China’s Cybersecurity Law enforces the cybersecurity rights and obligations of the government, network operators and users. Compliance with the new law has presented a range of new challenges for both businesses and individuals. In order to protect the rights of all stakeholders, it will be essential to ensure appropriate network operations, encourage network innovation, identify security risks and comply with regulation requirements.

All organisations collecting ‘personal information’ and ‘critical data’ in China could be impacted, including:

1. **Network operators.** The law enforces the security obligation of network operators, which are widely defined to include owners, administrators and operators of telecommunication/ information networks. This includes, but is not limited to, telecommunication operators, network information service providers, and important information system operators.

2. **Network product and service providers.** Organisations that provide information through networks or provide services for the purpose of obtaining information, including, users, network service providers and non profit organisations which provide network tools, devices, information, media, access, etc.

3. **Critical infrastructure operators.** The law specifies requirements related to the operational security of critical infrastructure operators, and stresses the importance of protecting critical infrastructure of public communication, media, energy, transportation, water conservation, financial services, public services and e-government industries.

4. **Overseas organisations and individuals.** Include but not limited to foreign trade enterprises, organisations, groups and individuals.
**Key challenges**

Enterprises will face more challenges to comply with the law and detailed regulations, especially as the scope has widened to span network operation security, content security, network monitoring and incident response reporting to authorities. Some initial challenges include:

1. Increased obligations to adhere to the law and appropriate business ethics, safeguarding network security, cooperating with inspections and undertaking social responsibilities.

2. More stringent regulations and requirements will be applied. For instance, security assessment is required prior to the transfer of cross-border personal sensitive data.

3. Organisations and individuals (including those from foreign countries) found guilty of attacking China's critical infrastructure are subject to punishment specified by the law.

4. Government authorities will have the right to take measures to shut down or limit network communications in the event of significant security emergencies.

5. What will become prohibited? With the new Cybersecurity law taking effect on 1 June 2017, the transferring/storing of personal data outside China and using network and password equipment not certified by the government will be prohibited.

**What are the penalties incurred?**

Organisations found violating the law will be subject to fines, with the responsible management/individuals subject to imprisonment and banned from taking network security and operation management positions in the future.

**Next steps**

Moving forward, organisations will need a pragmatic and customisable approach that enables them to effectively manage and complete the necessary activities required. Prior to the issuance of more detailed regulations which will provide more clarity, you can start asking yourself the following questions to aid your preliminary preparation:

- **Compliance and risk management status**
  - Do you fully understand your organisation’s compliance status? Where and how could you minimise gaps between your current cybersecurity compliance and the new China Cybersecurity law?
  - Do you use third parties for any important businesses and/or processes, and fully understand the risks?

- **Data & privacy protection mechanism**
  - Where does your company store critical business and personal information?
  - Is the data protection mechanism safe?
  - Is the collection of personal information treated appropriately?

- **Equip your employees**
  - Do you have regular communications and workshops to improve your company employee’s technical knowledge and security awareness?
  - Do your communications include hot topics such as email cloud computing, social media, mobile, big data, etc.?

- **Incident response mechanism**
  - Do you know what you need in order to adequately strengthen your network security monitoring and incident response mechanism?

- **System vulnerability**
  - Is your cybersecurity defense infrastructure able to machine learn and provide predictive analytics to quickly and accurately identify problems and provide solutions that protect your organisation from vulnerabilities and impacts from IT failures?
We will be publishing a series of articles to provide guidance regarding the new China Cybersecurity Law as more detailed regulations unveil.

**Speak to our team today**

We will ensure knowledge transfer so that your team can build and operate a sustainable process going forward.

You may choose any combination of our service components to meet your specific requirements.

An effective approach to help you throughout the preparation process to get ready for the new cybersecurity law in China.

---

**China North**

**Samuel Sinn**
+86 (10) 6533 2937
samuel.sinn@cn.pwc.com

LinkedIn

**China Central**

**CY Cheung**
+86 (21) 2323 3927
chun.yin.cheung@cn.pwc.com

LinkedIn

**China South**

**Shenzhen / Guangzhou**

**Kok-tin Gan**
+852 2289 1935
kok.tin.gan@hk.pwc.com

LinkedIn

**Hong Kong**

**Kenneth Wong**
+852 2289 2719
kenneth.ks.wong@hk.pwc.com

LinkedIn

**Marin Ivezic**
+852 2289 1817
marin.ivezic@hk.pwc.com

LinkedIn

**Legal Services**

**Jenny Zhong**
+86 (10) 6533 2908
jenny.j.zhong@cn.pwclegal.com

---

PwC’s professionals truly understand business and trends as they relate to cybersecurity and convey the IT and technology requirements to decision-makers.

**Kennedy Cybersecurity Consulting Report, Q4 2015**

PwC rated as a leader in Independent Information Security Consulting Services

**Report by Forrester, Q1 2014**

• Our team is comprised of professionals with expertise spanning multiple disciplines bringing substantial knowledge and experience from across the entire Cybersecurity lifecycle – from assessment, strategy and design to implementation including data privacy, outsourcing and offshoring, regulatory compliance, technology and operations, risks and controls. Our team can help you expedite the preparation process to meet the new cybersecurity regulations.

• You may choose any combination of our service components to meet your specific requirements.

• An effective approach to help you throughout the preparation process to get ready for the new cybersecurity law in China.

---

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