CHINA'S CYBERSECURITY LAW

QUESTIONS AND ANSWERS

(First Version, September 2017)

Cybersecurity and data protection are hot topics in many countries around the world. China is no exception. In addition to increasing the protection of personal data, China has also legislated a direct connection between cybersecurity and its national security. These developments come in the form of China's Cybersecurity Law, which came into effect on 1 June 2017.

The Cybersecurity Law provisions, especially those defining critical information infrastructure and regulating data localization and cross-border transfers, have caused significant concern for multinationals in China. Implementing regulations have attempted to clarify certain provisions under the Cybersecurity Law; however, concerns remain.

The Shanghai Corporate Team of Global Law Office has been advising international clients on cybersecurity developments in China from well before the official promulgation of the Cybersecurity Law. Our attorneys have a deep understanding of the regulatory regime and our clients' compliance concerns and needs.

The following questions and answers, which are not exhaustive, are intended to help develop your understanding of the Cybersecurity Law. Our answers are based on our interpretation of the law and our experience.

We trust you find these questions and answers informative and useful. We would be pleased to assist you with the specific circumstances of your company.

SHANGHAI CORPORATE TEAM
GLOBAL LAW OFFICE

I. Introduction 简介

1. What is the Cybersecurity Law and what does it aim to regulate? 什么是网络安全法，它的目标是什么?

China's Cybersecurity Law consolidates and expands pre-existing cybersecurity and data protection laws and regulations. The law has four key objectives:

a. ensure China's cybersecurity;

b. guard China's cyberspace sovereignty, national security, and public interests;

c. protect the legitimate rights and interests of individuals and organizations; and

d. promote the healthy development of information technology ("**IT**") in China.

The Cybersecurity Law, promulgated by the Standing Committee of the National People's Congress, came into effect on 1 June 2017. As is typical in China, the Cybersecurity Law sets out a broad set of principles, which are intended to be clarified through a series of implementing regulations and guidelines to be issued by the relevant authorities.

2. What implementing regulations are currently in force? 现行有效的配套法规有哪些?

a. Measures on Security Review of Network Products and Services ("**Product Review Measures**"), which came into effect on 1 June 2017. These measures are aimed at controlling the security of products and services used or provided via the Internet (see question 25 below).

b. The Catalogue of Critical Network Equipment and Special Network Security Products (First Batch), which came into effect on 1 June 2017. This catalogue sets out the list of critical network equipment and special network security products that are subject to certification (see question 25 below).

See question 38 for draft regulations that have been issued to the public for comments.

3. Does the Cybersecurity Law target foreign-invested companies in China? 网络安全法是否针对在华的外商投资企业?

The Cyberspace Administration of China ("**CAC**"), which is in charge of implementing the Cybersecurity Law, has stated that:

a. the Cybersecurity Law is not aimed at limiting the free flow of data;

b. the data transfer security reviews under the Cybersecurity Law (see section III below) will not be used to target any particular country or region; and

c. foreign technology or products will not be discriminated against, nor will their access to the Chinese market be limited, by the Cybersecurity Law.

Nevertheless, foreign-invested companies in China are more likely to be impacted by the data security reviews (see section III below) given that foreign-invested firms that collect data within China typically transfer the data to their offshore servers for storage and processing. Moreover, as the product certification procedures (see question 25 below) are not completely transparent, we cannot preclude the possibility that preference may be given to domestic products and equipment.

Notwithstanding, the CAC is of the view that the Cybersecurity Law will boost consumer confidence in products and services, and allow companies to expand their markets.

4. What is the CAC? 什么是网信办?

The CAC was set up by the State Council in 2014 to act as the central body in charge of censorship and oversight and control of the use of the Internet in China. The CAC reports to the Central Leading Group for Internet Security and Informatization, which is headed by the General Secretary of the Communist Party, Xi Jinping.

The first statutory reference to the CAC can be found in the Anti-Terrorism Law. In a press release on 31 May 2017, Xi Jinping mentioned that national security could not be achieved without cybersecurity. We believe it was this concern which gave birth to the CAC.

The local CAC branches supervise, administer, and implement the Cybersecurity Law within the locality of their respective jurisdictions (i.e., as zones, cities, and provinces). The central CAC oversees cases that have or could have a nationwide impact.

We understand that local CAC branches have been set up. However, in some localities these are not independent bodies, but merely a department under the municipal government – for example, the local CAC branch in Shanghai is a department under the Shanghai Municipal government.

5. To whom and what does the Cybersecurity Law apply? 网络安全法的调整对象和适用范围?

It regulates the construction, operation, maintenance, and use of a "network" in China, and applies to:

a. Network operators (see question 7 below);

b. Network operators of critical information infrastructure ("**CII**") (see question 0 below); and

c. Providers of critical network equipment and specialized cybersecurity products (网络关键设备和网络安全专用产品) (see section IV below).

6. What is a network? 什么是网络?

"Network" is defined broadly as a "system comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange, and processing."

7. Am I a network operator? 何为网络运营者?

"Network Operator" is defined as (a) network owners, (b) network managers, and (c) network service providers.

Based on the legislative history of the Cybersecurity Law, it appears that the scope of "network service provider" was purposely drafted to be broad and vague. Accordingly, it may be argued that any enterprise that uses a network to collect, store, transfer, exchange, or process information through networks to provide products and services to end users may constitute a "network service provider". This position is supported by similar terms used in other laws. If so, every business that uses a network in any sector or industry will be subject to the Cybersecurity Law.

8. What are my main obligations? 网络运营者主要有哪些义务?

Network operators are subject to both general obligations and specific obligations for handling personal information.

a. Key General Obligations

Chapter 3 of the Cybersecurity Law requires network operators to:

(i) Implement mandatory national and industry standards to achieve network security. The National Information Security Standardization Technical Committee (a standards committee under the CAC, also known as TC260) has issued standards and draft requirements for a tiered protection system, as well as detailed guidelines for personal information protection, such as:

- the Information security technology – Classification guide for tiered protection of information system security, and
- Information security technology - Guideline for personal information protection within information system for public and commercial services.

Among other things, these standards require the use of technology that is "secure and controllable". This and related terms remain problematic and could be used to disadvantage international firms vis-à-vis local competitors in China.

(ii) Implement tiered security systems, which includes (1) formulating internal security management systems and operating rules, (2) adopting technical measures to prevent cyber-attacks and compromises to the network, (3) monitoring and recording of network operational statuses and network security incidents, and maintaining network logs, and keeping the records for at least six months, and (4) backing-up "important data" (see question 16 below) and adopting encryption measures, mandatory standards and technical measures.

(iii) Provide security maintenance for their products and services.

(iv) Require users to provide their personal information, and if the information provided is false, to cease providing them with services. This obligation applies only to network operators providing services relating to network access, domain registration, phone network access, information publication, or instant messaging.

(v) Formulate emergency response plans for network security incidents, and report the same to the authorities.

(vi) Monitor networks to ensure false information is not disseminated and no unlawful activities (e.g., using information to commit fraud) are being conducted.

(vii) Provide technical support and assistance to China's public security agencies and state security agencies for those agencies to maintain national security and investigate crimes in accordance with the law. Potentially, this means that a network operator would need to give full access to data to these Chinese governmental agencies if demands were made to assist with a criminal investigations; not only is there a risk of compromising of data, the network operator might not be compensated for the time and resources spent assisting with an investigation (see questions 30 and 0 below).

b. Key Additional Obligations

If a Network Operator also handles personal information, it will have additional obligations to:

(i) collect and use personal information in a legitimate, appropriate, and necessary manner;

(ii) before collecting and using the data, fully explain to and obtain the consent of the information provider regarding the purpose, method, and scope of the collection and use of the data;

(iii) ensure that it keeps the data strictly confidential and not disclose, sell or unlawfully provide the information to a third party; neither should the data be tampered with or destroyed; and

(iv) secure the safety of the information and protect it from being leaked, destroyed, or lost.

The draft Measures for Security Assessment of Cross-Border Transfer of Personal Information and Important Data ("**Draft Data Transfer Measures**") also requires network operators to perform security assessments when transferring abroad any personal information or "important data" collected within China (see section III below). It is interesting to note that the main statute, the Cybersecurity Law, only imposes this cross-border transfer restriction on operators of CII. This discrepancy has resulted in a legal loophole – there are no statutory penalties on network operators who fail to perform this obligation. We expect this issue to be addressed in the next round of revisions of the Draft Data Transfer Measures or other implementing regulations.

II. Personal Information 个人信息

9. What is Personal Information? 什么是个人信息?

Article 76(5) of the Cybersecurity Law defines "personal information" as "information that is recorded in electronic or any other form and used alone or in combination with other information to recognize the identity of a natural person, including but not limited to the name, date of birth, ID number, personal biological identification information, address, and telephone number of the natural person."

In the Draft Data Transfer Measures, the definition varies slightly in that "personal information" also includes information that reflects the activities of a particular natural person, including contact information, account passwords, property status, locations, and behavioral information. If issued in its current form, the effect of the Draft Data Transfer Measures would be to include as personal information such things as online shopping histories, travel plans, and credit card usage.

10. What restrictions does the Cybersecurity Law place on the collection, use, and transmission of personal information? 网络安全法对个人信息的收集、使用和传播有何限制?

a. Collection -- Chinese companies, including foreign-invested companies, may collect personal information as long as they comply with their obligations as set out in our answer to question 8 above. Additionally, if the business is considered a CII, and the personal information is collected

in China, then the company must store such information in China (see section III below).

b. Use -- Chinese companies must use personal information in line with the statutory obligations set out in our answer to question 8 above.

c. Transmission -- If a Chinese company runs a business that is considered CII (see question 0 below) and collects personal information in China, it must store such information in China. Furthermore, all network operators must conduct a security assessment before transmitting the information abroad (see section III below).

11. Are there disclosures of personal information for which individual consent cannot be given? 是否存在未经个人同意披露个人信息的情形?

Yes, individual consent cannot be given for disclosures or types of usage that are not legitimate or appropriate. For example, individual consent does not allow the use of that person's information to be used to compromise China's national security.

12. Are network operators expected to notify the CAC of a security incident? 如发生网络安全事件，网络运营者是否需要通知网信办?

Yes. The Cybersecurity Law also requires network operators to have an emergency response plan and to report all network security incidents, including any security flaws and vulnerabilities in products and services (see question 8.0.0 above).

13. Can individuals claim compensation for unlawful disclosure of personal information? 个人是否可以就非法披露其个人信息而要求赔偿?

Yes, an individual may bring a tortious claim against a network operator for unlawfully disclosing personal information and infringing his or her right to privacy. The individual whose right to privacy is infringed is entitled to claim from the tortfeasor losses arising from the breach as well as damages for emotional harm. These rights of claim are set out in Article 12 of the Provisions of the Supreme People's Court on Application of Laws to Cases Involving Civil Disputes over Infringement upon Personal Rights and Interests by Using Information Networks.

III. Cross-border Data Transfer 数据跨境传输

14. Am I a CII? 何为 CII?

You will likely be a CII if you operate network facilities and information systems, which, if subject to any damage, dysfunction or data leakage, might severely jeopardize national security, people's livelihood or the public interest. This is set out in Article 18 of the Regulations for the Security Protection of CII (Draft for Comment) circulated by the CAC on 10 July

2017 ("**Draft CII Regulations**"), which provides that the following entities are CII:

a. government agencies and entities in the energy, finance, transportation, water conservation, healthcare, education, social insurance, environmental protection and public utilities sectors;

b. entities which own and/or operate information networks, such as telecommunication networks, broadcast television networks and the internet, and entities providing cloud computing, big data and other large-scale public information network services;

c. research and manufacturing entities in sectors such as science and technology for national defense, chemical industry, and food and drug sectors, and entities manufacturing large equipment in any sector; and

d. media units such as broadcasting stations, television stations, and news agencies.

The specific scope and security measures for CII are yet to be developed by the State Council. However, we understand that 400-500 enterprises, mostly state-owned enterprises, have already been designated, and notified, by the CAC as CIIs. This list of CII is not publicly available.

According to our recent consultation with CAC officials, the CAC has begun to focus on compliance of information network entities, such as telecommunication networks, entities providing cloud computing, big data, and other large-scale public information network services. Specifically, the CAC has focused on ensuring the compliance of Baidu, Alibaba, and Tencent, which are China's largest internet companies.

15. What are the main legal obligations of a CII? CII 主要有哪些义务?

Apart from the obligations of network operators (see question 8 above), CII operators must also satisfy the following obligations:

a. Ensure that their formation will be able to support a stable business and sustain operations and that technical security measures are planned, established, and implemented.

b. Security protection obligations:

   (i) set up a dedicated security management body, designate a person in charge, and review the security backgrounds of the person in charge and others in key positions;

   (ii) periodically conduct cybersecurity training, technical training, and skill assessment for employees;

   (iii) conduct disaster recovery backup of important systems and databases;

(iv) work out an emergency plan for cybersecurity incidents and carry out drills regularly; and

(v) perform other obligations provided for in relevant laws and administrative regulations.

c. Obligations when purchasing network products and services

(i) ensure that any purchase of network products and services by CII operators that might impact national security is subject to the national security review conducted by the CAC together with competent departments of the State Council; and

(ii) when purchasing network products and services, enter into an agreement with the product or service provider; this agreement must specify each parties' obligations and responsibilities with respect to confidentiality and network security.

d. CII operators must store in China all personal information and "important data" collected and generated from their operations in China.

e. Each CII operator must examine and assess its potential cybersecurity risks at least once a year. It may do this by itself or by engaging a cybersecurity service provider. Although there are no statutory requirements, we understand that it is very likely that these service providers will need to be accredited by the CAC. The examination and assessment results, as well as improvement measures, must be submitted to the competent authorities in charge.

f. CII operators must inform the authorities in advance of any remote maintenance. The general rule is that maintenance for CII must be carried out in China. However, if remote maintenance is necessary for business operations, the CAC and the public security bureau should be informed in advance.

16. What is "important data"? 何为"重要数据"?

The Cybersecurity Law does not provide a definition for "important data". However, a vague definition can be found in the Draft Data Transfer Measures. These draft measures state that "important data" is: "data closely related to national security, economic development, and social and public interests; the specific scope of important data shall be determined with reference to relevant national standards and guidelines on the identification of important data." This points us to the draft Guidelines for Data Cross-Border Transfer Security Assessment ("**Draft Guidelines**").

Appendix A of the Draft Guidelines states general criteria for identifying "important data": data, including raw and derivative data but excluding state secrets, whether collected by the government, enterprises or individuals in China, which (i) relates closely to national security, economic development and the public interest, and (ii) if disclosed without authorization, lost, abused,

tampered with, destroyed, aggregated, integrated, or analyzed may cause any of the listed negative consequences, including, damage to state property or dereliction of statutory duty.

The Draft Guidelines then set out 28 sections, each covering an industry or sector, including energy, electronic manufacturing, e-commerce, finance, geographical information, military, telecommunications, and utilities. Each section sets out information that may be considered important data for that sector. For example, in the equipment manufacturing sector, information relating to investments is considered to be important data. And for the civil nuclear facilities sector, civil nuclear facilities operation information is considered to be important data, as is the financial information of natural and legal persons for the finance sector. The headings or sub-headings also branch out to include more specific types of information.

17. What are the types of security assessments? 安全评估有哪几种?

The Data Measures create two forms of security assessments – self-assessment and government assessment – depending on the type, amount, and importance of the data.

a. Self-Assessment

This can be done by a network operator itself, or by network security service agencies accredited by the CAC.

b. Government Assessment

A government assessment will need to be conducted in the event that the data to be transferred contains:

(i) within one year, more than 500,000 individuals' personal information;

(ii) information on nuclear facilities, biochemistry, national defense, population health, large-scale projects, marine environment, sensitive geographic information, important financial data, and other important data;

(iii) information on the CII's security deficiencies, specific security measures, and other network security information; or

(iv) information that may affect national security, economic development, and social public interests.

18. What does the security assessment entail? 什么是安全评估?

The focus of a security assessment will be:

a. The necessity of the data transfer to overseas, and the legitimacy of the transfer.

b. The quantity of personal information, including the number, scope, type, sensitivity, and whether the personal information provider has consented.

c. For important data, the number, scope, and type of important data.

d. The security protection mechanisms in the place and the country to which the information is going.

e. The risk of the transferred information being divulged, damaged, tampered with and misused.

f. Possible risks to national security, public interests and legitimate personal interests.

Reference can be made to Draft Guidelines for the detailed technical requirements of the security assessments.

19. Are security assessments required for data transfer between the branches of multinational companies located in China and abroad? 跨国公司境内外分支机构之间的数据传输是否需要安全评估?

Yes, if the transfer will involve data collected in China being transferred abroad.

20. How often are security assessments required? 多久需要进行安全评估?

The Draft Data Transfer Measures clarify that security assessments should be conducted annually, unless:

a. there is a change in destination, scope, and type of data;

b. there is a change in the person receiving the data; or

c. a major security event occurs.

If any of these changes occur, then an additional security assessment may need to be carried out.

21. Other than the important data, can other data be freely transferred cross-border? 除了重要数据之外，其他数据能否自由地进行跨境传输?

Article 2 of the Draft Data Transfer Measures requires all network operators to conduct a security assessment before transferring offshore any important data or personal information collected in China. However, Article 37 of the Cybersecurity Law imposes the same obligation only on operators of CII.

22. Can I maintain my data center outside China? 我能否把我的数据中心建在中国境外?

If your business is considered CII, all important data and personal information collected in China must be stored in China. Also, Article 31 of

the Cybersecurity Law encourages all network operators (not just CIIs) to store such data in China. In practice, this may mean that you will be obliged to maintain a data center in China.

IV. Network Products and Equipment 网络产品与设备

23. May I use foreign-made hardware and software? 外国制造的软硬件能否使用?

Yes. However, if the hardware or software constitute "critical network equipment" or "specialized network security products", then they will need to meet the requirements discussed in question 25 below before they can be purchased and used in China.

24. Can I still sell my technology products in China? 我还能在中国出售我的科技产品吗?

Yes. However, if the products fall under the category of "critical network equipment", "specialized network security products", or "products which may impact national security and are to be used by CII", then foreign technology products will need to meet the requirements discussed in question 25 below before they can be sold in China.

25. Are there any security review requirements for foreign-made hardware or software? 外国制造的硬件或软件有无进行安全审查的要求?

There are no requirements specifically targeting foreign hardware and software. However, Article 23 of the Cybersecurity Law specifies that "critical network equipment" and "specialized network security products" must "meet national standards, be certified by a qualified establishment, and meet the requirements of a safety inspection" before they can be sold or used in China. Further, when CII network operators purchase network products and services that might impact national security, these products and services must also pass the network security review.

The scope of critical network equipment and specialized network security products are set out below.

a. Critical network equipment

   (i) Routers

   (ii) Switches

   (iii) Servers (rack-mounted)

   (iv) Programmable logic controllers

b. Specialized network security products

(i) All-in-one data backup

(ii) Firewall (hardware)

(iii) Web application firewall

(iv) Intrusion detection system

(v) Intrusion protection system

(vi) Security isolation and information exchange products (gatekeeper)

(vii) Anti-spam email products

(viii) Network integrated audit system

(ix) Network vulnerability scanning product

(x) Security data system

(xi) Website recovery products (hardware)

The security review regime with respect to critical network equipment and specialized network security products under the Cybersecurity Law can be found in the Product Review Measures. The security review focuses on verifying that products and services are "secure and controllable" and are not a threat to national security. "Secure and controllable" is a concept that already exists under the National Security Law.

For the Product Review Measures, "secure and controllable" takes the form of a risk assessment, under which the following will principally be examined:

a. risk of the products or services themselves being unlawfully controlled, interfered with, or disrupted;

b. risk arising during the production, testing, delivery, and provision of technical support of/for the products and their key components;

c. risk of product or service providers illegally using products and services to collect, store, process, or use personal information;

d. risk of product and service providers taking advantage of users' reliance on the products and services to harm network security or the interests of users; and

e. risk that might endanger national security.

The review itself will also cover a review of the network security of the products and services and their supply chains, and use a combination of laboratory testing, on-site inspections, online testing, and background investigations.

Additionally, depending on the nature of the product, you may need to register the products with the various industry authorities. For example, the sale of specialized security products for computer information systems requires a license issued by the Ministry of Public Security.

26. Who will conduct the security review for network products and equipment? 谁来对网络产品和设备进行安全审查?

a. General Security Review

A tiered structure will be adopted to conduct the review:

(i) The CAC, together with other relevant departments, will establish a Network Security Review Committee, which will formulate policies on the security reviews, organize review efforts, and coordinate on key issues related to the security review;

(ii) The Network Security Review Office will organize the implementation of the network security reviews and form the Network Security Review Experts Panel; and

(iii) Third-party institutions and experts accredited by the Network Security Review Committee will carry out the actual assessments, while the Network Security Review Experts Panel will assess the security risks associated with the network products and equipment based on the accredited third party's evaluation.

b. CII Security Review

Various CII industry regulators, such as the China Insurance Regulatory Commission for the insurance sector, will conduct the security review of network products and securities used by CII network operators in the sectors which they regulate.

27. Under what circumstances are CII network products and services considered a danger to national security? 什么情况下 CII 网络产品和服务会被视为威胁国家安全?

The Cybersecurity Law and its existing implementing rules and regulations do not set out criteria as to the kind of CII network products and services that are considered a danger to national security. Rather, the specific criteria will likely be determined by the relevant industry regulators of CII.

Before the Cybersecurity Law, the main regulatory protection of national security focused on the unlawful disclosure of state secrets, with almost every department of the State Council having promulgated a scope of state secrets for their respective industry. In the absence of a statutory scope of "a danger to national security" under the Cybersecurity Law framework, we are of the view that the departmental rules on the scope of state secrets are a good source of reference as to what network products and services would be considered a threat to national security.

28. What is the difference between the previous grading and protection system and the grading and protection system under the Cybersecurity Law? 现行的等级保护制度与网络安全法下的等级保护制度有什么区别?

The pervious tiered protection system under the Administrative Measures for the Tiered Protection of Information Security ("**Information Security Measures**") applies to "information security", and does not cover more modern technology developments such as cloud computing. The Information Security Measures require companies operating and using information systems to self-grade themselves as tier one, two, three, four or five. Following the self-grading, the company must appoint a third-party organization recognized by the Ministry of Public Security to assist it to compile a tiered protection system grading report and conduct a subsequent evaluation.

Experts and academics consider that the Cybersecurity Law expands the existing grading and protection system to apply to "networks", with detailed implementation guidelines to be issued by TC260, for instance, the Information Security Technology – Implementation Guide for Cybersecurity Classified Protection (Draft for Comments) and Information Security Technology – Testing and evaluation technology guide for Cybersecurity Classified Protection (Draft for Comments).

29. Can I conduct the test overseas? 能否在国外进行检测?

The CAC will work with other departments of the State Council to promote mutual recognition of overseas security certificates and security tests to avoid duplication of certification and tests.

30. Will I need to disclose my source code to the Chinese government during the security assessments? 企业会否在安全检测过程中向中国政府提供产品源代码?

It is not clear at this stage whether source code will need to be disclosed. However, we are of the view that in most cases, the source code will not need to be disclosed for a security assessment. However, if the industry regulator or CAC involved in the security assessment forms the view that the network product or equipment might affect national security, then it is quite possible that source code will need to be disclosed.

31. Will the requirement for "secure and trusted" network products interfere with the commercial interests of foreign-invested companies in China? 网络产品"安全可信"的要求是否会限制在华外商投资企业的商业利益?

The CAC has stated that the purpose of implementing the security reviews is to improve user confidence and promote the expansion of high-quality products in the market and that foreign and domestic business will be treated equally under the review. Therefore, the requirement will hopefully, in practice, not interfere with the commercial interests of foreign-invested companies.

V. VPN

32. May I use a VPN provided by a foreign VPN provider? 能否使用境外 VPN 服务商提供的 VPN?

No. Chinese companies (whether domestic or foreign-invested) are not permitted to use or rent unauthorized VPNs or use other software or methods which are aimed at illegal cross-border access to the internet without approval from the Ministry of Industry and Information Technology ("**MIIT**"). The prohibition is set out in the Circular on Clearing up and Regulating the Internet Access Service Market, issued on 17 January 2017 ("**VPN Circular**"). Currently, only local VPN providers like China Telecom, China Mobile, and China Unicom, are authorized VPN providers.

VI. Latest enforcement 最新执法情况

33. Who enforces the Cybersecurity Law? 网络安全法由谁实施?

Enforcement is led by the CAC, together with industry regulators (e.g., China Insurance Regulatory Commission for the insurance sector, and the China Banking Regulatory Commission for the banking sector). The State Administration for Industry and Commerce will also assist with enforcing penalties such as the confiscation of illegal earnings and the suspension of business.

34. What are the penalties or sanctions for a breach of obligations under the Cybersecurity Law? 违反网络安全法义务会受到何种惩罚或制裁?

Penalties for non-compliance with the Cybersecurity Law include temporary suspension of operations, closing down of websites, fines, and revocation of operation permits and the business license.

35. Can the legal representative or any company personnel be imprisoned for non-compliance? 公司法定代表人或人员是否会因不合规而面临牢狱之灾?

Yes.

a. Criminal Law

The legal representative and/or other staff members might face the risk of imprisonment under the Criminal Law of China if a company:

(i) unlawfully cancels, alters, or jams the functions of the computer system, thereby making it impossible for the system to operate normally;

(ii) fails to perform its obligations as a security manager;

(iii) unlawfully uses the Internet to commit a crime under the Criminal Law of China; or

(iv) offers an individual access to the internet, or technical support, to commit a crime.

b. Cybersecurity Law

If a company is found to be in violation of the Cybersecurity Law, such as by providing technical support which endangers cybersecurity, then the persons directly in charge and other directly-responsible personnel of the company can be detained by the local public security bureau for up to 15 days. If the unlawful activity threatens national security, then the individual may be detained by the national security bureau.

36. Will a violation of the Cybersecurity Law be recorded in the credit archive? 违反网络安全法的行为是否会记入信用档案?

Yes. Article 71 of the Cybersecurity Law states that any violation of the Cybersecurity Law will be recorded in the credit archives and made public.

The "credit archive" referred to in the Cybersecurity Law, although not expressly specified, most likely includes the basic database of financial credit information maintained by the People's Bank of China. This means that failure to comply with the Cybersecurity Law may reduce a company's creditworthiness and may cause it difficulties when trying to take out a loan from a Chinese domestic bank.

VII. Miscellaneous 其他

37. Will I be required to give the Chinese government access to my data? 我是否需要向中国政府提供我的数据?

You will have to give the Chinese government access to your data in the event of any of the following:

a. during a cross-border data transfer security assessment;

b. in responding to any request from the CAC, or any other competent authority, to conduct inspection and supervision of a network operator pursuant to Article 49(2) of Cybersecurity Law; and

c. when coordinating with the competent authorities for supervision and inspection matters, and the provision of technical support or assistance to the public security and national authorities under Article 28 of the Cybersecurity Law.

If your data is encrypted, you will need to decrypt the data and allow the Chinese government access to the data if so requested. This is because Article 49 of the Cybersecurity Law imposes a statutory obligation on network operators to cooperate with governmental authorities.

38. What other developments are anticipated? 其他法律法规还有何进展?

There are several measures likely to come into force in the near future:

a. Draft Information Security Techniques and Personal Information Security Specifications, which has been circulated for public comment and is expected to be issued soon. The core focus of this specification is the protection of personal information. The specifications aim to address the security of personal information during the rapid development of IT.

b. Draft Regulations on the Protection of the Use of the Internet by Minors, which was circulated for public comment in January 2017. This draft provides for censorship of certain content the State deems unsuitable for minors (defined under the Minor Protection Law as persons under the age of 18); for example, content that would encourage minors to take up smoking.

c. The Draft Encryption Law, which was circulated for public comment in April 2017. This law is the first statute in China to comprehensively address encryption. It would also regulate "the research, production, management, import and export, testing, authentication, use, and administration of encryption".

d. The Draft Regulations on the Implementation of the Law on the Protection of the Rights and Interests of Consumers, which was circulated for public comment on 16 November 2016. This draft reiterates and supplements data privacy and security obligations imposed by existing consumer laws – namely, the Law on the Protection of the Rights and Interests of Consumers and the Measures on Penalties for Infringing Upon the Rights and Interests of Consumers. For example, the draft clarifies that business operators must retain proof, for at least 3 years, that they have obtained consent from users before collecting and using their personal information; and

e. Draft E-Commerce Law was circulated for public comment on 27 December 2016. This draft would regulate both domestic and cross-border e-commerce activities. The draft also sets out specific obligations on e-commerce operators. For example, persons engaged in e-commerce activities must provide accurate information when registering with a platform, and platform operators must safeguard the personal information of individuals.

39. Is there a grace period for implementing the data transfer? 实行符合新规的数据传输之前是否存在宽限期?

Yes. The Draft Data Transfer Measures provide a grace period for companies to comply with the rules and enforcement. If the Draft Data Transfer Measures are issued in their current form, then the grace period will end on 31 December 2018.

40. How should I proceed? 应该如何应对?

a. Critical Equipment and Security Products

Companies are advised to work closely with their IT specialists and legal counsel to keep abreast of the changes to the legal framework regulating cybersecurity and examine their network products and services (whether for sale or purchased) to ensure that they comply with the Product Review Measures.

b. Data Security

Companies should also (1) review their global data security and privacy policies and procedures and identify the ones that need to be localized, and (2) review their global data security and privacy training materials and draft or localize training materials for Chinese employees to ensure awareness of data security and protection policies and procedures.

c. Personal Information and Cross-Border Transfer of Data

Companies are advised to:

(i) review their current data security and privacy policies regarding the collection and use of personal information and, check whether adequate notice has been given to users and proper consent has been obtained;

(ii) create a list of identifiers for personal information and important data mapping, including where and how personal information is stored, and which third parties may be provided personal information;

(iii) review and update existing agreements, employment contracts, and privacy policies and update them so they comply with the existing Chinese law requirements.

d. Other Obligations

Since the Cybersecurity Law was implemented on 1 June 2017, the CAC has penalized several companies that failed to properly conduct a tiered protection evaluation. Thus, it appears that compliance with the grading and protection system under the Cybersecurity law may be the CAC's initial focus.

Until the relevant regulating authorities are specified and more guidance is given on how to comply with the state's "tiered system of network security protections," companies are strongly advised to take adequate steps to implement as many of the outlined precautions as possible, taking into account the amount and types of data involved.

41. How will it affect me? 有何影响?

We set out below the main ways in which foreign business will be affected:

a. Foreign-invested companies in China must pro-actively protect users' personal information. Very likely this means higher costs for compliance reviews, implementing new procedures (especially regarding consent) and systems to offer adequate protection of personal information and networks from security breaches, training employees on how to monitor and ensure compliance with the Cybersecurity Law and, obtaining security certifications from the relevant authorities.

b. The data localization requirement and data transfer restrictions means that foreign-invested companies which qualify as CII operators and whose business requires the transmission of personal information and important data to servers based outside China will have to store such data in China (which can be very costly) or sub-contract these services to a third-party service provider in China. Other network operators will need to ensure they conduct security assessments in full compliance with the Cybersecurity Law and its implementation regulations before transferring any personal information and important data outside of China.

c. The obligation to cooperate with state security services and other government authorities to report and investigate cybercrimes and clear security assessments (in the case a company wishes to sell network security products and equipment or transfer personal information or important data out of China), raises concerns about possible infringement of trade secrets and intellectual property rights. As mentioned in question 0 above, companies may be required to disclose data to the Chinese government.

42. How will the Cybersecurity Law affect businesses which rely/use cloud computing? 网络安全法将如何影响依赖/使用云服务的企业?

Any company running such businesses, if categorized as a CII, and if the business involves the collection of personal information and important data in China, will be required to move its data server to China and conduct a security assessment with the relevant industry regulator before transferring data overseas.

****