KPMG

Cyber security in China

Management Consulting

KPMG China

—

August 2016

Cyber security overview

Given the rapid growth of the IT industry, reliance on technology is ever increasing. As a result, cyber security risks brought about by this development have emerged as a hot topic. In China, cyber security has received greater attention having been elevated to the level of national security.

By providing an overview of cyber security developments in China, KPMG China aims to outline the major topics affecting cyber security management in the mainland and to provide an analysis of recent trends in the field of IT that will likely affect future policy developments.

Importance: increasing emphasis on cyber security

Growth: increasing coverage of cyber security

Emerging trends: cyber security in the future

Cyber security in China

Cyber security today

Organisations in China across a whole range of industries including e-commerce, insurance, banking, IT, education, tourism and automotive are in possession of an increasing amount of personal information and transaction data. These organisations are now the main targets of cyber attacks with sensitive data often being leaked due to organisational system vulnerabilities. These include:

- insufficient security controls over data transfer, access control and security management; sensitive data (in transition, storage or in use) can be leaked intentionally or unintentionally;
- insufficent capabilites in security services and incident response, which makes it difficult for organisations to react and respond to potential security threats effectively;
- inadquate resources devoted to fixing data leakage channels after being discovered; this could lead to further attacks resulting in the leakage of even more sensitive data;
- weak organisational security architecture and security operations, which makes it more difficult for organisations to respond to cyber attacks.

91.5 Billion

According to statistics for the past 12 months, Internet users in China have suffered financial losses of up to **RMB 91.5 billion** due to personal information leakage, fraud, junk email, etc.

About 37% Internet users have encountered security problems while using online payment systems; **51%** of them have suffered a financial loss.

In the first half of 2016, **37%** of Internet users have suffered an economic loss due to various types of Internet fraud and **84%** have experienced some sort of negative impact from personal information leakage.

Data from：*Right Protection Report for Chinese Internet Users in 2016*、*National Cyber Security Situation and Computer & Mobile Device Virus Infection Survey Report*

Cyber security today – National level

China has fully recognised the significance of cyber security and has elevated its potision to one of national security. Aside from establishing its leading group for cyber security, the National People's Congress (NPC) has conducted a second review of its Cyber Security Law in June 2016.

Earlier

Focus on legislation regarding security of systems and infrastructure:

- State Council - *computer information system protection regulation*, *administration of Internet information services procedures;*
- Ministry of Public Security - *measures for the prevention and control of computer viruses;*
- Ministry of Public Security, etc - *measures for the graded protection of information security;*
- NPC Standing Committee - *law of the People's Republic of China on guarding state secrets.*

2014

In February 2014, the leading group for cyber security and informationisation was established with President Xi Jinping named as the group leader. Moreover, cyber security was included in the recent *Report on the Work of Government* delivered by Premier Li Keqiang.

2015

In June 2015, the NPC Standing Committee reviewed the *Cyber Security Law (draft)* and canvassed advice from the public in early July. It is expected that when the Cyber Security Law is ratified, other related security laws and regulations will be introduced as well.

2016

In June 2016, the NPC Standing Committee performed a second review of the *Cyber Security Law (draft)* and clarified the requirements for protecting key information infrastructure and sensitive data.

In July 2016, the second edition of the *Cyber Security Law (draft)* was officially published on the NPC's website and made available for public comment.

Cyber Security Law

The *Cyber Security Law* is an important milestone in the evolution of China's cyber security legislation. In the second draft of the *Cyber Security Law*, organisaions from all industries should focus on the following points:

Subject	Term	Content	Potential influence
Sensitive data storage	Article 35	Individual information and important business data collated by Internet service providers (ISPs) shall be stored within China. If the data needs to be sent overseas, a security evaluation should be performed based on regulations established by the State Council and other departments.	This article requires that personal information and important business data is stored in China. It may affect some multinational firms, especially those holding Chinese citizens' personal information.
Internet service providers	Term 3, Article 20	ISPs should retain network related logs. The period for retaining logs should be greater than 6 months.	These articles raise explicit requirements for ISPs to retain network logs and to collect personal information. Besides, the *Cyber Security Law* makes explicit requirements for ISPs' incident response, personal information usage, compliance channels, etc.
	Term 2, Article 47	ISPs should comply with lawful supervision and inspection conducted by related government departments.	
	Article 23	When offering Internet related services, the ISPs should ask users to provide real personal identity information	
Use of personal information	Term 1, Article 41	ISPs shall not divulge, tamper or destroy any personal information they collect. Without consent from the owners of the information, ISPs shall not provide personal information to others.	These articles raise explicit requirements for the use and protection of personal information. This will increase the requirement on individual privacy protection in China and indicates that China is placing greater emphasis on individual privacy protection.
	Term 2, Article 41	ISPs should adopt technical and other necessary measures to ensure personal information security.	
	Article 38	Information obtained for the protection of key information infrastructure by the National Network and Information Office and other departments should only be used for cyber security purposes and not for any other purpose.	
Secure and trustable	Article 15	To promote secure and trustable Internet products and services.	'Secure and trustable' has become the focus point of infrastructure security and it may affect organisations when selecting infrastructure in the future.
Security service	Article 16	Organisations are encouraged to perform cyber security testing and risk assessment.	This encourages enterprises from different industries to engage in cyber security related activities.

Cyber security regulators

With the establishment of the *Cyber Security Law,* the government has sought to clarify the regulatory bodies responsible for overseeing cyber security in China. In the draft version of the law, the following departments are mentioned as having regulatory responsibilties:

- the National Network and Information Office: overall coordination for cyber security supervision and management;
- the telecommunications department of the State Council, the Ministry of Public Security and other related departments: responsible for cyber security protection and supervision within each department's remit.

The departments listed above will be among the key cyber security regulators in China.

From an industry perspective, regulators in different sectors, especially for financial services, have been paying closer attention to cyber security in recent years.

The laws and regulations related to cyber security in different industries are as follows:

China Banking Regulatory Commission

- *commercial bank information technology risk management guidelines,*
- *commercial bank business continuity supervision guidelines,*
- *risk management guidelines for financial institutions on outsourcing risk management,*
- *stronger risk management requirements on IT outsourcing for financial institutions,*
- *instructions for using secure and controllable IT technology and stronger regulations on cyber security and informationisation for the banking industry,*
- *guidelines for promoting controllable application security technology in the banking industry.*

China Insurance Regulatory Commission

- *information systems security management guidelines for insurance companies,*
- *procedures for authenticating and managing client information for individual insurance,*
- *insurance organisations' informationisation regulation (draft).*

China Securities Regulatory Commission

- *information security assurance measures for securities and futures business,*
- *information security incidents reporting and investigation measures for securities and futures business.*

Payment & Clearing Association of China

- *information technology risk management guidelines for non-banking payment institutions (2016.6),*
- *personal information protection technical guidelines (2016.6).*

Trends & hot topics

1、Traditional security management: still the focus of regulations

- According to the *Cyber Security Law* and guidelines published by regulators in various industries, traditional information security management remains the focus point of supervision. Some of the details include:
  - information technology governance,
  - information technology risk management,
  - information technology audit,
  - systems development migration and maintenance,
  - business continuity,
  - outsource management,
  - information security.
- From an industry perspective, banking has the stongest industry regulations in place. The CBRC performs regular audits based on cyber security requirements and performs both on-field and off-field assessments. The assessment results will have an impact on the compliance level of each bank.
- The focus of external regulations in the banking industry has shifted from 'IT risk management' to more specific topics including business continuity, outsourcing risk management and technology controllability.
- Enterprises in other inductries such as healthcare, IT and manufacturing manage their application system security and IT infrastructure security based on the *Measures for the Graded Protection of Information Security*, issued by the Ministry of Public Security and other authorities.

2、Emphasis on emerging technologies

As new technologies emerge, security risks brought about by these technologies are starting to be reflected in the details of regulatory requirements such as:

- the CIRC's *insurance organisations' informationisation regulation,* Article 64:

  "insurance companies should actively track, study and apply emerging technologies. While encouraging business innovation, they should improve the capability for information security protection… and fully consider the risk elements such as the security of sensitive data that run on the cloud computing platforms, reliability of implemented security control measures and completeness of systems and data transferring plans."

  - This article clarifies the security management requirements of insurance institutions for emerging technologies and emphasises data security on cloud computing platforms.
- the PBOC - research on the maturity of cyber security capabilities in the banking industry:
  - this includes 'situational awareness' requirements related to cyber security, integrated collection, analysis, monitoring, presentation and use of cyber security information; it also outlines higher requirements regarding trend analysis of cyber security.

Cyber security is gradually gaining attention in other industries as well, for example:

- automotive industry: the Internet of vehicles is improving users' driving experience but at the same time brings with it huge challenges for car and Internet safety;
- public cloud computing: the increasing sophistication of the cloud is leading to more and more enterprises re-allocating their business systems to cloud platforms. While saving costs and increasing usability, public clouds also raise issues regarding data security, tenant isolation, access control, etc, which has gradually become the focus point of these enterprises.

KPMG China insights

Cyber Security : increasing importance

National level - gradually elevated to the legislative level

- In 2015, the new National Security Law raised the concept of 'maintain[ing] national cyber space sovereignty' for the first time.
- The *Cyber Security Law*, which is in draft currently, is the first Chinese law focused on cyber security. It is expected to come into effect in late 2016 or early 2017.
- The *Cyber Security Law* raises Internet infrastructure security and citizens' personal information security to the legislative level. It shows that the government has started to recognise that cyber security is of the utmost importance due to the proliferation of new forms of technology.
- Protection of individual privacy has become a hot topic globally. After the EU passed the General Data Protection Regulation, it is expected that individual privacy protection in China will become stricter with compliance costs for enterprises increasing as a result.

Industrial regulations - regulations will be strengthened

- Industry regulatory bodies (e.g. the CBRC, CIRC, CSRC, etc) are increasingly emphasising cyber security for financial institutions.
- After the issuance of the *Cyber Security Law*, it is expected that further legislation in relation to cyber security will be issued. Regulators for various industries are expected to clarify existing guidelines shortly such as the National Network and Information Office, the telecommunication department of the State Council, the Ministry of Public Security, etc.
- Matters such as individual privacy protection, data storage, infrastructure security and incident response are expected to be hot topics among all major industries.

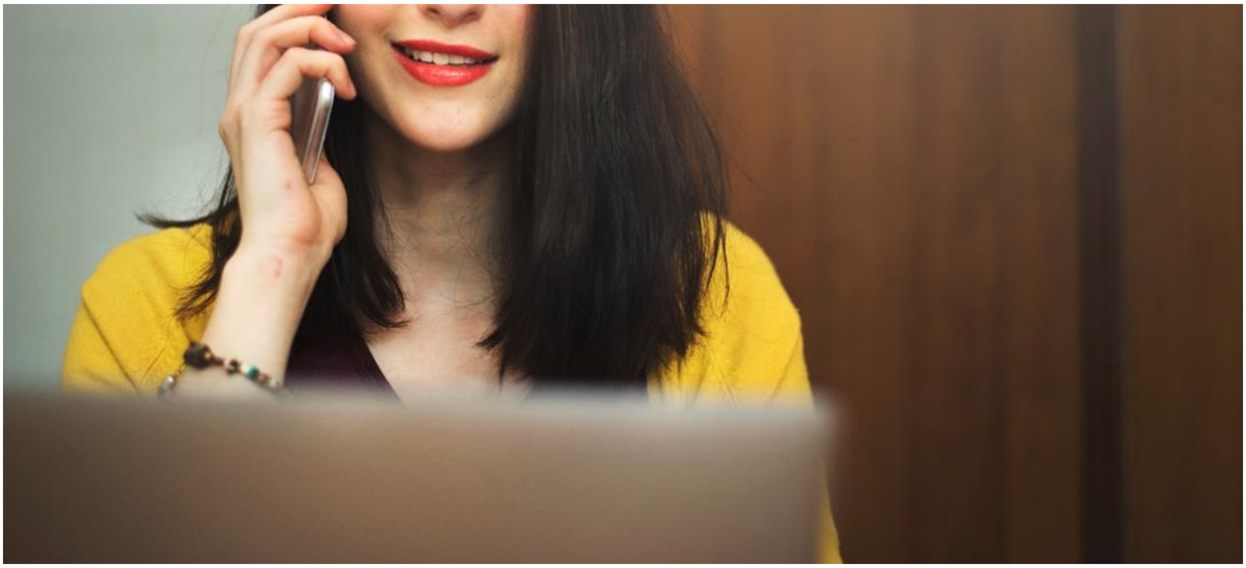
KPMG China insights (cont'd)

Coverage of cyber security: wider range

- Whereas before most industry regulators focused on infrastructure and information systems, in recent years, as new technologies, channels and businesses have emerged, cyber security coverage has been expanding to include protection of individual privacy, customer channels, transaction security, business continuity, corporation reputation, etc.
- With regards to cyber security management, enterprises in each industry have started to shift their approach from responding to individual breaches to taking a proactive approach to defending their security.

Future trends in cyber security

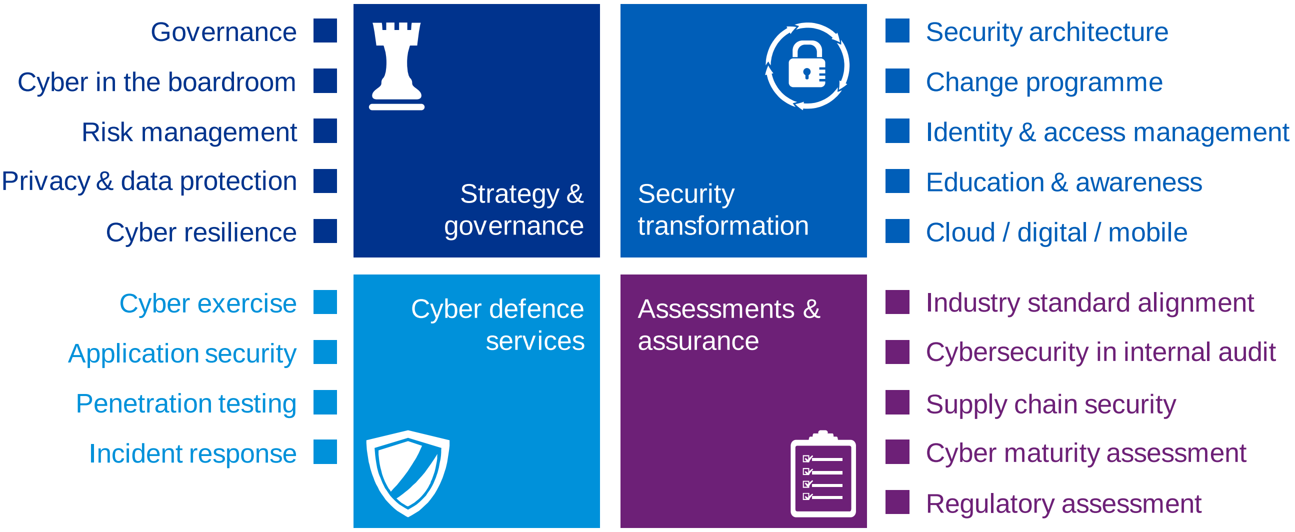
- Based on the *Cyber Security Law* and other related laws and regulations, enterprises will continue to build robust internal cyber security management systems with the goal of increasing their cyber security management capabilities.
- Due to the emergence of new technologies such as biological recognition, Internet finance, big data, blockchain, mobile applications, the Internet of Things, etc, cyber security management will become even more important in the future.
- Emerging security management topics such as security trend analysis, mobile security management, cloud security management and new forms of identity authentication technology will also become increasingly important.
- Future enterprises, especially those involved with important cyber infrastructure, will gradually increase the level of technology sourced from Chinese vendors and reduce their reliance on foreign technology.



Cyber security services from KPMG China

KPMG China has been providing cyber security advisory services for many years and has a thorough understanding of the current cyber security situation in China including existing laws and regulations.

KPMG China is experienced in delivering different types of advisory services based on our clients' needs. KPMG China's philosophy of managing cyber security is based upon the following four components:



Strategy & governance

- Governance
- Cyber in the boardroom
- Risk management
- Privacy & data protection
- Cyber resilience

Security transformation

- Security architecture
- Change programme
- Identity & access management
- Education & awareness
- Cloud / digital / mobile

Cyber defence services

- Cyber exercise
- Application security
- Penetration testing
- Incident response

Assessments & assurance

- Industry standard alignment
- Cybersecurity in internal audit
- Supply chain security
- Cyber maturity assessment
- Regulatory assessment

Contact

Henry Shek

Partner

Tel：+ 852 2143 8799
henry.shek@kpmg.com

Richard Zhang

Director

Tel：+ 86 (21) 2212 3637
richard.zhang@kpmg.com

Calfen Cui

Director

Tel：+ 86 (10) 8508 5470
calfen.cui@kpmg.com

Alvin Li

Associate Director

Tel：+ 852 2978 8233
alvin.li@kpmg.com

Matrix Chau

Associate Director

Tel：+ 852 2685 7521
matrix.chau@kpmg.com

Shane Wang

Associate Director

Tel：+ 86 (21) 2212 3651
shane.wang@kpmg.com

Jason He

Associate Director

Tel：+ 86 (755) 2547 1129
jason.rk.he@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.