CYBERSECURITY LAW CHINA

December 2019

START

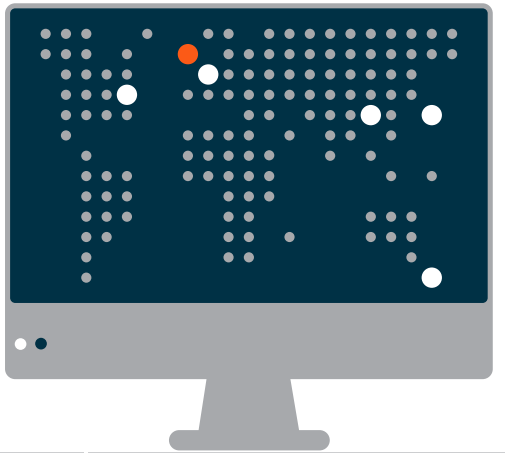
Osborne Clarke

Introduction – Doing business in Asia

Cybersecurity regulations in China and Hong Kong SAR: Risk management and governance issues and compliance for businesses

On 1 June 2017, China implemented The Cybersecurity Law of the People's Republic of China ("The Cybersecurity Law"), providing heightened regulatory oversight over the Internet network domain for mainland China. Issued as a milestone foundational guidance law, The Cybersecurity Law embodies the Chinese government's mission to reinforce China's cybersecurity standards amid rapid changes in the international geo-political cybersecurity environment.

Over the last two years, a variety of public consultations have led to the enactment and publication of further and more detailed implementing legislation and clarification, with more expected to follow. In the light of the more recent implementations coming into force, we are here to recap and look forward in our comprehensive overview for anyone undertaking or considering business activity in China and Hong Kong.



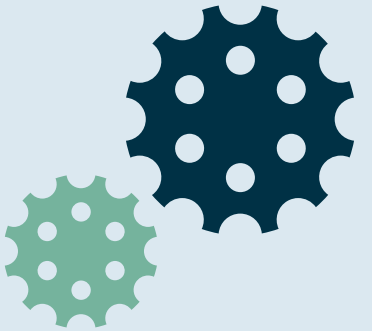
Introduction – Scope of The Cybersecurity Law

The Cybersecurity Law applies to the construction, operation, maintenance and use of information networks, and the supervision and administration of cybersecurity in China.

As with many other key Chinese laws, The Cybersecurity Law has a complicated structure and introduces a pyramid of implementing regulations and measures, guidance notices, national and technical standards, with high-level general legal principles in its core text. The Chinese government has issued multiple auxiliary and supporting regulations, specifications and measures to facilitate the implementation of The Cybersecurity Law. These include the Information Security Technology – Personal Information Security Specification (the "Specification"), and drafts of the Regulation on the Protection of Critical Information Infrastructure, Measures on Cybersecurity Review and the Measures on Security Assessment of the Cross-border Transfer of Personal Information (the "Draft Measures").

However, the Cybersecurity Law, the Specification and the Draft Measures do not apply to Hong Kong, which is a Special Administrative Region of China, operating under the "one country, two systems" principle. Hong Kong does not have specific cybersecurity legislation, but the issues around cybersecurity are addressed under Hong Kong's Personal Data (Privacy) Ordinance (Chapter 486, Laws of Hong Kong) insofar as they relate to personal data.

All businesses – from multi-nationals looking to expand or operate in Hong Kong and/or China, 'to local' Hong Kong or mainland China companies looking to trade or operate in the other jurisdiction – will need to be aware of and comply with the applicable China and Hong Kong cybersecurity regimes. To this end, we explore the key elements of The Cybersecurity Law, and compare and contrast significant concepts with the Hong Kong-equivalent regime from a business risk management and internal risk governance perspective.



Why should businesses care about The Cybersecurity Law?

The Cybersecurity Law broadly imposes data-privacy obligations on all network operators[1], critical information infrastructure[2] operators and network products and services providers in China.

In addition to covering entities which operate and provide network services in a conventional sense (for example, telecommunications service providers), it is likely to be treated as extending to entities administering or managing network systems, such as Internet businesses operating and providing services through websites and online credit banking institutions. The data-privacy obligations of The Cybersecurity Law apply to all organisations in China that provide services over the Internet or an information network (including, arguably, internal networks and systems). This means The Cybersecurity Law has a very wide ambit and is capable of applying to almost all business operations involving such networks in China.

The Cybersecurity Law defines "personal data" as information that identifies a natural person either by itself or in combination with other information. Examples include an individual's name, address, telephone number, date of birth, identity card number and biometric identifiers. The Cybersecurity Law now regulates the collection, use, processing, storage and security of such personal data by network operators, critical information infrastructure operators and network products and services providers in China.

The Cybersecurity Law adopts a gradated-protection approach depending on the "significance" of entities. In addition to standard security measures adopted by network operators, critical information infrastructure operators must adopt data localisation (for personal data and important data[3] collected and generated during operations in China) and conduct an appropriate security assessment prior to any cross-border transfer of data. Government guidelines on how "critical information infrastructure" is classified and how a security assessment should be conducted have been issued in separate regulations and measures. Businesses should be aware of these obligations as they have evolved, and are likely to continue to evolve.

Moreover, the imposition of the security assessment requirement seems likely to impact cross-border data flows with raised levels of uncertainty and compliance costs. The proviso that network operators are encouraged to comply with these requirements voluntarily means they should closely monitor how these requirements evolve.

1. "Network operator" is defined as "network owner, manager and network service provider". Network is defined as "a system comprised of computers or other information terminals and related equipment that collects, stores, transmits, exchanges and processes information in accordance with certain rules and procedures".

2. "Critical information infrastructure" is not defined in The Cybersecurity Law. Some examples given include public communications, information services, energy, transportation, water resources, finance, public services and electronic governmental affairs. The draft *Regulation on the Protection of Critical Information Infrastructure*, published by the Cyberspace Administration of China in July 2017, provides guidelines on the identification of "critical information infrastructure".

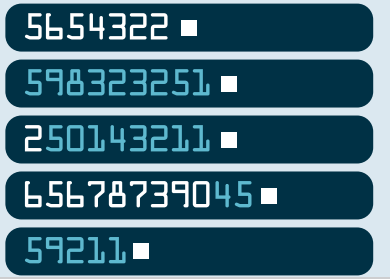
3. "Important Data" is not defined in The Cybersecurity Law. However, the identification of "important data" is explained in the draft Measures for Personal Data and Important Data Cross-Border Transfer Security Assessment published by the Cyberspace Administration of China in April 2017, and the draft Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment published by the National Information Security Standardisation Technical Committee in May 2017.

Why should businesses care about The Cybersecurity Law?

The Draft Measures issued by the Cybersecurity Administration of China in 2019 have introduced a broad jurisdictional scope for regulating cross-border transfers of personal information: all network operators are obliged to undergo the security assessment process before they may transfer personal information collected in the course of their operation in China to recipients outside the country.

Penalties for contravening The Cybersecurity Law in serious cases could be hefty. These include maximum fines of RMB 1 million and orders to suspend business; suspend certain operations and undergo rectification; shut down websites; or revoke business permits or licences. There are therefore clear incentives for businesses to implement measures and controls to avoid contraventions in the first place.

With increased commercial activities and interaction between China and Hong Kong and more multinationals looking to operate in both territories, businesses will benefit from familiarity with the Chinese government's regulatory approach towards Internet network regulation as illustrated by The Cybersecurity Law, as well as the equivalent Hong Kong privacy and cybersecurity regime.



Key Aspects – Regulatory approach and structure

Regulatory approach and structure

The Cybersecurity Law aims to build cybersecurity capability and impose obligations on stakeholders within the cybersecurity community. Mobilising resources and personnel on national and local levels, it requires cooperation by all stakeholders in safeguarding cybersecurity, ranging from the state, provincial and local government, industry and business to individuals.

The Cybersecurity Law adopts a three-pronged regulatory approach based around "Prevention, Control and Penalty":

Prevention	**Part two** Cybersecurity support & promotion	Specifies how the state, provincial and local governments should reinforce cybersecurity through support and promotion
Prevention and control	**Part three** Security of network operations **Section one** General provisions **Section two** Security of the operation of critical information infrastructure	Section one details measures covering network operations and product and service security to be implemented by network and critical information infrastructure operators and network-products-and-services providers for cybersecurity protection, defence and monitoring. Section two specifies further security requirements to be adopted by critical information infrastructure operators including data localisation and security assessment
Prevention and control	**Part four** Security of network information	Cybersecurity includes not only security of network operations but also security of network information, which includes personal data Light input on principles of personal data
Prevention and control	**Part five** Monitoring, early warning & emergency handling	The state, provincial and local government and network operators are to coordinate to monitor, gather intelligence and issue early warning on potential cybersecurity incidents, and devise emergency response plans to handle cybersecurity incidents
Penalty	**Part six** Legal liability	Penalties for breaching The Cybersecurity Law

Key Aspects – Main Requirements and Impact on Business Risk Management and Internal Governance

1. Network Operations Security Requirements

Network operators must:

- adopt the following security measures to prevent network interference, damage or unauthorised access, and prevent network data from leakage, theft or alteration:
  - set up an internal security management system and designate personnel responsible for its operation
  - adopt technical measures to prevent computer virus and network attacks or interference
  - monitor and record network operation and cybersecurity incidents, keeping records for at least six months
  - conduct data classification, backing up and encrypting important data
- formulate cybersecurity emergency response plans and handle security risks on a timely basis, such as when cybersecurity incidents happen, initiate the response plan, take remedial actions and report to the relevant competent department[4]
- provide technical support and assistance to law enforcement and national security agencies on national security and crime investigation

Note

The Chinese government encourages network operators that fall outside the scope of critical information infrastructure to voluntarily participate in this regime.

Critical information infrastructure operators must:

- adopt the following further security measures (in addition to security measures above):
  - designate responsible personnel for security management and conduct background checks for them
  - regularly conduct cybersecurity education, technical training and skills assessments for employees
  - implement disaster recovery backup plans for important systems and databases
  - formulate cybersecurity emergency response plans and conduct regular drills on those plans
- conduct internal and external network security risk assessments at least once a year and report outcomes and improvement measures to the relevant competent department
- comply with measures coordinated by the Cyberspace Administration of China including:
  - random testing of security risks of critical information infrastructure
  - regular conduct of cybersecurity emergency drills to raise response level and collaboration ability

Impact on business risk management and internal governance

- **Businesses should review and ensure that their network systems, security measures, controls, personnel and resources are in place and adequate to comply with legal requirements**
- **If necessary, businesses should correspondingly update their security measures to be capable of dealing with and protecting against the latest forms and trends of cybersecurity attacks**
- **Businesses should ensure they fulfill the six-month requirement of keeping records on network operation and cybersecurity incidents**
- **Businesses should consider how to reconcile data privacy concerns in product design and controls with the legal requirement of providing support to law enforcement and national security agencies**

4. This may create complications for businesses as The Cybersecurity Law does not give clear guidance on how businesses can identify a relevant competent department.

Key Aspects – Main Requirements and Impact on Business Risk Management and Internal Governance

2. Product safety and certification

Network products and services providers must:

- not insert malicious programmes
- when discovering safety loopholes and risks in network products and services, promptly take remedial actions[5] and notify users and the relevant competent department in time
- only sell or provide network critical equipment and network safety specialised products after obtaining security certification from or passed security testing by qualified institutions[6]

Critical information infrastructure operators must:

- when procuring network products and services which may impact national security, submit the products and services to Cybersecurity Administration of China and the State Council departments for a review for national security purposes

Impact on business risk management and internal governance

- **Businesses should arrange for internal checking of network products and services to remedy loopholes and arrange for network critical equipment and network-safety-specialised products to obtain security certification or pass security testing**
- **Businesses should draw up corporate guidelines to decide when network products and services may potentially impact national security requiring a review for national security purposes**

5. This may create complications for businesses as The Cybersecurity Law does not specify what kinds of remedial actions businesses should take.

6. The Cybersecurity Law does not specify a list of qualified institutions. However, the Certification and Accreditation Administration of the People's Republic of China and the Cyberspace Administration of China have jointly published the *Circular Concerning the Implementation of Safety Certification Requirement for Network Critical Equipment and Network Safety Specialised Products* in May 2018, to specify a list of qualified institutions.

Key Aspects – Main Requirements and Impact on Business Risk Management and Internal Governance

3. Information Monitoring and Intelligence Gathering

- **Network operators** are required to monitor information posted by users. If information is posted or transmitted in contravention of Chinese laws or administrative regulations, network operators should immediately cease the transmission, delete the information and prevent spread of the information. They should keep records and report any such occurrence to the relevant competent department
- Individuals or organisations transmitting electronic information in China or providing applications for use within China are prohibited from inserting malicious programs therein and are obliged to ensure that such programs do not contain any information contravening Chinese laws or administrative regulations. If **Electronic information sending service providers and application software download service providers** discover such occurrence, they should immediately cease providing service to the user; delete such information; and keep records of and report such occurrence to the relevant competent department
- **Network operators** are required to set up a cybersecurity complaints and reporting system, to publicise rules for making complaints and reports, and to handle such reports and complaints on a timely basis

Impact on business risk management and internal governance

- **Businesses should set up an effective information monitoring system and keep records of any offensive data detected and handled. They should also dedicate personnel and system resources to perform automated or manual checking of information which should guarantee effective and accurate detection of offensive data. Businesses should consider how best to reconcile this with privacy regulatory requirements. For example, in the Specification[7], businesses are required to minimise the data collected, notify individuals of the purposes of data collection and use, and obtain individuals' consents when collecting their data. Yet, businesses' efforts to monitor individuals and collect their information may conflict with such privacy requirements**
- **Businesses should set up an effective system to receive and handle complaints and reports, and should conduct staff training to facilitate the smooth operation of the system**

7. Published by the National Information Security Standardisation Technical Committee.

Key Aspects – Main Requirements and Impact on Business Risk Management and Internal Governance

4. Monitoring, Early Response and Emergency Handling

- The Cyberspace Administration of China and relevant departments for protecting critical information infrastructure are mandated to arrange to set up a comprehensive security risk assessment and emergency handling mechanism and/or formulate a cybersecurity emergency response plan and conduct regular drills.
- Government authorities at provincial level or above are obliged to:
  - require relevant departments, institutions and personnel to do real-time gathering and reporting of incidents information and strengthen monitoring of network cybersecurity risk
  - coordinate relevant departments, institutions and professionals to analyse cybersecurity risk and predict the possibility, impact scope and risk level if an incident happens
  - release early cybersecurity risk warnings to society, along with potential mitigating measures to take
  - after any cybersecurity incident, initiate an emergency response plan, investigate and assess the incident, and then ask **network operators** to take technical and necessary steps to remove the risk and warn the public

Impact on business risk management and internal governance

- **Businesses should coordinate with relevant stakeholders to devise systems to gather intelligence and share information, and consider how to reconcile this with privacy regulatory requirements, which require data minimisation, transparency and notification for collection and use of data**
- **Businesses should draw up and test the efficacy of their cybersecurity response plans, conduct regular reviews of those plans and implement drills to prepare for cybersecurity incident emergency handling. In doing so, they should dedicate adequate resources and staff training to facilitate smooth implementation of those plans. Businesses should refer to the Specification which provides a set of remedial actions in the case of a cybersecurity incident**

Key Aspects – Main Requirements and Impact on Business Risk Management and Internal Governance

5. Data Localisation

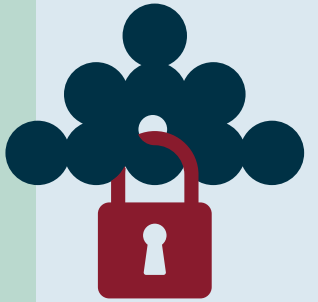
- **Critical information infrastructure operators** collecting and generating personal data and important data during their operations in China must store such data within China
- If it is necessary to provide any of this kind of data to any overseas party due to business needs, these operators are required to conduct a security assessment, following the measures stipulated by the Cyberspace Administration of China and relevant State Council departments. If other Chinese laws or administrative regulations provide otherwise, these provisions must be followed

Note

The Chinese government encourages network operators falling outside the scope of critical information infrastructure to voluntarily participate in this regime.

Impact on business risk management and internal governance

- **Businesses should review and seek specialist advice on the separate regulations and measures issued by the Chinese government on how critical information infrastructure and important data is classified and will be interpreted in relation to their own activities, to determine whether and if so to what extent they need to comply with data localisation. If applicable, they should:**
  - **prepare for data localisation by transferring the relevant data back into China (for example, storing data in China's data centres)**
  - **review their external data flows inventory and determine which data flows will be subject to the requirement for security assessment**
  - **review the government's guidelines for security assessment (as these may be revised from time to time) and ensure familiarity with the required procedures**
  - **Network operators should also keep an eye on the evolution of the Draft Measures which have brought the network operators into the scope for regulating the localisation and cross-border transfers of personal data**



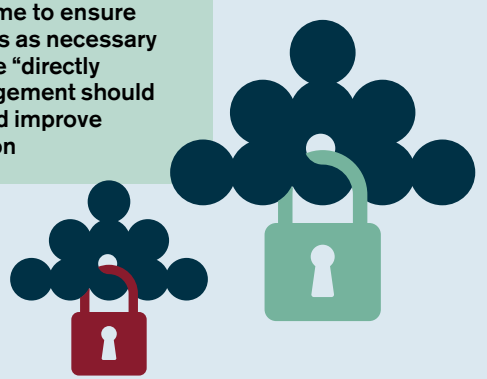
Key Aspects – Main Requirements and Impact on Business Risk Management and Internal Governance

Penalties for 1 - 5 above

- Penalties may range from a rectification order, warnings, and/or confiscation of profits to fines against operators or providers and/or directly responsible persons (the maximum fine is RMB $1 million)
- For serious cases, there may be orders to suspend business, suspend operations, undergo rectification, shut down websites or revoke any business permit or licence

Impact on business risk management and internal governance

Given there may be significant disruptive impact on business operations where cases are considered serious, businesses should proactively review their internal corporate governance regime to ensure compliance with The Cybersecurity Law and adopt measures as necessary to avoid contravention. With potential personal liability for the "directly responsible persons", in addition to corporate liability, management should be acutely aware of these obligations and consequences and improve internal corporate governance regimes to avoid contravention



Key Aspects – How does The Cybersecurity Law Compare with Hong Kong?

Since the element of data protection is present in both China's Cybersecurity Law and Hong Kong's Personal Data (Privacy) Ordinance it is instructive to compare and contrast the requirements of the two pieces of legislation, and see how much interoperability can be established between the two, so that businesses that have presence in both China and Hong Kong can reduce duplication of compliance efforts as they establish new business ventures in China.

	China Cybersecurity Law	**Hong Kong** Personal Data (Privacy) Ordinance
Regulated Entities	▪ Network operator ▪ Critical information infrastructure operator ▪ Network products and services provider	Data user able to control, in or from Hong Kong, the collection, holding, processing or use of personal data
Impact on Business Risk Management and Internal Governance	While The Cybersecurity Law regulates cybersecurity-related entities, the Ordinance regulates data users in all industries so long as they control personal data processing in or from Hong Kong.	

Key Aspects – How does The Cybersecurity Law Compare with Hong Kong?

	China Cybersecurity Law	Hong Kong Personal Data (Privacy) Ordinance
Definition of Personal Data	Data recorded electronically or by other means, which alone or in combination with other data enables a natural person to be identified, including but not limited to his name, date of birth, identification document number, biometric data, address and telephone number	Data relating directly or indirectly to a living individual, from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and in a form in which access to or processing of the data is practicable
Impact on Business Risk Management and Internal Governance	There is a similar broad coverage of "personal data". Businesses should carefully review which data constitutes "personal data" under The Cybersecurity Law, subjecting them to specific provisions on data privacy protection. If necessary, businesses should create a personal data inventory and map all processing of personal data for record-keeping and monitoring.	

Key Aspects – How does The Cybersecurity Law Compare with Hong Kong?

	China Cybersecurity Law	Hong Kong Personal Data (Privacy) Ordinance
Data Collection/ Use/Disclosure	**Network operators must:** ▪ follow principles of lawfulness, legitimacy and necessity in collecting and using personal data ▪ publicise rules for data collection and use, give clear notification to individuals (purposes, manner and scope) and obtain individuals' consent ▪ only collect personal data relevant to its services provided, and collect and use data in compliance with Chinese laws, administrative regulations and parties' mutual agreements ▪ not disclose individuals' personal data to third parties without consent, unless the data has been processed in such a way that it can no longer identify specific persons and be restored to its original state Network products and services providers must give clear notifications to users and obtain consent during data collection, and comply with The Cybersecurity Law and regulations on data protection contained in other relevant Chinese laws and administrative regulations	**Data users must:** ▪ collect personal data lawfully and fairly, and for purposes directly related to its function/activity ▪ collect only adequate and non-excessive personal data ▪ notify data subjects such as the purposes and potential classes of transferees ▪ not use or disclose data for a new purpose (purpose other than the original collection purpose or a directly related purpose) unless the data subject gives express consent voluntarily
Impact on Business Risk Management and Internal Governance	The Cybersecurity Law differs from the Hong Kong Ordinance in that it requires consent for any collection or disclosure of personal data. This may entail corresponding record keeping obligations of consent for businesses. Evolving technologies and limited space for network and online businesses may also require businesses to be creative and flexible in giving clear notification and seeking consent from individuals to fulfill The Cybersecurity Law's requirements.	

Key Aspects – How does The Cybersecurity Law Compare with Hong Kong?

	China Cybersecurity Law	Hong Kong Personal Data (Privacy) Ordinance
Data Security and Data Breach Reporting	**Data users must:** ▪ Keep users' data strictly confidential ▪ Adopt technical and other necessary measures to prevent data leakage, damage or loss ▪ Whenever incidents of data leakage, damage or loss have happened or may happen, immediately take remedial actions and report to users and relevant competent department in time	**Data users:** ▪ **must** take all practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use ▪ **may** report breach incidents to users and the Privacy Commissioner voluntarily
Impact on Business Risk Management and Internal Governance	The Cybersecurity Law requires mandatory data breach reporting[8]. There is only a voluntary regime under Hong Kong's Ordinance. This is obviously a key difference. Businesses should ensure they have in place a breach reporting and breach response plan to accommodate best practices in both jurisdictions.	

8. Although the Cybersecurity Law does not clarify whether the reporting obligation to the competent department would apply to all scale of data breaches, it seems that some minor data breaches may be exempted from reporting. Under the Regulations on the Protection of Personal Information of Telecommunications and Internet Users, the internet service providers are only required to report the data breaches having caused or may cause serious consequences.

Key Aspects – How does The Cybersecurity Law Compare with Hong Kong?

	China Cybersecurity Law	Hong Kong Personal Data (Privacy) Ordinance
Individuals' Right to Request Data Deletion or Correction	▪ An individual who discovers that a network operator has collected and used their personal data in contravention of Chinese laws, administrative regulations or parties' mutual agreements is entitled to request the operator to delete that data ▪ An individual who discovers that their personal data collected and stored by network operator is incorrect is entitled to request the operator to correct the data ▪ In both cases, the network operator must take measures to delete or correct the relevant data	▪ Data users must ensure that, along with the data processor they engage, do not keep personal data for longer than is necessary for fulfilling the purpose for which data is or is to be used ▪ Data users must take all practicable steps to ensure personal data is accurate for the purpose for which data is or is to be used. Data subjects are entitled to submit data correction requests to data users, and data users who are satisfied that the personal data to which a data correction request relates is inaccurate must make the necessary correction
Impact on Business Risk Management and Internal Governance	Under The Cybersecurity Law, individuals are given the right to make data deletion requests with obligatory effect on businesses. This is not present in the Hong Kong Ordinance. Businesses should have in place guidelines and conduct staff training for proper handling of data deletion and correction requests under The Cybersecurity Law, and should keep records of reasons for and circumstances of all refused requests.	

Key Aspects – How does The Cybersecurity Law Compare with Hong Kong?

	China Cybersecurity Law	Hong Kong Personal Data (Privacy) Ordinance
Individuals' Right to Request Data Deletion or Correction	**For a network operator or network services or products provider contravening data protection principles above:** **General cases** – one or more of following: ▪ rectification order ▪ warning ▪ confiscation of illegal profits ▪ fines equivalent to one to 10 times of illegal profits ▪ if there are no illegal profits, (a) fines against operators or providers (<RMB $1 million) and (b) fines against directly responsible persons (>RMB $10,000 and <RMB $100,000) **Serious cases:** ▪ orders to suspend business, suspend operations and undergo rectification, shut down websites or revoke business permits or business licences	For a data user, contravening Data Protection Principle is not a criminal offence directly. Nevertheless, the Privacy Commissioner may serve an enforcement notice requesting the data user to remedy the contravention. Contravening an enforcement notice is a criminal offence and data user is liable on conviction to HK$50,000 fine and two-year imprisonment. It is also a criminal offence for a data user to contravene a main body provision without reasonable excuse. A data user is liable on conviction to HK$10,000 fine
Impact on Business Risk Management and Internal Governance	The possibility of being awarded a hefty maximum fine of RMB $1 million and for serious cases, potential orders to cease operations, shut down websites or terminate licences or permits, may cause serious disruption to business. Management should be alert to potential personal liability for "directly responsible persons", in addition to corporate liability. Businesses should make the mitigation of risks of contraventions and adoption of preventive measures a strategic priority.	

The way forward

The Cybersecurity Law has innovatively placed businesses operating in China at the heart of a layered cooperative approach in safeguarding cybersecurity. It requires them to work with regulatory bodies and various stakeholders in the cybersecurity community, including the State Council, the provincial and municipal government bodies and other network-related industry organisations.

For businesses, this close connection with various stakeholders requires caution in navigating the intricate requirements of these different entities. Businesses currently operating or intending to operate in Hong Kong should also be aware that a different legal regime applies for data protection and cybersecurity issues. While similar concepts and issues are covered under both The Cybersecurity Law and Hong Kong's Privacy Ordinance, there are some clear distinctions and differences between the two, as regards not only obligations but also penalties.

In view of the penalties which may be imposed under The Cybersecurity Law for non-compliance, businesses should carefully review and ensure that their internal cybersecurity systems and controls measure up to the requirements, provide training to their staff, and monitor and comply with both regimes if they operate in both jurisdictions. If necessary, businesses should consider obtaining appropriate and skilled legal advice in setting up, or reviewing and upgrading their internal systems and procedures accordingly in compliance with The Cybersecurity Law.

In recent years, the importance attached to cybersecurity issues has undoubtedly raised its profile on the corporate agenda. Deep assessment, and plans for mitigation, of legal, commercial and reputational risks associated with cybersecurity, data and privacy issues remain paramount. This is especially so in a jurisdiction like China, which is expected to continue to exert control over information and technology, particularly data issues, to ensure requirements of security (national and otherwise) and regulatory control are satisfied, including in areas such as encryption.

Across Osborne Clarke's international network we have a deep understanding of the cybersecurity and data privacy regulatory and legal landscapes, whether in China, Hong Kong, more widely in Asia or in Europe. This is derived from many years of experience assisting clients, including many international corporates, in navigating complex issues of multi-jurisdiction data security and compliance.

Please contact our experts in our Hong Kong or Shanghai offices for further information.

Contacts

Prepared by

Osborne Clarke
OCHK Office

Albert Yuen
Head of TMC, Hong Kong
T: +852 2535 0114
E: albert.yuen@osborneclarke.com

Alice Li
Partner, Hong Kong
T: +852 2994 3591
E: alice.li@osborneclarke.com

Jasmine Yung
Trainee Solicitor, Hong Kong
T: +852 2535 0116
E: jasmine.yung@osborneclarke.com

上海法乐律师事务所
Zhang Yu & Partners
OC China

Guohua Zhang
Managing Partner, Co-founder
T: +86 21 6279.8808
E: guohua.zhang@oclegalchina.com

Danny Yang
Associate
T: +86 21 6279.8916
E: danny.yang@oclegalchina.com