Understanding China's Cybersecurity Law

INFORMATION FOR NEW ZEALAND BUSINESSES

Ministry of Foreign Affairs and Trade, and New Zealand Trade and Enterprise

China's Cybersecurity Law came into effect on 1 June. It aims to protect national security – the definition of which extends to maintaining territorial integrity, social and economic stability, and the public order. It regulates how organisations and businesses should protect digital information, including whether and under what circumstances it can be transferred out of mainland China, and introduces measures aimed to safeguard internet systems, products and services against cyber-attacks.

It's important that you understand how the law's requirements may relate to you. This information sheet provides general information and does not constitute legal advice. You may wish to seek expert advice specific to your circumstances.

OVERVIEW

Areas of the law that could impact on business operations include:

- Requirements to establish systems to prevent data leaks and theft, and report any cybersecurity incidents to users and relevant authorities
- Draft requirements to conduct security self-assessments when seeking to transfer personal information or other "important data" generated in China out of mainland China, to take effect from 1 December 2018
- A range of additional, more stringent, obligations on critical information infrastructure operators
- New requirements to construct cloud service platforms within mainland China, and requirements that cloud services facilities and data storage for services that target Chinese users remain in China
- Requirements for telecoms businesses to use licensed virtual private networks (VPNs), and requirements for foreign businesses to rent VPNs from "authorised" carriers.

BACKGROUND

China's Cybersecurity Law reflects a broader global trend to regulate cyberspace activities and counteract cyber-threats that could undermine public security.

The rapid growth in electronic commerce and electronic payment methods, and technological advances in cloud computing and big data analytics, has given rise to new cybersecurity concerns. The online trade of personal information has also become big business in China, leading to concerns and more stringent rules around the collection, use and storage of personal information online.

Increased investment into 'smart' manufacturing and 'Internet of Things' technologies is also driving moves to ensure that so-called 'smart' machines as well as infrastructure-supporting industries deemed critical to national security are secure and not vulnerable to cyber-attacks.

The newly-created Cyberspace Administration of China oversees implementation and enforcement of the Cybersecurity Law. It is actively implementing a long and growing list of measures and standards.

The law came into effect on 1 June, but draft regulations continue to be issued, many of which are subject to a comment period – so further changes can be expected.

The main points of obligation under the law are on network operators and critical information infrastructure operators. These terms have been defined broadly, and the extent and scope of the obligations on these operators continue to be worked out through draft guidelines.

SCOPE OF THE LAW AND KEY PROVISIONS

China's Cybersecurity Law focuses on the nature and flow of digital information that has been generated in China. It places a strong emphasis on securing personal information and other important data that has been collected in China, and standardises its collection and usage.

Network operators (currently defined as the owners and administrators of networks and network service providers) are expected, amongst other things, to:

- clarify cybersecurity responsibilities within their organisation;
- take technical measures to safeguard network operations and prevent data leaks and theft; and
- report any cybersecurity incidents to both users of the network and the relevant implementing department for that sector.

According to recently released draft guidelines, network operators can transfer data overseas under most circumstances. However they would be required to carry out regular security self-assessments to gauge the risk of data transfers based on factors such as quantity, scope and sensitivity of the data. Where the nature of the data is deemed to be "important" (for example, if it relates to population and health, marine environment or sensitive geographic information, or other information likely to affect national security or the public interest), network operators would be subject to further inspection, and could be prevented from transferring the data overseas. According to the draft measures, network operators have until 1 December 2018 to conform to the data transfer provisions.

PUBLISHED: SEPTEMBER 2017

Critical information infrastructure operators face additional, more stringent, obligations. There is currently no fixed definition of the term "critical information infrastructure operator". This means that organisations operating in sectors removed from telecommunications infrastructure could still be impacted by the law's more stringent requirements. Such operators are expected, amongst other things, to:

- store personal information and important data collected and generated in China within mainland China. If transmission of such data out of China is necessary due to business needs, clearance procedures shall be followed according to separate rules formulated by the Cyberspace Administration of China;
- procure "safe and controllable" Internet technologies, products and services; and
- conduct regular audits of cyber-technology systems and processes.

Securing the supply chain – regulating the use of certified network products and services

Specialised equipment, products and services designed to ensure network security (such as routers, switches and servers) must adhere to compulsory government standards in order to be used in China. Any critical information infrastructure operator using network-related products and services that are important to national security and the public interest must go through network security reviews.

Related measures on cloud services operations

Cloud service operators are expected, amongst other things, to:

- hold a value-added telecommunications license (which are still subject to certain foreign investment restrictions);
- construct cloud service platforms within the territory of China; and
- locate service and data storage facilities in China for services that target Chinese users.

Cloud service providers may also need to follow the same draft requirements for security self-assessment and potential audits by regulators as are applicable to network operators when transferring personal information and "important data" across borders.

VPN regulations

New directives have also been released aimed at "clearing up" and regulating the Internet access service market, by 31 March 2018. Under these moves, telecom businesses will need prior approval before providing VPN services. Businesses using unapproved VPNs could be impacted if the particular VPN they are using is affected by the regulations.

Foreign businesses who need to access cross-border networks can rent VPNs from authorised carriers. We recommend checking whether the provider of your VPN is licensed in China.

WHAT STEPS CAN NEW ZEALAND BUSINESSES TAKE?

This is an evolving area of law that applies to companies differently, depending on their nature and the area they operate in. We'll keep you informed as changes develop – in the meantime though, we recommend that you:

- consider the updates to Chinese cybersecurity law and how they will relate to your business;
- review your policies on information technology, information security management and personally identifiable information;
- check whether your VPN provider in China is a "licensed" provider; and
- consider whether you might need to seek specialised legal and/or technical advice.

CONTACTS FOR FURTHER INFORMATION

New Zealand Trade and Enterprise (exporthelp@nzte.govt.nz) or the Ministry of Foreign Affairs and Trade (exports@mfat.govt.nz) can provide information on who you could contact for more specialised advice, as required.

The Ministry of Foreign Affairs and Trade is also interested to learn about possible barriers to trading in the China market. If your business is experiencing difficulties operating in the China market due to Cybersecurity Law-related requirements, or any other legal or regulatory requirement, we encourage you to contact us at exports@mfat.govt.nz. You can also complete a non-tariff barriers form, which is available at the following address:
mfat.govt.nz/en/trade/how-we-help-exporters/non-tariff-measures-form

The New Zealand Government, through the Cyber Security Strategy, is committed to engaging with trading partners on the development of cybersecurity regulations to ensure that new requirements do not create barriers to trade. Information about New Zealand's Cyber Security Strategy is available at the following address:
www.dpmc.govt.nz/our-business-units/security-and-intelligence-group/national-cyber-policy-office

PUBLISHED: SEPTEMBER 2017