

www.pwc.com

www.vischer.com

SWISS  
CHINESE  
CHAMBER  
OF  
COMMERCE

# *China Cyber Security Law*

**Challenges, Impacts and Responses**

Swiss-Chinese Chamber of Commerce (SCCC)  
Luncheon, June 12, 2017

Felix Sutter, President SCCC and Head Asia  
Business Group PwC

Lukas Zuest, Attorney at Law, Counsel and  
Head China Desk VISCHER

瑞  
中  
經  
濟  
協  
會

**pwc**

VISCHER

## *Overview*

- 1. Chinese Cyber Security Law (CSL)*
- 2. Definitions of Major Terms*
- 3. Data Localisation*
- 4. Security Review*
- 5. Next Steps*

---

# *1. Chinese Cyber Security Law (CSL)*

---

## ***Cybersecurity Law - Scope of Jurisdiction and Application***

This law applies with respect to the **construction, operation, maintenance and usage of networks**, as well as **network security supervision and management within the mainland territory** of the People's Republic of China. (Article 2)

Scope of Application:

- Cyber Security
- National Security
- Censorship
- Personal Data Protection
- Data Localization

---

## *2. Definitions of Major Terms*

---

# ***Network Operators***

When talking about network operators, people usually refer to the Internet service providers, cloud service providers and etc. Cyber Security Law Article 76 (point 3) gives the definition of “Network Operators”: “Network operators” refers to **network owners, managers and network service providers**.

Under this definition, **the applicable scope of “network operators” will be extended**. Enterprises and institutions who provide service and carry out business through the internet may be considered as “network operators”. Other than traditional telecommunication operators and internet enterprises, network operators may also include:

- Key industries (i.e. Public communication and information services, Finance, Public service, Electronic governance, etc.), which collect / manage personal information and provide online services;
- Network security services and product providers;
- Companies who own websites and provide network services.

# Critical Information Infrastructure Operators

The Cybersecurity Law's Article 31 mentions that “the specific scope and security protection measures for Critical Information Infrastructure will be formulated by the State Council”. **The State Council has not issued the specific scope of the Critical Information Infrastructure.**

However, the Office of the Central Leading Group for Cyberspace Affairs (a central communist party organization, not under the State Council), issued the **Critical Information Infrastructure Identification Guideline (Trial)** in 2013, which provides **guidance to regulators** to identify “Critical Information Infrastructure Operators”. **It is uncertain whether State Council will adopt the same guideline in classification.**

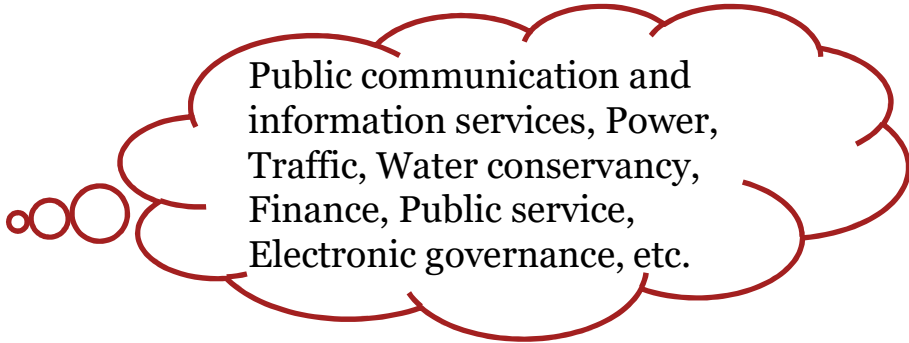
Area	Condition
<b>Website</b>	In the event of network security incidents: leakage of more than <b>1,000,000 users' personal information</b> ; leakage of sensitive information of a large amount of institutions and enterprises
<b>Platform (User amount)</b>	More than <b>10,000,000 registered users</b> or more than <b>1,000,000 active users</b> (login at least once daily)
<b>Platform (Range of Influence)</b>	In the event of network security incidents: more than RMB 10,000,000 direct economic loss; leakage of more than <b>1,000,000 users' personal information</b> ; direct impact to life and work of more than 10,000,000 people; leakage of sensitive information of a large amount of institutions and enterprises
<b>Production Operations</b>	Data centres with more than 1,500 standard racks

---


# ***Critical Information Infrastructure***

Article 31, Cybersecurity Law:

Important  
Industries/Areas



Public communication and information services, Power, Traffic, Water conservancy, Finance, Public service, Electronic governance, etc.



National security  
National welfare  
People's livelihood  
Public interest

Impact of the Information Infrastructure being destroyed, losing function or leaking data



# “Personal Information” Scope

## 第七章 附 则

### Clause

第七十六条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

According to the **China Cybersecurity Law**, "personal information" refers to all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including, but not limited to:

- natural persons' full names
- birth dates
- identification numbers
- personal biometric information
- Addresses
- telephone numbers
- Etc.

---

## ***Important Data***

Important Data is defined as : «data closely related to national security, economic development and public interest» (Article 17 Draft Measures for Evaluation the Security of Transmitting Personal Information and Important Data Overseas)

Question: Are data derived from personal information such as statistical data qualified as important data?

---

## *ISA 315 (excerpt from the standard)*

### Regulatory Factors

A19. Relevant regulatory factors include the regulatory environment. The regulatory environment encompasses, among other matters, the applicable financial reporting framework and the legal and political environment. Examples of matters the auditor may consider include:

- Accounting principles and industry-specific practices.
- Regulatory framework for a regulated industry.
- Legislation and regulation that significantly affect the entity's operations, including direct supervisory activities.
- Taxation (corporate and other).
- Government policies currently affecting the conduct of the entity's business, such as monetary, including foreign exchange controls, fiscal, financial incentives (for example, government aid programs), and tariffs or trade restrictions policies.
- Environmental requirements affecting the industry and the entity's business.

A20. ISA 250 includes some specific requirements related to the legal and regulatory framework applicable to the entity and the industry or sector in which the entity operates.<sup>7</sup>

---

## ***3. Data Localization Requirements***

---

## **Data Localisation Requirement (1/2)**

**Personal information and other important data** gathered or produced by **critical information infrastructure operators** during operations within the mainland territory of the People's Republic of China, shall **store it within mainland China**. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State network information departments and the relevant departments of the State Council to conduct a security assessment; but where laws and administrative regulations provide otherwise, follow those provisions. (Article 37)

Cyberspace Administration of China (CAC) published the “**Measures for Security Assessment of Transmitting Personal Information and Important Data Abroad** (Draft) (hereinafter referred to as “the Measures”) on Tuesday, 11 April 2017, which is an important echo of the China Cyber Law.

**Potential impacts:** The most significant aspect of the Measures is that it applies to **Network Operator, not only the Critical Information Infrastructure Operators (CIIO) as stated in Article 37** which requires “personal information and important data gathered or produced by CIIO during operations within the mainland territory of the PRC shall be stored within mainland China.” As a result, **all of the Network Owners, Network Managers, and Network Service Providers need to comply with the Measures.**

---

## *Data Localisation Requirement (2/2)*

**Two types of security assessment:**

### **I. Self-Assessment**

1. the necessity of transmitting data overseas; 2. content related to personal information, including the quantity, scope, type and sensitivity of personal information, as well as whether or not the **subjects concerned agree to transmit their personal information overseas**, etc.; 3. content related to **important data**, including the quantity, scope, type and sensitivity of important data; 4. safety protection measures, capabilities and levels of data recipients, as well as the network security environment in their countries and regions, etc., 5. **risks such as leakage, damage, falsification and abuse of data** after the data is transmitted overseas and re-transferred; 6. risks to **national security, public interests** and personal legal advantage which are likely to arise due to transmission of data to overseas parties and gathering of overseas data; and 7. other significant matters required to be evaluated.

### **I. Official Security Assessment:**

1. where the data involves or totally involves the personal information of **over 500,000 individuals**; 2. where the data volume **exceeds 1,000 GB**; 3. where the data contains information in the **fields of nuclear facilities, chemical biology, national defense and military, population health and the like, and information about major engineering activities, the marine environment and sensitive geography**; 4. where the data contains network security information such as system vulnerabilities and security protection of critical information infrastructure; 5. where **critical information infrastructure operators** provide personal information and important data for overseas parties; and 6. other factors which **may affect national security and public interests**, and should be evaluated by the competent authority or regulator of the industry.

---

## *4. Security Review*

---

## ***Measures on the Security Examination of Network Products and Services (promulated on May 2 2017)***

**Critical network equipment** and **specialized network security products** shall follow the national standards and mandatory requirements, and be safety **certified** by a qualified establishment or meet the requirements of a safety inspection, before being sold or provided. The state network information departments, together with the relevant departments of the State Council, formulate and release a **catalogue of critical network equipment and specialized network security products**, ... (Article 23)

**Potential impacts:** The purchase of the critical network equipment and specialized security products will be impacted if those equipment or products do not have the safety certification or not comply with the national standards/mandatory requirements. If the current in-use network equipment were out of the catalogue, they could not be upgraded and have to be switched to other products when they became outmoded, which may cause more cost.

**How to respond:** Before the release of the catalogue of critical network equipment and specialized network security products, enterprises may refer to Article 21 of the *Administrative Measures for the Graded Protection of Information Security* (《信息安全等级保护管理办法》) published by the Ministry of Public Security, etc. in 2007 to have a assessment of the in-use network equipment, the relevant purchase plan, and the vendor qualification.



---

## *Security Review (2/2)*

### **Strengthening of government supervision and controls**

- Network operators carrying out business and service activities must follow the laws and administrative regulations, ..., **accept supervision from the government** and public, and bear social responsibility. (Article 9)
- **At least once a year, critical information infrastructure operators** shall conduct an **inspection and assessment of their network security and risks** ... and submit a network security report on the circumstances of the inspection and assessment as well as improvement measures... (Article 38)
- Network operators shall provide **technical support and assistance to public security organisations and state security organisations**;... (Article 28)
- Adopt technological measures for monitoring and recording network operational status and network security incidents, and follow relevant provisions to **store network logs for at least six months** (Article 21, Item 3)

---

## *5. The Next Step*

---

## ***ISA 315***

Who is affected?

Timeline?

What is expected?

What are the options?

---

# *What questions should a Swiss Company that is active in Mainland China consider?*

## **Compliance:**

- Do you understand your organization's compliance status?
- Are you an enforcement target?
- Do you use third parties for important businesses processes?

## **Data Privacy:**

- Is the data protection mechanism safe?
- Where does your organization store critical business data and personal information?
- Do you have obtained the consent from the individual to process and transmit their personal data?

## **Security Review:**

- Are the products and services sold or purchased by your organization subject to the security review?

## **Emergency Response:**

- Do you know how to strengthen your cyber security monitoring and incident response mechanism?

## **Infrastructure Vulnerability**

- Can your cyber security infrastructure provide quickly responses to IT problems?

## **Employee Awareness:**

- Do you have regular workshops to improve your employee's security awareness and technical skills?

# *SCCC your partner along the way*

SWISS  
CHINESE  
CHAMBER  
OF  
COMMERCE

Luncheons

Round Tables

Position Paper

Interaction with Swiss and Chinese Governments

瑞  
中  
經  
濟  
協  
會

## ***Your contacts:***

Felix Sutter, President SCCC and Head Asia  
Business Group PwC

[felix.sutter@ch.pwc.com](mailto:felix.sutter@ch.pwc.com)

+41 58 792 2820

Lukas Zuest, Attorney at Law, Counsel and  
Head China Desk VISCHER

[lzuest@vischer.com](mailto:lzuest@vischer.com)

+41 58 211 34 35



This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2017 PricewaterhouseCoopers Limited and VISCHER Ltd. All rights reserved. PwC refers to the China or Hong Kong member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.