

# China Cybersecurity Law. A bigger change than Y2K?

The paradigm-shifting compliance requirements of Cybersecurity Law present unprecedented challenges for financial institutions with operations in China. Are you ready?



The better the question. The better the answer.  
The better the world works.





For financial institutions with a footprint in the nation, China's first comprehensive privacy and security regulation for cyberspace will require the type of all-system response last seen in the late '90s as companies worked feverishly to upgrade computers and application programs to be Y2K-compliant.

The global Y2K effort, which costs USD\$300B, was considered a one-off, never-to-be-repeated event. But, for those who went through Y2K, China's Cybersecurity Law is creating flashbacks.

For foreign institutions operating in China and local institutions with overseas operations, Cybersecurity Law is raising major concerns about the amount and cost of the work required to assess all computer systems to ensure compliance.



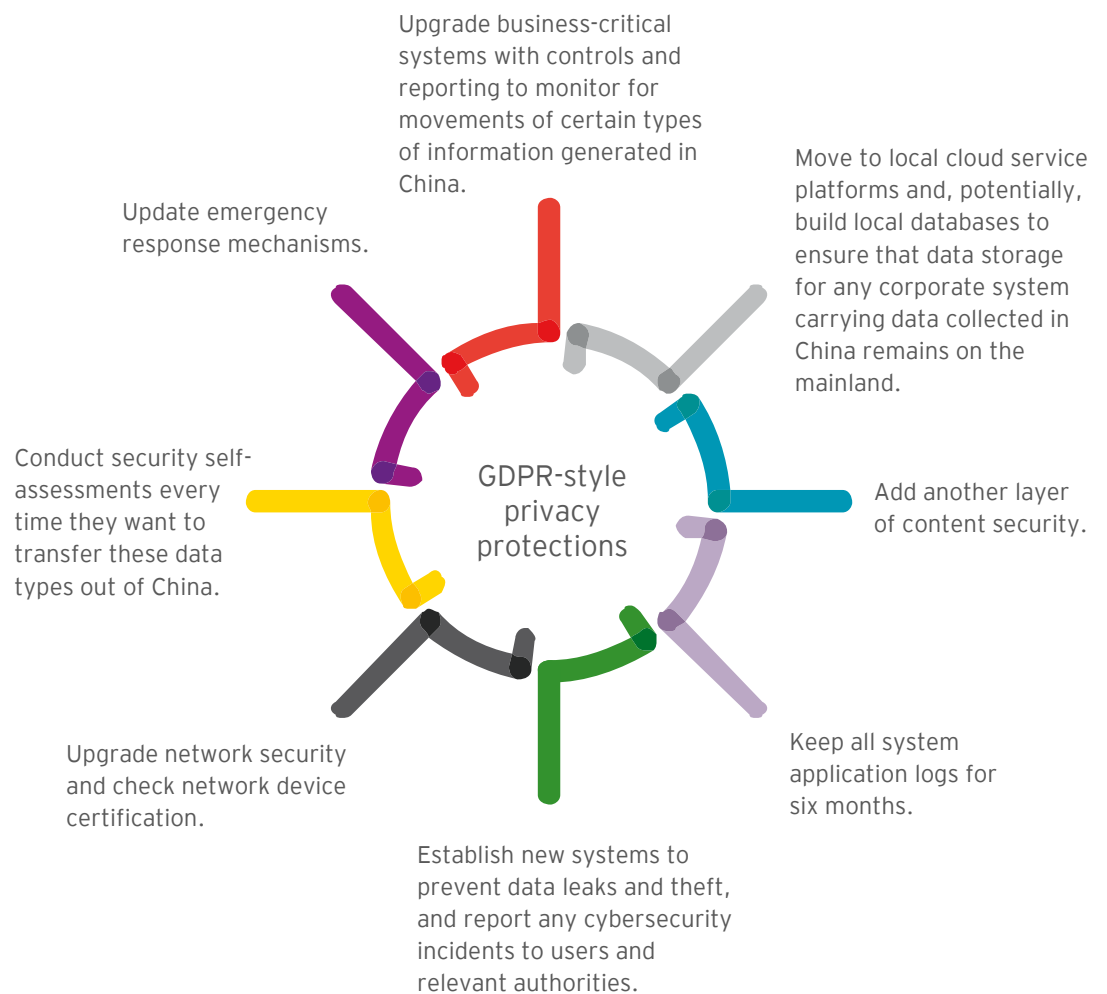
## What are the immediate implications of the Cybersecurity Law for financial institutions?

### *Seeing the scale and scope of the issue*

Unlike the China Great Firewall, which controls external information inflow into China, Cybersecurity Law is designed to protect data outflow. The law, which is still evolving, applies to operators of critical information infrastructure, putting financial institutions firmly in its scope.

Together with a dozen other related legislations, guidelines, and industrial standards already released or being drafted, the principles-based Law establishes a range of new responsibilities for financial institutions.

In addition to GDPR-style privacy protections, its long and growing list of measures, standards and compliance requirements mean that any financial institution with operations in China may need to:



## Why is complying with Cybersecurity Law so challenging?

### *Understanding China's approach to cybersecurity*

Cybersecurity Law reflects the broader global trend to regulate cyberspace activities and counteract cyber threats that could undermine public security. Part of its purpose is to bring China in line with global best practices for cybersecurity. But it does more than that. It's also designed to exert jurisdictional control over data and content generated in China - to strongly assert, "within Chinese territory, the Internet is under the sovereignty of China".

This means Cybersecurity Law comes with an overlay of a specifically Chinese nature, with implications that most Western companies would take time to be familiar with. Compliance will require financial institutions to radically change the way they collect, store, transmit and use data that is generated in China. For example, it:



#### Introduces new data categories

Cybersecurity Law focuses on the nature of flow of information generated in China, with a strong emphasis on, not just "personal information", but "important data" - a new category of data for Western enterprises. China regards information to be "important" if it relates to anything likely to affect national security, the broader economy or the public interest.

Important data will be different in different industries. For financial institutions, it's likely to cover business transaction data with material impact to the macro economy. But in China, what constitutes important information is likely to be decided by the authorities on a case-by-case basis.



#### Introduces a data localization requirement

Financial institutions now have to locally store any "personal information" and "important data" collected within China, unless the business passes the Government's security assessment. To avoid violating this requirement, institutions that currently transmit data to overseas headquarters will need to restructure their mechanisms regarding data transfer, building in mechanisms to perform the necessary assessment. The criteria for security assessments are still being developed.



#### Comes with strict and wide-ranging requirements

Cybersecurity Law extends to information security, communication security, computer security, automation and control system security. And its requirements drill right down to the network hardware level. Certain network equipment and cybersecurity products must be certified by a qualified establishment and found to be in compliance with national standards.

Adding to the challenge, China's legislative and enforcement style - which is written in Chinese, principles-based and involves elements of judgment in its application - means Cybersecurity Law could be complicated for and easily misunderstood by Western companies.

## Adapting to operate under China's Cybersecurity Law

### Responding appropriately to the new compliance requirements

Depending on the maturity of existing network security, complying with Cybersecurity Law will require most financial institutions to:



#### 1 Strengthen network security

Current network security devices may not effectively and efficiently provide the level of network security required under the Law. Institutions will need an orchestrated approach to:

- a. Put the right "gates and surveillance" at the application and network architecture levels
- b. Standardize and simplify technology stacks
- c. Centralize the flow of data packets to provide a complete and transparent view
- d. Use security orchestration automation and response (SOAR) tools to pull all the security logs together, diagnose genuine threats and respond quickly
- e. Create a business-oriented scorecard so executives can visualize threats and attacks

2



#### Introduce content security

Institutions need to start monitoring the information in their networks for restricted content. All text, audio and video content has to be screened for messages deemed inappropriate. Illegal content must then be removed, recorded and reported. For institutions that record broker-to-client phone calls as part of their advice audit trail, this is already creating enormous challenges.

3



#### Establish new security audits

Institutions must conduct regular audits of cyber-technology systems and processes, including emergency response protocols. The Law includes specific requirements for emergency response that go above and beyond the standard incident response capabilities in most cybersecurity practices.

4



#### Protect personal information

Institutions collecting customer information must obtain consent, tell customers about the information's intended use, notify the Government of breaches and delete or amend personal data on the user's request.


5



#### Minimize cross-border data transfer

Multinationals with centralized CRM, HR, procurement or other critical business systems will need a strategy for dealing with the data that flows to these central hubs. Some institutions are already considering building local data centers or moving to cloud-based services hosted on China-based data centers.





Even though Cybersecurity Law is still evolving, the Chinese authority has already begun initiating enforcement actions for violations, including fines of up to RMB 500,000, business license suspensions and detention.

As a priority, financial institutions need to assess the gaps between the Law and their current operations and create a plan to close these gaps based on the quantum of risk attached to each exposure.

Don't be surprised if the body of work eclipses that required for Y2K.

---

**China's Cybersecurity Law requires far-reaching change. Financial institutions need to assess their exposure now and begin the complex transition.**

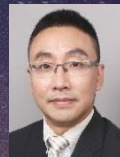
---

## Contacts



**Sherman Leung**

Partner, Risk Advisory Services  
FSO Advisory Risk Leader  
Greater China  
+86 10 5815 3236  
sherman.leung@cn.ey.com



**Wilson Feng**

Partner, Risk Advisory Services  
FSO Advisory Risk  
Greater China  
+86 21 2228 6855  
wilson.z.feng@cn.ey.com

EY | Assurance | Tax | Transactions | Advisory

**About EY**

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit [ey.com](http://ey.com).

© 2019 Ernst & Young, China  
All Rights Reserved.

APAC no.03007806  
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

[ey.com/china](http://ey.com/china)

**Follow us on WeChat**

Scan the QR code and stay up to date with the latest EY news.

