pittsburgh  
Portland  
Richmond

Sacramento  
Salt Lake City  
San Francisco  
San Jose  
Seattle  
Stamford  
St. Louis  
Tampa  
Washington, D.C.  
Winchester  
Woodbridge

**ARGENTINA\***  
Buenos Aires

**BRAZIL\***  
Rio de Janeiro  
Sao Paulo

**CANADA**  
Kitchener-Waterloo  
Toronto

**CHILE\***  
Santiago

**COLOMBIA\***  
Bogota

**MEXICO\***  
Mexico City

**PERU\***  
Lima

**VENEZUELA\***  
Caracas

**EUROPE  
MIDDLE EAST  
AFRICA**

**FRANCE**  
Paris

**GERMANY**  
Frankfurt  
Munich

**ITALY**  
Milan  
Rome  
Turin

**NETHERLANDS**  
Amsterdam

**UNITED KINGDOM**  
London

**BAHRAIN\***  
Manama

**KUWAIT\***  
Kuwait City

**OMAN\***  
Muscat

**QATAR\***  
Doha

**SAUDI ARABIA\***  
Riyadh

**SOUTH AFRICA\***  
Johannesburg

**UNITED ARAB  
EMIRATES\***  
Abu Dhabi  
Dubai

**ASIA-PACIFIC**

**CHINA**  
Beijing  
Hong Kong  
Shanghai  
Shenzhen

**JAPAN**  
Osaka  
Tokyo

**SINGAPORE**  
Singapore

**INDIA\***  
Bangalore  
Hyderabad  
Kolkata  
Mumbai  
New Delhi

**AUSTRALIA**  
Brisbane  
Canberra  
Melbourne  
Sydney

\*MEMBER FIRM