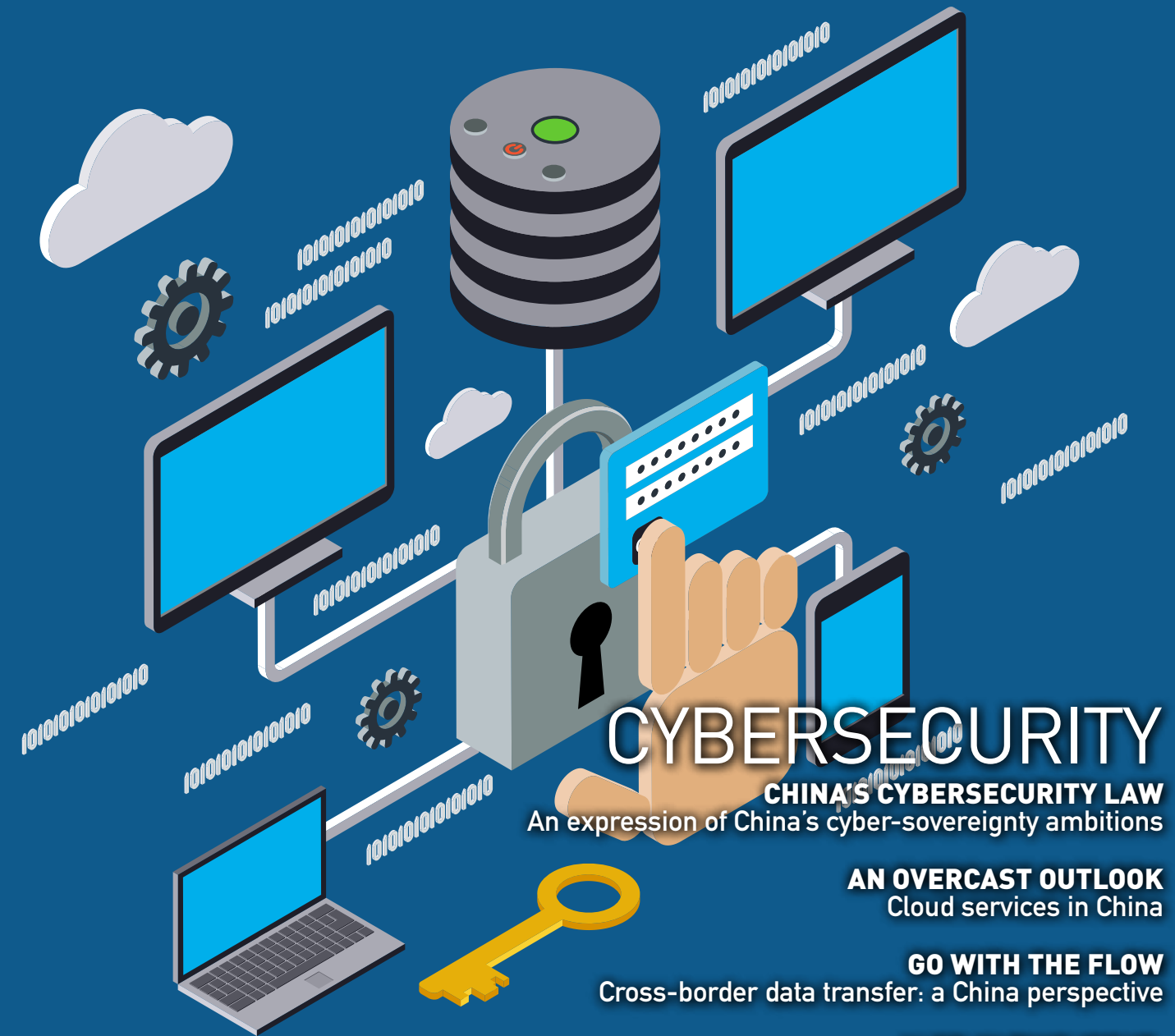


Journal of the European Union Chamber of Commerce in China

# EURObiz

[www.eurochamber.com.cn](http://www.eurochamber.com.cn)

January/February 2017



## CYBERSECURITY

### CHINA'S CYBERSECURITY LAW

An expression of China's cyber-sovereignty ambitions

### AN OVERCAST OUTLOOK

Cloud services in China

### GO WITH THE FLOW

Cross-border data transfer: a China perspective

### ALSO IN THIS ISSUE:

#### A GAME CHANGER?

The PRC Foreign NGO Law

### CHAMBER ANNUAL CONFERENCE

Is globalisation in retreat?



European Chamber  
中国欧盟商会



# 你为未来 做的计划 总是赶不上 变化

## 成长充满活力

企业各个部门像有机体一样协同、成长和发展。SAP S/4HANA®帮助中型企业自动化并整合业务流程，在当下激发企业活力。所有职能部门一同成长，无人掉队。

[sap.com/china/growth](http://sap.com/china/growth)

# TABLE OF CONTENTS

## COVER STORY

### 06 CHINA'S CYBERSECURITY LAW

An expression of China's cyber-sovereignty ambitions.

### 08 CYBERSECURITY

Attacks, effects and the role of the law.

### 11 IN THE KNOW

Cybersecurity: what are we dealing with?

### 14 AN OVERCAST OUTLOOK

Cloud services in China.

### 17 PROTECTING YOUR PRIVACY

Private data protection in China.

### 20 GO WITH THE FLOW

Cross-border data transfer: a China perspective.

### 23 DIGITAL DOs AND DON'Ts

China's e-commerce market restrictions for SMEs.

### 26 CYBER PROTECTION

Executives adopt new tech to manage cyber threats.

## FEATURES

### 32 A GAME CHANGER?

The PRC Foreign NGO Law.

### 35 LEVELLING THE PLAYING FIELD FOR SMEs IN CHINA

European Chamber's recommendations included in revised China SME Promotion Act.

### 38 CHAMBER ANNUAL CONFERENCE

Is globalisation in retreat?

## REGULARS

### 05 PRESIDENT'S FOREWORD

### 30 LOBBY REPORT

### 42 MEDIA WATCH

### 44 EVENTS GALLERY

### 48 CHAMBER BOARD







## European Chamber Chapters:

**Chief Editor**  
Carl Hayward

**Art Director**  
Wenwen Gu

**For European Chamber Membership:**

**National Member Relations Manager**

Paula Mueller  
Tel: +86 (21) 6385 2023  
ext 114  
pmueller@european-chamber.com.cn

**For advertising in EURObiz:**

**Advertising and Sponsorship Manager**  
Queenie Cheng

Tel: +86 (10) 6462 2066 ext 54  
qcheng@european-chamber.com.cn

EURObiz is published bimonthly by the European Union Chamber of Commerce in China, and is distributed free to all Chamber members.

All material is copyright ©2016 by the European Union Chamber of Commerce in China. No part of this publication may be reproduced without the publisher's prior permission. While every effort has been made to ensure accuracy, the publisher is not responsible for any errors. Views expressed are not necessarily those of the European Union Chamber of Commerce in China.

### Beijing

Beijing Lufthansa Center,  
Office C412  
50 Liangmaqiao Road  
Beijing, 100125, PR China  
北京市朝阳区亮马桥路五十号  
燕莎中心写字楼C-412室  
Tel: +86 (10) 6462 2066  
Fax: +86 (10) 6462 2067  
euccc@european-chamber.com.cn

### Nanjing

806, No.99 Zhongshan  
Road, Xuanwu District,  
Nanjing  
南京市玄武区中山路99号  
806室  
Tel: +86 (25) 8362 7330 /  
8362 7331  
Fax: +86 (25) 8362 7332  
nanjing@european-chamber.com.cn

### Shanghai

Unit 2204, Shui On Plaza  
333 Huai Hai Zhong Road  
Shanghai, 200021  
PR China  
上海市淮海中路333号  
瑞安广场2204室  
Tel: +86 (21) 6385 2023  
Fax: +86 (21) 6385 2381  
shanghai@european-chamber.com.cn

### Shenyang

Room 646, Sofitel  
Shenyang Lido, 386  
Qingnian Street, Heping  
District, Shenyang, 110004  
P.R. China  
沈阳市和平区青年大街386号  
丽都索菲特酒店646室  
Tel: +86 (24) 6683 4376  
Fax: +86 (24) 6683 4376  
shenyang@european-chamber.com.cn

### South China - Guangzhou

Unit 2817, 28/F, Tower A,  
China Shine Plaza  
9 Linhe Xi Road  
Tianhe District  
Guangzhou, 510613 PR  
China  
广州市天河区林和西路9号  
耀中广场A座2817室  
Tel: +86 (20) 3801 0269  
Fax: +86 (20) 3801 0275  
prd@european-chamber.com.cn

### South China - Shenzhen

Rm 308, 3/F Chinese  
Overseas Scholars  
Venture Bld  
South District, Shenzhen  
Hi-tech Industry Park  
Shenzhen, 518057  
PR China  
深圳高新区南区  
留学生创业大厦3楼308室  
Tel: +86 (755) 8632 9042  
Fax: +86 (755) 8632 9785  
prd@european-chamber.com.cn

### Southwest - Chengdu

04-A, F16, Tower 1 Central  
Plaza  
8 Shuncheng Avenue  
Jinjiang District, Chengdu  
成都市锦江区顺城大街8号中  
环广场1座16楼04-A  
Tel: +86 (28) 8527 6517  
Fax: +86 (28) 8529 3447  
chengdu@european-chamber.com.cn

### Southwest - Chongqing

1-1, 23F, B4 Block,  
Chongqing Foreign  
Business District, 12 Yun  
Shan Nan Lu, Yubei District,  
Chongqing, China  
中国重庆市渝北区云杉南路  
12号重庆涉外商务区B4栋23  
楼1-1室  
Tel: +86 (23) 63085669  
chongqing@european-chamber.com.cn

### Tianjin

41F, The Executive Center,  
Tianjin World Financial  
Center, 2 Dagubei Lu,  
Heping District, Tianjin  
300020, PR China  
天津市和平区大沽北路2号天  
津环球金融中心41层德事商  
务中心  
Tel: +86 (22) 5830 7608  
tianjin@european-chamber.com.cn



**JOIN THE EUROPEAN  
BUSINESS CONVERSATION  
IN CHINA  
Advertise in EURObiz**

Reach **24,000** senior European and Chinese business executives, government officials and more than **1,600** member companies of the EU Chamber nationwide with the only publication dedicated to covering European business in China.

To place your ad,  
please contact:

**Queenie Cheng**

**Advertising and Sponsorship Manager**

Tel: +86 (10) 6462 2066 ext 54  
qcheng@european-chamber.com.cn

# CYBERSECURITY'S IMPACT ON EUROPEAN (AND CHINESE) BUSINESS



**Jörg Wuttke**  
President of The European Union  
Chamber of Commerce in China

A handwritten signature in blue ink, appearing to read 'J. Wuttke'.

On 7<sup>th</sup> November, 2016, the Chinese authorities passed a new Cybersecurity Law that will have significant ramifications for the operations of European businesses when it comes into force on 1<sup>st</sup> June this year. For one, existing requirements for localising their storage of data on servers located within Chinese territory will be further strengthened. This includes the personal data of their customers as well as important business information. Network operators will also be required to provide 'technical support' for national security and law enforcement, which may include pressure to compromise their encryption.

All of this fits with the speech that President Xi Jinping delivered during an October 2016 Politburo meeting on cyber and ICT issues, which was attended by most members of the Leading Small Group for Cybersecurity and Informatisation that President Xi leads. He stated that China "must accelerate the advancement of domestic production, indigenous and controllable substitution plans, and the building of secure and controllable information technology systems."<sup>1</sup> This sent a clear signal to the bureaucracy that these issues continue to be a top priority for the senior leadership. It also aligned with the Science and Technology Innovation Five-year Plan that was released in August 2016, on the importance of strengthening indigenous innovation capabilities and fully realising the effectiveness of science and technology innovation in safeguarding national security.<sup>2</sup>

These messages delivered at the highest level of the Chinese Government and Communist Party combined with the market share targets included in the China Manufacturing 2025 implementation roadmap indicate that European business will play a diminishing role in China's ICT industry. However, this is not just an issue for ICT companies, it will impact many others. The emerging Industry 4.0 model is powered by big data that can be utilised and shared throughout entire industrial value chains. While this enables companies to respond to challenges and opportunities in real time and to better understand how different aspects of their business connect with each other, they need to be fully confident that they will not lose control of their proprietary information.

The new law will also have a serious bearing on Chinese companies. The reduction in market-driven competition in China's ICT industry will negatively impact China's capacity to drive innovation overall. Chinese enterprises across a wide range of industries will also be increasingly unable to adopt the best technologies available internationally, and requirements to adopt 'secure and controllable' technology instead—which may not serve their business needs—will compromise their ability to enter, and successfully operate in, international markets.

While every country has legitimate security interests in industries related to IT, the approach that the Chinese authorities have taken is distorting the market and will carry a real economic cost. For example, it has been calculated that the potential de-globalisation of China's ICT industry more broadly could lead to a 1.8 to 3.4 per cent reduction in China's GDP. Based on 2015 figures, this amounts to EUR 190 billion per year, and by 2025 could amount to a cumulative reduction of EUR 2.85 trillion.<sup>3</sup> This would result in part from a reduction in transfers of knowhow and the related decline in efficiencies and domestic innovation as a consequence of reducing openness to foreign business.

The European Chamber will continue to engage with the Chinese authorities on why the new legislation is not in the country's own long-term interests. We also encourage Chamber members to take the time necessary to understand how these issues may impact their business. This issue of *EURObiz* presents an important opportunity to do so.

---

<sup>1</sup> Martina, Michael, *Xi Says China Must Speed Up Plans for Domestic Network Technology*, Reuters, 9<sup>th</sup> October, 2016, viewed 4<sup>th</sup> January, 2017, <<http://www.reuters.com/article/us-china-inter-net-security-idUSKCN1290LA>>

<sup>2</sup> *State Council: Notice on Science and Technology Innovation 13<sup>th</sup> FYP*, State Council, 8<sup>th</sup> August, 2016, viewed 9<sup>th</sup> January, 2017, <[http://www.gov.cn/zhengce/content/2016-08/08/content\\_5098072.htm](http://www.gov.cn/zhengce/content/2016-08/08/content_5098072.htm)>

<sup>3</sup> *Preventing Deglobalisation: An Economic and Security Argument for Free Trade and Investment in ICT*, US Chamber of Commerce, Rhodium Group and Covington & Burling LLP, 1<sup>st</sup> September, 2016, viewed 4<sup>th</sup> January, 2016, p. 8, <<http://rhg.com/reports/preventing-deglobalization>>



# CHINA'S CYBERSECURITY LAW

## An expression of China's cyber-sovereignty ambitions

Coming in to effect later this year, the final draft of the China's Cyber Security Law contains a number of positives, such as the strengthened measures against cyber fraud and the further clarification of the sectors that will fall under the scope of 'critical information infrastructure'. However, the European Chamber holds deep concerns that many controversial provisions that we commented on in the previous draft remain unchanged. These include the requirements for strict data residency and restrictions on cross-border data flow. The overall lack of transparency over the last year concerning this significant and wide-reaching piece of legislation has also created a great deal of uncertainty among the business community. The European Chamber remains concerned that the new law will hinder foreign investment and businesses operating in and with China.

**Bruce Fu**, Director at **APCO Worldwide**, delves deeper and explains that China's Cybersecurity Law, beyond functioning as an overarching legal framework for regulating cyberspace, is a statement of China's intent to assert its 'cyber-sovereignty'.

China's recently approved Cybersecurity Law is set to take effect on 1<sup>st</sup> June, 2017, and serves as an overarching legal framework to govern cyberspace activities. In many respects, this law follows the global trend of increasing regulation of

cyberspace in response to elevated threats worldwide. The EU, for example, just recently adopted The Directive on Security of Network and Information Systems (NIS Directive) in July 2016. But China's Cybersecurity Law includes more than just network security. Its 79 articles



cover ground including security requirements for network-related products, data security and privacy, and online content control.

In this respect the Cybersecurity Law should be understood in the context of China's continued push for national security and 'cyber-sovereignty' – the belief that the Chinese Government should have supervisory power and jurisdiction over the activities that take place in the cyberspace that falls within China's territory.

### Scope

For companies wondering how this will affect their China business, the law does not provide a clear sense of its own practical application. It is full of subjective terms such as 'important data', while the two most important terms in the law—'network operator' and 'critical information infrastructure (CII)'—lack a clear definition. The latter of these terms is crucial as the most stringent security obligations are reserved for CII operators. The law states that CII includes traditionally sensitive sectors such as "public telecommunications and information services, energy, transportation, irrigation, finance, public services, e-government", but also includes the catch-all phrase "as well as other areas that may harm national security, the economy, and the public interest." Furthermore, the law also encourages network operators outside of CII to "voluntarily participate".

### Key provisions

Some of the key provisions in the law include:

- **Data localisation:** CII operators will have to keep 'important' data and personal information in Mainland China. If it is truly necessary for a business to provide data outside of China it may be possible to do so but a security assessment must first be conducted. (Key Article: 37)
- **Personal information protection:** Network operators will be limited in collecting and using personal information. Personal information refers to information that allows the identification of a natural person's individual identity, including, but not limited to, their name, date of birth, identity card number, personally distinctive biological information, address and telephone number. (Key Articles: 40-43, 76)
- **Compulsory certification requirements:** Critical network equipment and specialised network security products, both undefined, will have to follow compulsory standards and security certification. The law also implies that compulsory certification will no longer only be a requirement for government


procurement. (Key Article: 23)

- **Cooperation with public security bodies:** When requested, network operators will have to provide technological support and assistance to public security and national security bodies. (Key Article: 28)
- **National security review:** Network operators will be subject to a multi-level protection scheme (MLPS), where they are graded based on the potential consequences of network damage and social impact. In addition, products and services procured by CII operators that may have an impact on national security must pass a national security review. (Key Articles: 31, 35)

### Preparation measures

Lacking a clear roadmap, foreign companies can start preparing themselves by paying close attention to their cybersecurity practices and upgrading where appropriate. If not for the law, elevating cybersecurity issues in corporate boardrooms across industries would be a positive outcome anyway.

Second, numerous implementation measures, including technical standards in various industries, will come out before and after the Cybersecurity Law is enacted on 1<sup>st</sup> June, 2017. These measures will be key to how the law's provisions are implemented in practice. Companies should proactively engage in discussions with their regulators and industry groups on how to best adopt the Cybersecurity Law in their areas of operation. It is especially important for likely CII operators, or those companies selling to likely CII operators, to engage with stakeholders and ensure compliance.

Finally, more important than parsing through each word of the Cybersecurity Law and the coming implementation measures, is to recognise and understand where your company stands in relationship to China's overall cybersecurity and technology development goals. Over the long-term, companies that can align themselves with China's vision, and contribute to it, are well placed to succeed. 

*Headquartered in Washington DC, **APCO Worldwide** is a global independent consultancy firm and a leading provider of corporate advisory, government relations and strategic communication services in China. APCO's Greater China team includes more than 100 professionals, including former diplomats, Chinese government officials, business leaders, journalists and NGO professionals. We advise cutting edge and innovative businesses, technology companies and disruptors on critical regulatory issues and their stakeholder engagement strategy.*



# CYBERSECURITY: ATTACKS, EFFECTS AND THE ROLE OF THE LAW

Every day, Internet users around the globe create an estimated 2.5 quintillion bytes of data.<sup>1</sup> Such a level of interconnectedness brings greater opportunities, but it also heightens the risk of cyber-attacks. The level of attention that this topic has been receiving at the highest levels of government has been recently highlighted by the European Union's new regulation—the EU General Data Protection Regulation (EU GDPR)—and complimentary directive on the matter. **Giovanni Pisacane** from **GWA Asia** looks at the growing risk of cyber-attacks and makes a comparison between how it is being dealt with in Europe and China.

---

<sup>1</sup> <https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html>



## Cyber-attacks: a growing concern

Today, all companies are reliant on IT to some degree, which necessitates making cybersecurity a top priority. While data can be lost or stolen through employees, the biggest attacks in the last five years have been as a result of hacking.<sup>2</sup> But even with the well-documented adverse effects of hacking, many companies do not have sufficient policies in place to protect against this threat.<sup>3</sup>

Egress Software Technologies carried out a survey during Infosecurity Europe 2016 and found that two thirds of respondents admitted they could do more to protect data, while 61 per cent disclosed that they had suffered a security breach within the past year.<sup>4</sup> Companies are clearly not prioritising data security, and this is costly for several reasons.

A data breach can lead to customers and clients severing their connections with a company out of fear that their interaction can impact other areas of their lives. Moreover, Semafone, a UK-based fraud prevention company, found that businesses are less likely to trade or conduct deals with businesses that have been breached, particularly if the breach included sensitive data.<sup>5</sup> Thus the breach can translate into a financial loss for the enterprise.

## Global standards of cybersecurity: the role of the law

The law performs two vital roles: enhancing cyber security preparedness and protecting consumers.

By having a common, minimum and mandatory standard of security, companies within the same jurisdictions can present a unified defence against attacks. This helps facilitate trust and business relationships since companies understand that partners and other stakeholders that they deal with are also protecting their data.

Additionally, an international legal standard is useful in breaking down the barriers between nations and facilitating a united front.

The law can enforce protection by requiring firms to report breaches, enabling the relevant government authorities to take action to strengthen security and empower individuals to mitigate harm, as well as encouraging organisations to adopt effective security measures and protect internal systems.

## Europe: looking to the future

<sup>2</sup> <https://www.cpni.gov.uk/advice/cyber/Cyber-Attack-Types/>

<sup>3</sup> <https://www.cpni.gov.uk/advice/cyber/Cyber-Attack-Types/>

<sup>4</sup> <https://www.egress.com/blog/data-breach-survey-2016>

<sup>5</sup> <http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html>

The EU is moving to bolster user protection by introducing mandatory minimums and increasing accountability and responsibility.

The EU GDPR creates new obligations in areas such as data anonymisation, compulsory breach notifications and the appointment of data protection officers, requiring organisations handling EU citizens' data to make major changes to the way they operate. Enterprises are required to notify authorities of a security breach within 72 hours of awareness: non-compliance with the regulation would cost four per cent of a company's annual turnover or EUR 20 million, whichever is higher.

On 17<sup>th</sup> May, 2016, the EU Council officially adopted the first EU-wide legislation on cybersecurity – the *Network Information Security Directive (Directive)*. The *Directive* complements the EU GDPR by imposing obligations on businesses that act as “operators of essential services” in high-risk sectors such as energy and finance, requiring them to take measures to minimise their cyber risk, and to report certain cyber incidents.<sup>6</sup>

Preparing a company for compliance with the new regulation must start by ensuring that all employees are aware of the implications of a cyber security attack.

The regulation highlights a risk-based approach, making it imperative that companies implement secure procedures for data storage and transfer, as well as controls to protect sensitive information. Breaches that affect compliance will incur hefty penalties.

## China and cybersecurity

It is estimated that more than 700 million Chinese people have access to the Internet and that around 400 million of these consumers are conducting the majority of their payments using smartphones. The country's IT market is worth in excess of USD 300 billion.<sup>7</sup> Despite this vast and impressive online infrastructure, the *Booz Allen Cyber Power Index 2014* placed China in thirteenth place in terms of their 2015 global cyber power ranking.<sup>8</sup> Unlike its western counterparts, who focus on risk-based and consumer protective approaches, China's goal in using the law as a cyber regulatory tool is attached to its motive to use the Internet as a means to build up a domestic information economy and secure network infrastructure that directly benefits national economic development and political stability. For China, protecting domestic structures is at the heart of cyber law reform. We can see such a move in the PRC Cyber Security Law (2016).

<sup>6</sup> [http://knowledge.freshfields.com/en/global/r/1501/new\\_eu\\_cyber\\_security\\_law\\_time\\_to\\_assess\\_your\\_cyber\\_risk](http://knowledge.freshfields.com/en/global/r/1501/new_eu_cyber_security_law_time_to_assess_your_cyber_risk)

<sup>7</sup> <http://www.information-age.com/chinas-new-cyber-security-law-threat-international-businesses-123463385/>

<sup>8</sup> BOOZ ALLEN HAMILTON, CYBER POWER INDEX 2-6 (2014) [http://www.boozallen.com/media/file/Cyber\\_Power\\_Index\\_Findings\\_and\\_Methodology.pdf](http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf)




The new law will require, domestic and international, software companies, network-equipment manufacturers and other technology suppliers to disclose their proprietary source code—the core component and intellectual property running their software—in order to prove that their products cannot be compromised by hackers. The government wants firms which operate in ‘critical’ areas to store any personal information or important data that they gather in China, within China’s borders. The definition of ‘critical’ is vague, but what is clear is that it would apply to areas such as information and communication technology (ICT) services, energy and finance. These requirements can be seen to be rather demanding on smaller companies. The longer the company operates the more data that it will collect from within China, thus more storage space will be required, further necessitating expense.

The initial reception of these regulations proved negative, especially from multinational corporations, which typically rely on cross-border flows of business data. This is compounded by the worry that the law will not only require additional expense with regard to new investments, but also increase the risk of data theft. Further, companies will be required to obtain security certifications for important network equipment and software. Foreign firms expressed a fear that this might be used to pressure them into turning over security keys and other patented software, which would then be disseminated to state-owned rivals.<sup>9</sup>

China appears to have adopted a shelter mentality, concerned more with domestic protectionism than actively reassuring cyber defences and rooting out cyber criminals, a position that lends itself poorly to cross-border cooperative security operations and efforts.

### Conclusion

Companies appear unaware of the growing trend in both the scale and sophistication of cyber security threats, and this is worrying. With newer legislation, priorities may begin to shift, particularly in light of the non-compliance penalties. The law is a powerful tool to assist with setting a high standard in data protection. Cyber-attacks will only increase as the world becomes increasingly connected, thus it is up to the leaders of businesses and organisations to be ahead of the curve in the fight against cyber-crime. 

**GWA Greatway Advisory** is an international consulting firm operating in Asia since 2004, with offices in Shanghai, Beijing, Hong Kong and Italy. GWA, with its team of experts lawyers and certified public accountants, assists its clients in a wide range of cross-border and domestic transactions and offers a strong network of reliable alliances and partnerships around Asia and Europe.

<sup>9</sup> <http://www.wsj.com/articles/microsoft-intel-ibm-push-back-on-china-cybersecurity-rules-1480587542>



## IN THE KNOW

### CYBERSECURITY - WHAT ARE WE DEALING WITH?

The Internet has evolved greatly over the last half-century, and the associated information and communication technology (ICT) is now ubiquitous and increasingly integral to almost every facet of modern life. However, structural and technological changes arising from telecommunications privatisation, liberalisation and the explosion of mobile Internet, has resulted in a degradation of protocol-based networks. This has facilitated an increase in cyber-attacks, cyber-crime and the proliferation of viruses, worms, malware and spam. **Tebogo Thiophilas Basuti, Faisal Khurshid** and **Wonde Chubato** of **Dragon Sino**, with the cooperation of Aryaka, detail the potential threats and explain some of the measures that should be taken to protect your business.



## Types of cyber risks

A whole range of traditional crimes are now being perpetrated via cyberspace:

- **Cybercrime:** when cyber actors work alone, or in organised groups, to extract money, data or cause disruption. They can acquire credit/debit card data and intellectual property, and impair the operations of a website or service.
- **Cyber war:** when a nation state conducts sabotage and/or espionage against another nation in order to cause disruption or to extract data.
- **Cyber terror:** when an organisation, working independently of a nation state, conducts terrorist activities through cyberspace.

The unregulated cyberspace has led to tremendous growth in inventiveness and ingenuity. However, much of this creativity has made cybercrime increasingly simple and cheap. The ability to operate from anywhere in the world, the linkages between cyberspace and physical systems and the difficulty of reducing vulnerabilities and consequences in complex cyber networks have all exacerbated the difficulties in securing cyberspace.<sup>1</sup> Ensuring cybersecurity requires coordinated efforts throughout an information system. Elements of cybersecurity include:

- Application security;
- Information security;
- Network security;
- Disaster recovery / business continuity planning;
- Operational security; and
- End-user education.

One of the most problematic elements of cybersecurity is the rapid and constantly evolving nature of security risks. The traditional approach has been to allocate the majority of security resources to the most crucial system components and to protect from the biggest known threats.<sup>2</sup> This approach leaves 'less important' system components poorly defended. It is an invitation to hackers to hunt for vulnerabilities in a system.

Instead, advisory organisations are promoting a more proactive and adaptive approach.<sup>3</sup> The National Institute of Standards and Technology (NIST), for example, recently issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments.<sup>4</sup>

According to Forbes, the global cybersecurity market reached USD 75 billion for 2005 and is expected to hit USD 170 billion in 2020.

**Application Security** is the use of software, hardware and procedural methods to protect applications from external threats. Countermeasures are taken to ensure application security. The most common software countermeasure is an application firewall that limits the execution of files or handling of data by specific installed programs.

**Information security** (InfoSec) is a set of strategies for managing the process, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. InfoSec responsibilities include establishing a set of business processes that protect information assets regardless of how the information is formatted or whether it is in transit, is being processed, or is at rest in storage.

Many large enterprises employ a dedicated security group to implement and maintain the organisation's InfoSec program. Typically, a chief information security officer leads this group. The security group is responsible for conducting risk management, a process through which vulnerabilities and threats to information assets are continuously assessed, and the appropriate protective controls are decided upon and applied.

**Network Security** consists of policies and practices adopted to prevent and monitor unauthorised access, misuse, modification or denial of computer network and network-accessible resources. Network security involves the authorisation of access to data in a network, which is controlled by the network administrator. Users are assigned authenticating information which permits access to resources and programs within their authority.

### **Disaster Recovery Business Continuity Planning (BCP) or Business Process Contingency Plan (BPCP)**

When a disastrous event prevents the continuation of normal functions, a BCP/BPCP consists of procedures to be taken to minimise the effects of a disaster to enable the organisation to either maintain or quickly resume mission-critical functions. It involves an analysis of business processes and continuity needs. It may also include a significant focus on disaster prevention. Interruption of service or loss of data can have serious financial impact, whether directly or through loss of customer confidence.

**End-User Education:** As the old InfoSec adage goes, "people are the weakest link in the cybersecurity chain." In a recent Enterprise Strategy Group (ESG) research survey, 58 per cent of enterprise security professionals identified "a lack of user knowledge about cybersecurity risks" as the most common factor for successful malware attacks.

<sup>1</sup> <http://whatistechtarget.com/definition/cybersecurity>

<sup>2</sup> [http://en.wikipedia.org/wiki/Network\\_security](http://en.wikipedia.org/wiki/Network_security)

<sup>3</sup> <http://searchcompliance.techtarget.com/definition/OPSEC-operational-security>

<sup>4</sup> <http://www.networkworld.com/article/2367106/cisco-subnet/end-users-must-be-part-of-cybersecurity-solutions.html>

The best practices in this area include:

- Awareness programmes: basic training, awareness campaigns.
- Leadership: business leaders must strive to make cybersecurity awareness and good online behaviour part of the corporate culture.
- Notifying end users of policy violations.
- Proactive spear phishing: This tactic involves sending bogus but authentic-looking emails to internal employees to see if they actively click on links, install software or open attachments. On average, between one-third and half of employees do not hesitate to install or open malicious software or attachments.
- End-user feedback: If employees are expected to become good cybersecurity citizens, then the security team should keep them up to date on how they are doing.

## TCP vulnerabilities

Traffic Control Protocol (TCP) vulnerabilities are making it easy for hackers to attack data several ways. The TCP is how data packets traverse public cyberspace.<sup>5</sup> Prior to any data entering cyberspace, a TCP breaks the data into packets, assigns each packet a sequence number then sends each packet on the best public cyberspace route. Upon reaching the final destination, the TCP reassembles the packets in their correct sequential order.

The results of a thorough security assessment of TCP, along with possible mitigations for the identified issues, were published in 2009, and are currently being pursued within the Internet Engineering Task Force (IETF).

## Denial of Service

By using a spoofed Internet protocol (IP) address and repeatedly sending purposely-assembled synchronous (SYN) packets, followed by many acknowledgement (ACK) packets, attackers can cause the server to consume large amounts of resources while keeping track of the bogus connections. The overloading of vast amount of data causes the server to crash.

## Connection Hijacking

An attacker who is able to eavesdrop a TCP session and redirect packets can hijack a TCP connection. To do so, the attacker learns the sequence number from the ongoing communication and forges a false segment that looks like the next segment in the stream. Such a simple hijack can result in one packet being erroneously accepted at one end.<sup>6</sup> When the receiving

host acknowledges the extra segment to the other side of the connection, synchronisation is lost. Hijacking combined with address resolution protocol (ARP) or routing attacks allow control of the packet flow to be taken, to get permanent control of the hijacked TCP connection.

## Conclusion

The lack of security on the Internet and of the devices connected to it, results in serious vulnerabilities. These create risks for infrastructures that increasingly rely on the Internet, including not just communications, but also power generation and distribution, air transport, and, in the near future, road transport.<sup>7</sup> It is easy and relatively inexpensive to access cyberspace and to obtain the means of conducting offensive cyberattacks. Thus, it is tempting to develop offensive cyber capabilities and indeed some countries are doing so, as published in their national cyber security strategies, and several countries have allegedly already carried out such attacks.

With all the vulnerabilities and the countermeasures associated with cyberspace, companies have to invest more labour and money in the protection of their data. The consensus within the disaster recovery industry is that most enterprises are still ill-prepared for a disaster. The Disaster Recovery site states,<sup>8</sup> "Despite the number of very public disasters since 9/11, still only about 50 percent of companies' report having a disaster recovery plan. Of those that do, nearly half have never tested their plan, which is tantamount to not having one at all."

## Countermeasures

There are numerous countermeasures that can be put in place. This can include, but is not limited to, having someone taking care of the system premises to: watch out for phishing and spear phishing; delete suspicious e-mails; configure intrusion detection systems (IDS) to block malicious domains/addresses; keep patches and updates current; and make sure that workers comply with organisation's policies. **Eb**

***Dragon Sino**, is the logistical backbone of Aryaka the world's leader in fully managed and hassle-free cloud-delivered WAN. Dragon Sino's success with the most difficult scenarios is why the IT industry relies on Dragon Sino for logistics and government compliance and why Aryaka teamed up with Dragon Sino in introducing Aryaka's service to Chengdu. With over 10 million users, 4,500 sites and a 99% satisfaction rating, Aryaka has created a faster cheaper and more reliable way to keep international offices connected.*

<sup>5</sup> <http://searchcompliance.techtarget.com/definition/OPSEC-operational-security>

<sup>7</sup> <http://www.sungardas.com/Documents/cyber-security-14-impactful-articles-MSV-EB0-020.pdf>

<sup>8</sup> <http://www.govtech.com/blogs/lohrmann-on-cybersecurity/State-CIOs-answer-questions-on-cybersecurity-and-disaster-recover-DR.html>

<sup>5</sup> [http://en.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](http://en.wikipedia.org/wiki/Transmission_Control_Protocol)



# AN OVERCAST OUTLOOK

## Cloud Services in China

China's booming technology, media and communications (TMC) sector provides great market opportunities for cloud computing and related services. Its size, coupled with the fact that it is still fast growing, means that it simply cannot be ignored. However, as with many other aspects of this market, the regulatory environment in China has never been easy. **Dr Michael Tan** and **Lynn Zhao**, both at **Taylor Wessing**, look at the legal aspects of operating cloud services in China—in particular a new draft circular that was disseminated for public comments in November 2016—and reveal a picture that is about as clear as a typical Beijing day.



For quite a long time, cloud services in general remained unregulated. In fact, it was not even possible to find the term explicitly addressed under the related telecommunication business classification catalogue (*Telecom Catalogue*), formulated by the Ministry of Industry and Information Technology (MIIT). It can be equated to the service model of Infrastructure as a Service (IaaS), since it requires an Internet Data Centre (IDC) licence, providing, as it does, facilities for data storage/computing and access management. However, under the *Telecom Catalogue* for service models of Platform as a Service (PaaS) and Software as a Service (SaaS) it had been difficult to tell exactly which service licence(s) would be required. It is very important to note, though, that just because it is not explicitly addressed it does not necessarily mean you are free to do it. On the contrary, in China this usually means you do not have a sound legal basis for launching operations.

All this creates uncertainty and complexities for a service operator – in particular a foreign one trying to properly structure its cloud computing business. Some clarity in this regard was achieved in 2016, when the MIIT updated the *Telecom Catalogue*, introducing a new entry termed ‘internet resources collaboration services’ as part of IDC services, which is a very general description supposed to cover all types of cloud-based services. However, there is still some ambiguity (and sometimes flexibility, based on past experience dealing with the MIIT) that can be applied when analysing a specific cloud service case when trying to determine whether or not it falls into this scope.

On 24<sup>th</sup> November, 2016, the MIIT presented to the public the draft *Notice on Regulating the Operation Behaviours in the Cloud Service Market (Draft Circular)* to solicit comments. Though its intention is to better regulate the market, as its name indicates, this *Draft Circular* unfortunately makes the picture foggy again. Its stated purpose is to improve the market environment, regulate administration and promote the healthy development of the Internet industry, but it comes with many new regulatory requirements and constraints which will have a substantial impact on existing business models, in particular those of foreign players. Below are some key highlights.

## Market Access

The *Draft Circular* defines the term ‘cloud services’ to be any Internet resource collaboration service that is part of an IDC service under the *Telecom Catalogue*. In other words, the use, via the Internet or other networks, of equipment and resources constructed on data centres to provide customers with services that include: data storage; a development environment for Internet applications; and the deployment of Internet applications and operation management to users, by way of easily accessible, use-on-demand, easily expanded and/or collaborative sharing. Such an expression could theoretically include

all cloud-based business models (IaaS, PaaS and SaaS), ranging from consumer applications to enterprise and Internet of Things (IoT) applications. Since an IDC service is classified as a class-one, value-added telecommunications service (VATS), which is still subject to foreign investment access restriction (i.e. a foreign stake of up to 50 per cent), full or majority foreign participation in the Chinese cloud service market will become impossible due to the broadened interpretation of the term ‘cloud services’ under the *Draft Circular*.

In the past, outsourcing parts of the business that are subject to sensitive regulations to a qualified local partner holding the required VATS licence was a practical way to circumvent licence requirements – some foreign players used this approach to expand their global offering to the Chinese market. However, the *Draft Circular* now closes the door on this model by explicitly prohibiting a qualified Chinese partner from, for example:

- letting or assigning in a disguised form its VATS licence to its foreign partner, or providing resources, a location or facilities that enable such a partner’s illegal operation;
- enabling its foreign partner to conclude a service contract directly with cloud service customers;
- delivering services to customers only using the trademark and brand name of the foreign partner; or
- illegally providing users’ personal information and network data to the foreign partner.

Obviously these cooperation models are viewed as ‘too aggressive’ by the MIIT. Since they have been practiced in the past, the *Draft Circular* will now deliver a heavy blow to those international players that have already entered the Chinese market via these routes. They may have to switch to form a 50:50 joint venture (JV) with a local partner to apply for the required VATS licence and adopt a co-branding approach, which will certainly have negative implications on their business. Also to be noted is that the JV route currently remains a theoretical possibility – it does not necessarily guarantee the issuance of a VATS licence for cloud business, not to mention the complicated procedural and time implications.

## Data Protection

With cyber security becoming a top priority of the Chinese Government, the *Draft Circular* also aims to reflect this political will by raising the below obligations for cloud service operators:

- Their cloud service platforms shall be constructed within the territory of China, and connection to overseas networks shall go through MIIT-approved Internet gateways. Connection to the outside via dedicated lines (专线 in Chinese) or VPNs are not allowed.



- Besides abiding by the general data protection rules (e.g. collection consent, data security, right to be forgotten), service facilities and data storage shall remain within China for services that target Chinese users. Any cross-border data transmission and management must follow statutory requirements.


These requirements appear understandable to an extent, and parallels can be drawn with existing mechanisms like the Great Chinese Firewall, which aims to better control cross-border data traffic. However, they will create hurdles for cloud services, in particular those that are internationally deployed. A key value of cloud services is seamless access from anywhere in the world. More value could only be created when all data are pooled together, for example to improve data sampling and data mining. Using a geographically-based concept to regulate services, including data flow, does not appear to fit the demand of business realities. The intention to rule out the use of some very popular technical solutions like VPNs also casts doubt over the value of such prohibitions in practice, since actual enforcement might prove very difficult.

The *Draft Circular* seems to keep the door open for cross-border data transmission by referring to statutory requirements. The fact that such statutory requirements and procedures are not yet clearly spelled out in sufficient detail for implementation makes this exemption less relevant at this stage, though.

## Other concerns and prospects

In addition to the above, the *Draft Circular* raises many other concerns that are making foreign players nervous. For example, it stipulates that technical cooperation with a qualified local partner must be reported to the regulator in written form. Since this kind of cooperation often involves technical and business secrets, which are of critical importance in the fast moving Internet sector, questions arise over the level of detail in relation to the cooperation that must be reported in order to secure endorsement from the regulators. Latest discussions with the MIIT

seems to indicate that they only need the information to evaluate regulatory implications but not to unduly probe commercial secrets. Nevertheless before the final version is inked, these kinds of concerns will remain.

Like it or not, the *Draft Circular* will land on the ground and its broad coverage will have a substantial impact on international players that are offering or using cloud solutions in their business. The extent of its impact could potentially lead to the MIIT softening its position regarding certain issues – for example, a more proactive approach could be taken allowing cross-border data flow under MIIT supervision by keeping an onshore copy of data instead of completely blocking such flow. As usual, the MIIT might also interpret the scope of cloud services in a more relaxed way, thereby leaving room for certain less sensitive cloud business models to survive, in particular those where their key added value relies on software and data services instead of telecom facility services. This is not too much different from the variable interest entity (VIE) example which remains theoretically illegal but practically tolerated. Whether or not all these will happen remains to be seen. 

**Dr Michael Tan** is a Partner at **Taylor Wessing**. He has profound experience in supporting multinational corporations in their business operations in mainland China, in particular in the corporate and commercial fields. Michael is also experienced in dealing with finance and foreign exchange control issues. His industrial focus is on TMC, aerospace, aviation, and other new technology driven sectors. At the same time, Michael supports Chinese companies in their 'going abroad' activities, including business expansion and IPOs in Europe. For more information please contact [m.tan@taylorwessing.com](mailto:m.tan@taylorwessing.com). Taylor Wessing is a leading full service law firm with over 1,200 lawyers in 33 offices around the world. Our China Group members are based in Shanghai, Beijing, Hong Kong, Munich, Frankfurt, Düsseldorf, Hamburg, Vienna, Paris, London and Singapore. Besides all areas of business law relevant to business transactions in China, we are also well known for our advice to Chinese companies investing overseas. For more information please visit [www.taylorwessing.com](http://www.taylorwessing.com).



# CYBER PROTECTION

## Executives Adopt New Tech to Manage Cyber Threats and Achieve Competitive Advantages

There is a distinct shift in how organisations are now viewing cybersecurity, with forward-thinking organisations understanding that an investment in cybersecurity and privacy solutions can facilitate business growth and foster innovation. *The Global State of Information Security® Survey 2017*, released in October 2016 by PwC in conjunction with CIO and CSO magazines, examines how executives are adopting technology and collaborative approaches to cybersecurity and privacy to manage threats and achieve competitive advantages. **Samuel Sinn**, Cybersecurity and Privacy Partner, **PwC China**, provides some highlights from the report below.



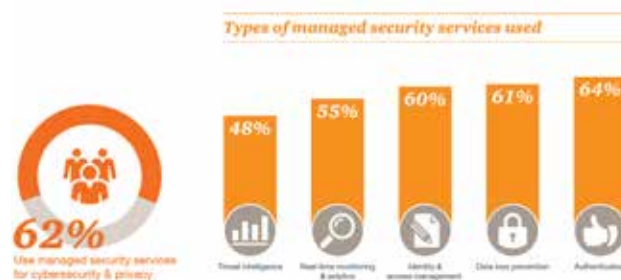
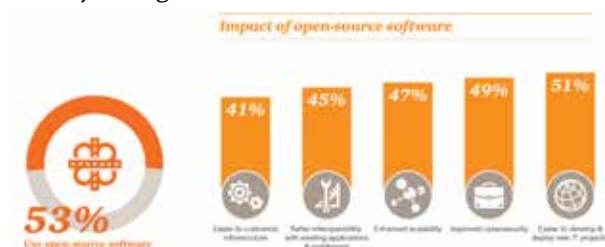
Many organisations no longer view cybersecurity as a barrier to change or as an IT cost. According to the *Global State of Information Security® Survey 2017*, 59 per cent of respondents said they have increased cybersecurity spending as a result of the digitisation of their business ecosystem. In this process, organisations not only create products, but also deliver complementary software-based services for products that extend opportunities for customer engagement and growth.

There is a distinct transformation in how business leaders are viewing cybersecurity and technology – no longer seeing technology as a threat and understanding that cybersecurity is a vital component that must be adopted into the business framework. To remain competitive, organisations today must make a budgetary commitment to the integration of cybersecurity with digitisation from the outset.

Survey results also found that as trust in cloud models deepens, organisations are running more sensitive business functions on the cloud. Today, the majority of organisations around the world—63 per cent of survey respondents—say they run IT services in the cloud. Additionally, approximately one-third of organisations surveyed were found to entrust finance and operations to cloud providers, reflecting the extent to which trust in cloud models is growing.

The fusion of advanced technologies with cloud architectures can empower organisations to quickly identify and respond to threats, better understand customers and the business ecosystem, and ultimately reduce costs. Cloud models have become more popular in recent years, and that trend will likely only continue as the benefits become increasingly clear.

According to survey respondents, organisations are also embracing both managed security services and open-source software to enhance cybersecurity capabilities, signalling that businesses are making cybersecurity a priority despite many not having the necessary in-house capabilities and lacking the talent required to fill key positions. More than half (53 per cent) of respondents employ open-source software and 62 per cent of respondents say they use managed security services for cybersecurity and privacy – relying on managed security services for highly technical initiatives such as authentication, data loss prevention and identity management.



Designing and implementing a cybersecurity and privacy programme is challenging enough, but once a programme is in place components must be thoroughly integrated, professionally managed and continuously improved. As this can be difficult for resource-constrained organisations, many are adopting managed security services and utilising open-source software.

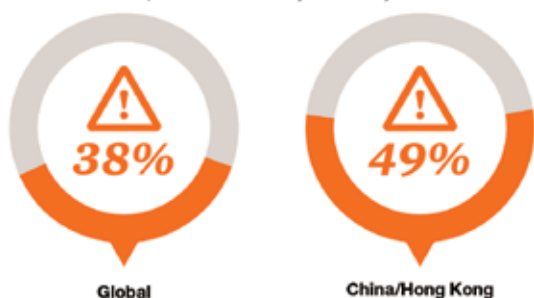
The survey responses in Mainland China and Hong Kong also indicate severe cybersecurity challenges. The average number of detected security incidents by survey respondents in Mainland China and Hong Kong reached 2,577 in 2016, marking a 969 per cent increase from 2014, and more than double the average recorded for 2015. The increasing domestic trend contrasts with global survey data which points to a slight decline, with a total worldwide average of 4,782 detected incidents reported in 2016, reflecting a three per cent drop from the global average number of detected incidents reported since 2014.

In terms of investment, survey responses indicate a decrease was seen in information security budgets by companies from Mainland China and Hong Kong in 2016, with a 7.6 per cent reduction compared to the previous year. Nevertheless, 88 per cent of those respondents acknowledged that digitisation has impacted their information security spending in 2016, and highlighted cybersecurity alignment with business strategy and security governance as the top priority for such spending over the period. Additionally, 31.5 per cent of respondents from Mainland China and Hong Kong registered a specific intention to invest in advanced security technologies including artificial intelligence (AI) and machine learning technologies.



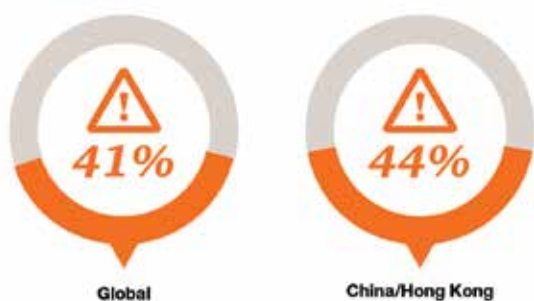
We can see forward looking organisations in the domestic market are investing in advanced cybersecurity to define and defend their own differentiated value, while safeguarding paths to robust business growth.

49% of respondents in China/Hong Kong cite business email compromise as the leading impact of incidents, while phishing becomes the top attack vector of cybersecurity incidents.



With regard to the nature of security incidents, 49 per cent of respondents from Mainland China and Hong Kong cited phishing as the top vector for cybersecurity issues over the last year, while business email formed the biggest impact of incidents for the period. Once again, the role of insiders was flagged as the most common source of detected incidents. Business insiders accounted for 44 per cent of all detected security incidents that were reported by respondents in Mainland China and Hong Kong this year. The figure reflects an increase from the 40 per cent attributed to insiders in the prior year, and stands above the global average of 41 per cent of incidents attributed to insiders in 2016. Also of note, 34 per cent of domestic respondents experienced security incidents attributed to competitors, markedly higher than the global average of 23 per cent.

Number of respondents that experienced incidents attributed to insiders has continued increasing.



As organisations face evolving opportunities and threats, steps to strengthen cybersecurity with Internet-of-Things-connected devices have become mainstream, along with the allocation of sensitive business functions to the cloud. Data for 2016 shows 57 per cent of survey respondents in Mainland China and Hong Kong are investing in a security strategy for the Internet of Things and 45 per cent of all IT services now run via cloud service providers, which compare to 46 per cent and 48 per cent with global respondents respectively.

Concurrently, both managed security services and open-source software are increasingly used to enhance capabilities, including cybersecurity, with some 75 per cent of respondents from Mainland China and Hong Kong documenting that they employ open-source software, compared to 53 per cent of respondents globally.

We are seeing more companies taking steps to develop their IT security systems in response to the real and rising threat of cyber risks. Adaptation of cloud technologies and open-source software signal how businesses are making cybersecurity a priority, despite not necessarily having the in-house capabilities in place just yet. While encouraging, companies will need to ensure their technology can keep up with these growing cybersecurity threats. **Eb**

At **PwC**, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services.

**Samuel Sinn** has more than 25 years of experience in providing information security, IT risk management and IT audit services to state-owned enterprises, listed companies and multinational corporations in China, Hong Kong and the United States. He has extensive experience in advising on technology risk management within the financial services industry, as well as exposures to industries, including telecommunication, technology and manufacturing.

The Global State of Information Security® Survey 2017 (GSISS 2017) was launched in China in November 2016, with China observations. GSISS 2017 is a worldwide study by PwC, CIO and CSO Magazine, which was conducted online from April 2016 to June 2016. GSISS 2017 is conducted among readers of CSO and CIO Magazine and clients of PwC from 133 countries, with responses from more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices worldwide. Forty-eight per cent of respondents from organisations with revenue of USD500 million+, while more than 40 questions on topics related to privacy and information security and how businesses are implementing innovative new safeguards. Locally we have got 440+ respondents from China/Hong Kong.





# GO WITH THE FLOW

## Cross-border data transfer: a China perspective

Before China enacted its new Cybersecurity Law on 7<sup>th</sup> November, 2016, cross-border data transfer was largely unregulated by the government. While many Chinese laws and regulations governed the collection, use and storage (including localisation) of data, no binding laws or regulations contained generally applicable legal requirements or constraints on the transfer of data across Chinese borders. **Yan Luo** of **Covington & Burling LLP** explains the changes proposed by the law and discusses potential data transfer compliance strategies that companies can adopt to comply with the new Chinese data transfer requirements.



## Cybersecurity Law: before and after

Once the Cybersecurity Law (the Law)<sup>1</sup> takes effect on 1<sup>st</sup> June, 2017, the regulatory landscape for cross-border data transfer will change completely: China will become another important jurisdiction to watch in the international data transfer space.

Before the Law was officially promulgated, China had already started efforts to consolidate its jurisdiction over data by imposing data localisation requirements in many industry-specific regulations.<sup>2</sup> However, there existed no comprehensive framework for regulating cross-border data flow.

A voluntary, non-binding national standard was issued in 2012 – the *Guidelines for Personal Information Protection within Public and Commercial Services Information Systems* (GB/Z 28828-2012) (*Guidelines*).<sup>3</sup> The *Guidelines* provided that “absent express consent of the personal information subject, or explicit legal or regulatory permission, or absent the approval of the competent government agencies, the administrator of personal information shall not transfer personal information to an overseas recipient of personal information, including an individual located overseas or an organization or institution registered overseas.” The *Guidelines*, however, lack the force of law and did not gain traction in practice.

Article 37 of the Law, for the first time expressly requires that operators of Critical Information Infrastructure (CII) store within China “citizens’ personal information and important data” collected or generated in the course of operations within the country.<sup>4</sup> If transfers of data offshore are necessary for operational reasons, a security assessment must be conducted by designated agencies, unless otherwise regulated by laws and regulations.<sup>5</sup>

The Law defines CII broadly as “infrastructure that, in the event of damage, loss of function, or data leak, might seriously endanger national security, national welfare or the livelihoods of the people, or the public interest”. Specific reference is made to ‘key sectors’ such as telecommunications, financial services, transportation and e-government.<sup>6</sup> This definition is sufficiently broad to potentially cover many sectors and industries. The Cyberspace Administration of China (CAC), the agency tasked with implementing the scheme, is expected to issue an implementing regula-

tion in the next six months to offer more guidance on the scope of CII.

## Data localisation vs data transfer

The CAC indicated in press reports that to protect China’s CII, personal information of Chinese citizens and “important data” collected and generated by CII operators should in principle be stored onshore.<sup>7</sup> Transferring data offshore can only be done if “absolutely necessary” and must “follow rules”.<sup>8</sup> To ensure “orderly” cross-border data transfer, when deciding whether to approve a data transfer requirement, the agency will primarily consider whether at the destination, Chinese data is properly safeguarded post-transfer.<sup>9</sup>

The CAC is expected to issue an implementing regulation that governs the security assessment prescribed by Article 37. While awaiting the formal issuance of the implementing regulation, we examine below potential requirements for the transfer of two different groups of data: personal information of Chinese citizens and ‘important data’.

## Cross-border transfer of personal information of Chinese citizens

The CAC is yet to provide any details on how it plans to evaluate whether foreign countries, organisations or individuals are “willing and capable of” safeguarding Chinese citizens’ personal information.<sup>10</sup> There is also no indication that the CAC will, in the near future, recognise that any specific countries can afford an adequate level of protection and thus automatically allow the transfer of data to such countries.

Without recognition of other countries’ data protection regimes, the CAC is likely to devise a data transfer mechanism that relies on CII operators’ commitments or binding contractual obligations to ensure that personal information is sufficiently protected outside of China. Although there is currently a lack of specifics, it is possible that at least some elements of this mechanism will be comparable to the European Union’s (EU’s) *Model Contracts and Binding Corporate Rules* (BCR) or Asia-Pacific Economic Cooperation’s (APEC’s) *Cross Border Privacy Rules* (CBPR) system.

The CAC has also not provided any details on what contractual arrangements or company internal rules and procedures can satisfy the agency’s requirements if companies are required to robustly protect Chinese citizens’ personal information outside of China. One potential benchmark is the *Information Security*

<sup>1</sup> *Cybersecurity Law of the People’s Republic of China*, effective 1<sup>st</sup> June, 2017.

<sup>2</sup> Stratford, Tim & Luo, Yan, *3 Ways Cybersecurity Law In China Is About To Change*, Law360, 2<sup>nd</sup> May, 2016, <<https://www.law360.com/articles/791505/3-ways-cybersecurity-law-in-china-is-about-to-change>>

<sup>3</sup> *Guidelines for Personal Information Protection within Public and Commercial Services Information Systems* (GB/Z 28828-2012), jointly released by the General Administration of Quality Supervision, Inspection, and Quarantine and the Standardization Administration of China, 5<sup>th</sup> November, 2012, effective 1<sup>st</sup> February, 2013.

<sup>4</sup> Article 37 of the Law.

<sup>5</sup> Data transfer requirements imposed by other laws and regulations will be ‘grandfathered’ by the Law. However, requirements imposed by department rules and local regulations are beyond the scope of this article.

<sup>6</sup> Article 31 of the Law.

<sup>7</sup> *CAC is Enacting Regulations on the Evaluation of Cross Border Transfer*, New Beijing Paper, 8<sup>th</sup> December, 2016, <<http://www.bjnews.com.cn/feature/2016/12/28/428788.html?from=timeline&isappinstalled=0>>

<sup>8</sup> Ibid

<sup>9</sup> Ibid

<sup>10</sup> Ibid

<sup>11</sup> *Information Security Technology – Personal Information Security Specification (Draft)*, National Information Security Standardization Technical Committee, 20<sup>th</sup> December, 2016, <[http://www.tc260.org.cn/zyjfb.jsp?norm\\_id=20160628214349&recode\\_id=21042&idea\\_id=20161221094921&t=0.20651056670257484](http://www.tc260.org.cn/zyjfb.jsp?norm_id=20160628214349&recode_id=21042&idea_id=20161221094921&t=0.20651056670257484)>

*Technology – Personal Information Security Specification* (the *Standard*), a new national standard proposed by the CAC.<sup>11</sup> The *Standard* establishes a comprehensive data protection framework for regulating the collection, storage, use, transfer (within China) and disclosure of personal information, and adopts eight principles identical to the Organization for Economic Co-operation and Development's (OECD's) privacy principles.<sup>12</sup> Although not legally binding, such a national standard can provide companies with useful insight into what Chinese regulators may consider to be best practice in protecting personal information. If a company were to ensure that its handling of personal information outside of China also meets requirements articulated in the *Standard*, it could be easier to argue that the protection of Chinese citizens' personal information is adequate, wherever data is processed.

## Cross-border transfer of 'important data'

Cross-border transfer of 'important data' will, however, be evaluated differently. The CAC has yet to fully define 'important data', although it is commonly understood as data relating to China's national security, which by itself is a sweeping concept under China's National Security Law.<sup>13</sup>

Chinese laws and regulations in two other areas could offer some clues regarding how the agencies may interpret this term, even though it is difficult to determine categorically which data falls within its scope. Any near-term assessment of the coverage of 'important data' will have to be made on a case-by-case basis.

The first law is China's Law on Guarding State Secrets (State Secrets Law).<sup>14</sup> Under this law and its implementing regulations, 'state secrets' are prohibited from leaving China.<sup>15</sup> The State Secrets Law offers a non-exclusive list of categories deemed 'state secrets', including, for example, information involving national defence construction and activities of the armed forces, diplomatic and foreign affairs activities, and activities related to national security investigations.<sup>16</sup> Examples of information that the government in the past considered as 'state secrets' include certain government statistics, geographical data about infrastructure, certain law enforcement activities and certain information on natural resources.

The second set of rules relates to China's export control regime. Similar to many other countries, China maintains a system that controls the export of munitions, military products and other dual-use goods and


technologies. Transfer of data related to products and technologies that are covered by the export control regime is expected to be banned or be subject to heightened scrutiny.

## Global data transfer compliance strategies: how does China fit in?

With China joining the club of countries regulating cross-border data flows, more compliance challenges lie ahead for companies that may be covered by Article 37 of the Law.

Setting aside the transfer of 'important data', which is likely to be subject to a case-by-case assessment, companies that transfer Chinese citizens' data into and out of China on a regular basis can consider taking steps to comply with the potential Chinese requirements, even though we still lack official guidance from the agencies.

For example, it is important that companies first have a good understanding of their data collection and flows into and out of China. They can then assess whether there is a need to supplement existing data protection compliance programmes in certain aspects, in anticipation of the new Chinese requirements.

Beyond China, when considering implementing a global data transfer strategy, it is also advisable to take the potential Chinese requirements into account up front. Although we cannot exclude the possibility that there may be (significant) differences between the future Chinese transfer mechanism and other regimes, such a mechanism may well share certain principles and characteristics of 'modern' data transfer regimes such as the BCR and the CBPR. Therefore, companies can potentially deploy a single, global data governance process that satisfies regulatory requirements in China and other jurisdictions at the same time. Investing in advance is likely to be a better strategy than being forced to adopt convoluted data protection policies specifically for Chinese citizens if and when transferring Chinese data for offshore processing later becomes necessary. 

*For nearly 100 years, **Covington** has been the preeminent law firm in dealing with the US Government. In the age of globalisation, Covington has expanded internationally to meet the challenges its clients face dealing with governments and regulatory regimes in key markets around the world.*

*Covington's Public Policy and Governmental Affairs Group (PPGA) draws on Covington's distinctively collaborative culture and unparalleled regulatory expertise and combines it with global reach. Our policy team of more than 50 members covers the globe, with extensive networks in key cities and regions, including: Washington, D.C., London, Brussels, the Middle East, Beijing, Shanghai, Seoul, Latin America and Africa.*

<sup>12</sup> Luo, Yan, *China Releases Seven Cybersecurity and Data Protection National Standards*, *InsidePrivacy*, 21<sup>st</sup> December, 2016, <<https://www.insideprivacy.com/international/china/china-seeks-comment-on-seven-draft-cybersecurity-and-data-privacy-national-standards/>> <sup>13</sup> National Security Law, effective 1<sup>st</sup> July, 2015.

<sup>14</sup> Law on Guarding State Secrets, effective 1<sup>st</sup> October, 2010.

<sup>15</sup> Article 9 of the State Secrets Law defines a 'state secret' broadly as a "matter that relates to the national security and interests as determined under statutory procedures and to which access is vested in a limited range of persons during a given period of time."

<sup>16</sup> *Ibid*



# DIGITAL DOS AND DON'TS

## China's e-commerce market restrictions for foreign SMEs

While China's e-commerce market presents a huge opportunity for foreign-invested enterprises (FIEs), there are a number of often complex restrictions that FIEs should be aware of. **Daniel Albrecht**, Director, **Starke**, provides an overview of the rules that they need to abide by, including those pertaining to enterprises that utilise mobile Apps as part of their business model. Of particular importance, he says, is the way that foreign enterprises are structured if they are to operate in China's e-commerce sector and remain compliant.



## China's e-commerce market

The China Internet Network Information Centre (CNNIC) reported 710 million Internet users in June 2016, and according to analysis by digital marketing researcher eMarketer, cross-border e-commerce in China was due to hit USD 85.76 billion in 2016, up from USD 57.13 billion in 2015. Notably, 40 per cent of China's online consumers are buying foreign goods.

eMarketer further estimated that each of China's digital shoppers would have spent an average of USD 473.26 in 2016. Its projections that cross-border e-commerce will have a compound annual growth rate of 18 per cent through to the end of the decade—reaching an estimated USD 222.3 billion—would mean that China's e-commerce market will become larger than those of the US, Britain, Japan, Germany and France combined by 2020.

## Internet Service Standards

All internet service providers (ISPs), whether foreign-invested or domestic, are subject to the provisions under the *Supervision of the Market Order of Information Services*, introduced in December 2011. It prohibits ISP enterprises from certain practices that are harmful to other ISPs, such as defaming other ISPs or making its platform incompatible with those of another ISP. Practices that are harmful to Internet users are also prohibited under the provisions.

On top of these provisions came the addition of the guidelines *Services Norms for E-commerce Trading Platforms*, which were issued in April 2014. These set out basic rules for the operation of trading platforms and requirements relating to the collection and retention of data, the verification of user's identities and fair trading practices in general.

Participants in this sector should keep in mind that the government will take a harder line on policing and taking action against ISPs and Internet businesses for non-compliant behaviour.<sup>1</sup>

Moreover, ISPs will be held more accountable for supervising their users' activities, which is also a feature of the National Copyright Administration's draft amendments to the PRC Copyright Law. Under the draft law, ISPs would be jointly liable for copyright infringement when they have been notified of an infringement but have failed to promptly delete, block or disconnect the offending content. The draft amendments also stipulate that ISPs would face joint liability if it is proved that they know, or should have known, about the infringement but have failed to undertake the necessary steps to stop it.<sup>2</sup>

<sup>1</sup> *E-Commerce in China: How can you get a piece of the action?*, Freshfields Brukhaus Deringer, September 2014, p.4, <<https://communications.freshfields.com/files/uploads/documents/external%20mailings/all%20other%20regions%20and%20offices/china/Freshfields%20E-Commerce%20in%20China%20briefing.pdf>>

<sup>2</sup> Ibid, p.5

## Telecommunications

Foreign participation in a range of Internet and e-commerce activities comes under the far-reaching PRC *Telecommunications Regulations*.<sup>3</sup> While the establishment of a foreign-invested, value-added telecoms services (VATS) enterprise is possible, with up to a maximum 50 per cent foreign investment, few joint ventures have emerged in this sector.<sup>4</sup>

However, the now well-known variable interest entity (VIE) structure has been repeatedly used to support foreign participation in PRC e-commerce businesses.<sup>5</sup> Under the VIE structure, a complex contractual arrangement is put in place under which the required VATS licence is held by a Chinese company, which is owned by a domestic company under the ownership of PRC nationals, who pledge their ownership of the domestic company to the foreign party and allow the VATS licence to be used for the foreign party's benefit.

There are strict measures surrounding the devial of any telecoms company in China and all must abide by the strict rules and regulations laid out in the *Measures for the Administration of Telecom Business Licensing* if they are to successfully operate in China and remain compliant. In order to even apply to operate a telecoms business, the criteria laid out in the *Telecommunications Regulations* must be adhered to, and all required documentation must be submitted to the China's Ministry of Industry and Information Technology (MIIT) to apply for a basic telecoms business permit. Even after the permit has been awarded, it must still be renewed every five years.

While the VIE structure appears to be broadly tolerated by the Chinese Government and is widely used in the e-commerce sector, the highest level official pronouncement by the MIIT, the 2006 *Circular on the Strengthening of the Administration of the Provision of Value Added Telecommunications Services Involving Foreign Investment*, states that FIEs must receive foreign investment approval to participate in VATS, and that VATS licencees are prohibited from lending their VATS licences to foreigners.

This circular was followed more recently by the publication of the government's provisions on the national security review, effective as of September 2011, which set out that a foreign investor cannot use contractual control arrangements (i.e. the VIE structure) to avoid the government's national security review and approval requirements.

The VIE structure raises risks for investors, including the ultimate risk that government authorities may require the structure to be unwound. If the government

<sup>3</sup> Ibid, p.2

<sup>4</sup> Ibid

<sup>5</sup> Ibid



were to issue a comprehensive ban of the VIE structure altogether, it would have a significant impact on the e-commerce sector in particular.

It should be noted that some Chinese regulators appear to be more overtly concerned with the VIE structure than others. Although FIEs that only engage in online sales of their own products and do not provide Internet services or platforms to third parties over the public switched telephone network do not require a VATS licence, they must still apply for an Internet content provider (ICP) approval or filing from the MIIT if the relevant content of their website is stored on a server located in China.

An ICP approval is required if the website directly generates revenue. If the website does not generate revenue, only an ICP filing is needed. However, it is important to note that the applicant for an ICP filing must be a Chinese entity with a local address, which in practice means that foreign businesses that do not have a presence in China often engage their local Chinese business partners or hosting service providers to apply for the ICP filing on their behalf.

In addition, the foreign business must obtain approval to establish its entity in accordance with the foreign investment laws that apply to its business sector, and the products and services it offers must be approved by, and registered with, the relevant state department.

## Mobile Apps in China

Developing an App is an excellent way to utilise China's thriving mobile technology. However, as of 2016, the rules and regulations surrounding Apps in China became

more stringent. The *Rules on the Management of Mobile App Information Services (App Rules)* were passed by the Cyberspace Administration of China (CAC) and came into effect on the 1<sup>st</sup> August, 2016.

Regulating the rapidly growing App market and addressing corresponding data privacy issues are the primary objectives of the *App Rules*.<sup>6</sup> Among other things, they impose cybersecurity, data privacy and content monitoring requirements on App and App store providers. According to Article 7, App providers are required to authenticate the identities of their users. Furthermore they are required to obtain "relevant qualifications" (Article 5), a term that is not specified but can be interpreted as 'licences' required under other laws and regulations that especially regulate the type of service rendered by a given App.<sup>7</sup> Moreover, providers have the duty to adhere to certain data privacy rules and establish systems for monitoring content on their platforms (Article 7). [Eb](#)

**Starke** was founded by **Daniel Albrecht**, a German attorney at law and Guest Professor of the China University of Political Science and Law. Starke operates in Beijing and in six cities in Germany through cooperation with its partner, Jordan Fuhr Meyer. Core competencies are legal advisory and IP. Starke is a Trademark Agent licensed by the State Administration and Commerce. With several years of experience in Asia we customise our advisory activities to the requirements of international companies and individuals who require advice on corporate, IP, contract and labour issues.

<sup>6</sup> *China Issues New Rules for Mobile Apps* by Ashwin Kaja and Eric Carlson, Covington, 1st July 2016, <<https://www.insideprivacy.com/international/china/china-issues-new-rules-for-mobile-apps/>>

<sup>7</sup> Ibid



# PROTECTING YOUR PRIVACY

## Private data protection in China

The rapid evolution of internet technology has necessitated the definition of 'personal private information' being expanded. While traditionally it included names, ID numbers, phone numbers, bank accounts and addresses, the definition now encompasses text messages, social media accounts and passwords, online transaction records and shopping and travel information, and with more personal information out in cyberspace comes more opportunity for data theft. **Richard Zhang**, Director of Management Consulting, **KPMG China**, explains what the Chinese Government has done so far to tackle this problem, and says that preventative measures are only likely to increase, in the near term at least.



## The rising challenge

Private information is used in many situations – booking flight or train tickets, checking in at a hotel, getting a credit card from the bank, purchasing insurance products or visiting a hospital. There is a high probability that personal information could be exposed and collected during these processes. In some cases, the collected information could possibly be illegally used for activities such as insurance telemarketing, advertising or even telecom fraud.

The issue of privacy protection has raised huge challenges for the Chinese Government, and existing measures to protect privacy and restrict the collection and usage of private information still need to be strengthened.

## Personal information crime: the facts

Over the past decade, telecom fraud in China has been increasing at an annual rate of 20 to 30 per cent.<sup>1</sup> In the first seven months of 2016 alone, around 355,000 cases of telecom fraud were recorded, an increase of 36.4 per cent compared with 2015. These cases have directly resulted in a loss of CNY 11.4 billion.<sup>2</sup> Some of the crimes and incidents have caused a significant social impact along with substantial financial loss:

- In August 2016, a teenager died due to a heart attack after her university tuition fee was stolen during a targeted telecom fraud.<sup>3</sup>
- In September 2016, a college professor lost around CNY 17 million, also a victim of targeted telecom fraud.<sup>4</sup>

These incidents quickly drew national focus, putting great pressure on the government. Similar tragedies have occurred, with most of these incidents occurring because personal information was leaked and utilised during telecom fraud.

The Chinese Government has been fighting against personal information crime, especially telecom fraud. By October 2016, the government had solved 93,000 related crimes, preventing the loss of CNY 4.87 billion. In addition to fighting crime, the government is also looking into the root causes and is working on improving the laws and regulations in order to better protect personal information.<sup>5</sup>

## Existing laws and regulations

The Chinese Government has published several laws and regulations in which the requirements for protecting private information have been raised, and important terms have been defined:

- Organisations should establish and enforce information security management policies and procedures to protect systems and data – *Computer Information System Security Protection Ordinance* (enacted in 1994).
- Definition of ‘consumer personal information’ is provided – *Consumer Protection Law* (first enacted in 1994, amended in 2013).
- Consent from consumers should be obtained before collecting consumer personal information – *Measures for Penalties for Infringing upon the Rights and Interests of Consumers* (enacted in 2015).
- Definition of ‘user personal information’ is provided – *Several Provisions on Regulating the Market Order of Internet Information Services* (enacted in 2012).
- Organisations providing Internet services (e.g. company websites) should protect their collected user personal information – *Guidelines of Protecting Telecommunication and Internet User Information* (enacted in 2013).

Moreover, the Cybersecurity Law was adopted at the National People’s Congress in November 2016, after a year of legislative process, and is scheduled to become effective from June 2017. Critical articles for privacy protection under the new law include:

- **Article 22:** Where network products and services have functions to collect user information, the provider shall indicate this to users and obtain agreement; where citizens’ personal information is involved, this shall abide by the provisions of this Law, as well as relevant laws and administrative regulations, concerning the protection of citizens’ personal information.
- **Article 41:** Network operators collecting and using personal information shall abide by principles of legality, propriety and necessity, disclosing their rules for its collection and use, explicitly stating the purposes, means and scope for collecting or using information, and obtaining the consent of the person whose data is gathered.

<sup>1</sup> <http://news.163.com/16/1128/10/C6UV6HT200014Q4P.html>

<sup>2</sup> <http://news.qq.com/a/20160913/051491.htm>

<sup>3</sup> <http://tech.sina.com.cn/t/2016-08-30/doc-ifyxixer7496083.shtml>

<sup>4</sup> <http://news.mydrivers.com/1/500/500560.htm>

<sup>5</sup> <http://news.163.com/16/1227/10/C99LH55M00018A0Q.html>

- **Article 44:** Individuals or organisations must not steal or use other illegal methods to acquire personal information, and must not sell or unlawfully provide others with citizens' personal information.

The Cybersecurity Law proffers specific requirements regarding the collection, use and protection of private information. The above articles clarified requirements for the collection of personal information, emphasising that personal information can only be collected after the user agrees to its purpose, method and scope.

## Industrial privacy protection requirements

From an industrial perspective, the level of private information protection varies based on different industries:

- The regulatory authorities in the finance industry, such as the China Banking Regulatory Commission (CBRC) and the People's Bank of China (PBOC), have been emphasising protection of personal information. In December 2016, the PBOC released a new regulation to protect the rights of financial consumers. The policy clearly states that private information obtained through financial business processes should be kept confidential. Illegal use/copy/storage/leaking of private information is prohibited. This regulation could be viewed as an enforcement measure in the finance industry following the privacy protection requirements raised in the Cybersecurity Law.
- For the telecom industry, in 2013, the Ministry of Industry and Information Technology (MIIT) released regulations to protect the personal information of telecom and internet users. The policy has stated the security requirements for telecom companies while collecting and using client personal information. This regulation has been the foundation for fighting against telecom fraud crimes.
- For other industries (like healthcare and education), though currently the supervision is not as strong as in the financial and telecom industries, the authorities are aware of the importance of protecting personal information. Following the enactment of the Cybersecurity Law, we can foresee that regulators will likely publish a series of industry-wide regulations to enhance the protection of personal information.


## Privacy protection in the future

Privacy protection will continue to be a hot topic going forward. Both government and other organisations will

need to step forward and continue to work on feasible privacy protection practices.

From a governmental perspective, as the Cybersecurity Law will become effective in June 2017, the Chinese State Council, the MIIT and other related industrial regulators will likely publish regulations and guidelines containing more detailed and practical requirements for privacy protection.

From an organisational perspective, if personal information is to be collected and used during the business process, the organisation will need to comply with the privacy protection requirements raised in the Cybersecurity Law and other detailed regulations. For instance, healthcare organisations in China will likely face regulations similar to the Health Insurance Portability and Accountability Act (HIPAA) to protect the privacy of patients; financial organisations will likely face stricter regulations, perhaps similar to the European Commission's *General Data Protection Regulation* (GDPR), on the collection and use of client personal information.

Regardless of what China's privacy protection requirements will be in the future, the overall trend is that privacy protection is becoming stricter, and companies and organisations will certainly be required to meet these protection requirements. 

For more information please contact: Richard Zhang @ Richard.zhang@kpmg.com (+21 2212 2637)

**KPMG** is a global network of independent member firms offering audit, tax and advisory services. The firms work closely with clients, helping them to mitigate risks and grasp opportunities.

Member firms' clients include business corporations, governments and public sector agencies and not-for-profit organizations. They look to KPMG for a consistent standard of service based on high order professional capabilities, industry insight and local knowledge.

KPMG member firms can be found in 152 countries. Collectively they employ more than 189,000 people across a range of disciplines.

Sustaining and enhancing the quality of this professional workforce is KPMG's primary objective. Wherever our firms operate, we want them to be no less than the professional employers of choice.



# THE ADVISORY COUNCIL OF THE EUROPEAN CHAMBER

The members of the European Chamber's Advisory Council are particularly active in representing and advising the Chamber, and make an enhanced contribution to the Chamber's funding.





# EUROPEAN CHAMBER LOBBYING HIGHLIGHTS

---

---



## Lobbying SIPO Vice Commissioner for IPR Protection

Chamber President Jörg Wuttke led a delegation to meet Vice Commissioner He Zhimin of China's State Intellectual Property Office (SIPO) on 16<sup>th</sup> November, 2016. Mr He outlined past IPR-related cooperation between the SIPO and the EU, and President Wuttke responded by expressing the Chamber's appreciation for the support that the SIPO has provided over the years. The Chamber delegation raised a number of specific concerns regarding IPR protection related to the implementation of the new Cybersecurity Law, as well as questions related to IPR enforcement more generally, which SIPO officials responded to. President Wuttke took the opportunity to present a copy of the Chamber's *Position Paper 2016/2017* to Vice Commissioner He, who agreed to send SIPO officials to attend relevant meetings and events organised by the Chamber.

## Four Foshan Bureaus Engage with the Chamber

On 29<sup>th</sup> November, the Chamber's South China Chapter co-organised a working-level session with Foshan Municipality's bureaus for commerce, human resources and social security, intellectual property and tax. The purpose of the event was to address specific issues concerning European companies operating in Foshan

and to learn more about new projects and initiatives that are currently being undertaken in the city. After a fruitful discussion the event concluded with Deputy Manager of the South China Chapter Anna Rudawska presenting copies of the *Position Paper 2016/2017* to representatives of each of the participating bureaus.

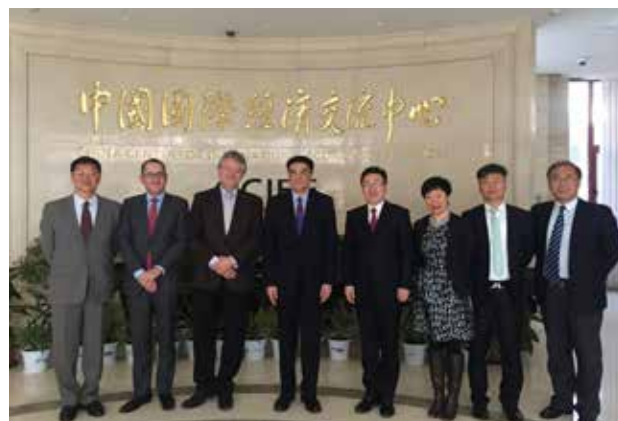
## Talking Reciprocity with President Li Wei of the SCDRC

President Li Wei of the State Council Development Reform Commission (SCDRC) received a major Chamber delegation on 30<sup>th</sup> November. President Jörg Wuttke conveyed to President Li the key messages from the Chamber's *Position Paper 2016/2017*, as well as those from the position papers recently released by the Chamber's local chapters. He then outlined European business' need for reciprocity in EU-China trade and investment relations as well as the value of allowing it to participate in the China Manufacturing 2025 initiative as a full partner. President Li commented on trends in EU-China bilateral trade and investment relations and stated that there is still considerable room for further development. Concerns of specific industries were conveyed to President Li and the two sides agreed that a successful conclusion to negotiations for the Comprehensive Agreement on Investment (CAI) can make a valuable contribution to bilateral economic ties.



## CCIEE Executive Vice Chairman Sees Need to Increase EU-China Trade and Investment

On 2<sup>nd</sup> December, 2016, a Chamber delegation led by President Wuttke met with Executive Vice Chairman Zhang Xiaoqiang of the China Centre for International Economic Exchanges (CCIEE). President Wuttke outlined the key messages of the Chamber's *Position Paper 2016/2017*, including the need for reciprocity in EU-China trade and investment relations, priorities in negotiations for the Comprehensive Agreement on Investment and the need for the China Manufacturing 2025 initiative to be driven by market forces. Executive Vice Chairman Zhang recognised the imbalance in two-way trade and investment between the EU and China and said that increasing bilateral investment will be of benefit to both sides. He also shared updates on cooperation between the CCIEE and two EU-based



think tanks as well as recent developments in dual-track dialogues between China and the EU.

## Chamber Discusses Anti-monopoly with the NDRC

On 7<sup>th</sup> December, Serafino Bartolozzi, Chair of the Chamber's Auto Components Working Group, met with Mr Xu Xinyu, Division Director of the National Development and Reform Commission's (NDRC's) Bureau of Price Supervision and Anti-monopoly. Their talks focused on opportunities to further strengthen cooperation, with the details of the Anti-monopoly

Guidelines for the auto sector discussed at length. The *Auto Components Position Paper 2016/2017* was presented to Division Director Zhang, who indicated his interest in incorporating some of its findings in the bureau's annual report. The two sides agreed to be in further contact in early 2017.



# A GAME CHANGER?

## The PRC Foreign NGO Law

The Law of the PRC on Management over Foreign NGOs' Activities in China (Foreign NGO Law), took effect on 1<sup>st</sup> January, 2017. It is the third of a series of laws that were proposed in 2015 to address the growing concerns of China's leadership about national security and foreign interference with China's domestic affairs.<sup>1</sup> **Sherry Gong** and **Sherry Hu** of **Hogan Lovells** examine the law and find that the final version includes some improvements from previous drafts and appears to relax certain previously proposed restrictions and burdens on foreign NGOs' activities in China. However, they also note that many issues are still not properly addressed.

<sup>1</sup> The other three are: (i) the National Security Law, which became effective from 1<sup>st</sup> July, 2015; (ii) the Anti-terrorism Law, effective from 1<sup>st</sup> January, 2016; and (iii) the Cyber Security Law, the draft of which was released for public comments on 6<sup>th</sup> July, 2015.



Following the adoption of the Foreign NGO Law, the Ministry of Public Security (MPS)—the registration and administration authority of foreign NGOs—issued two main implementing rules: (i) the *Guidelines on the Registration Procedures for Representative Offices and Record-Filing for the Temporary Activities of Foreign NGOs (Registration Guidelines)* on 28<sup>th</sup> November, 2016; and (ii) the *Catalogue of Areas and Projects for the Activities in China of Foreign Non-Governmental Organisations, and the Catalogue of Supervisory Authorities for Foreign Non-Governmental Organisations (2017) (National Catalogue)* on 20<sup>th</sup> December, 2016. Some local MPS at the provincial level (e.g., Guangdong Province, Shanghai and Tianjin) have also formulated and published their own catalogue applicable within their jurisdictions (the *Local Catalogues*). These are basically the same as the *National Catalogue*, except they specify the supervisory authorities as being the counterpart authorities at the provincial level.

## New regulatory scheme for foreign NGOs' activities in China

### *Two paths to conduct activities in China*

Foreign NGOs will now only be able to conduct activities through one of two paths in China:

1. Through a foreign NGO's representative office (RO) in China, which is the only type of legal form that Foreign NGOs are allowed to establish in China under the Foreign NGO Law.
2. As a 'temporary activity' approved by and filed with the relevant authorities (such record-filing is valid for up to one year unless a new record filing is done with the local MPS at the provincial level).

### *Dual-layer approval and registration mechanism*

The Foreign NGO Law sets out a 'dual layer' of supervision over foreign NGOs' activities in China. As to the first layer: (1) for establishing a RO, the foreign NGO shall secure the approval from the supervisory authority (listed in the *National Catalogue* and the *Local Catalogues*); or (2) for carrying out temporary activities, a foreign NGO is required to be sponsored by a Chinese partner (which can be a government agency, a people's organisation, a public institution or a social organisation), who must then obtain the relevant authorities' approval of such temporary activities.

The second layer falls under the authority of the MPS and its branches at provincial level, and consists of either its approval of the registration application for a RO establishment or the record filing with the MPS for the temporary activities.

## Unclear scope of carve-out

The Foreign NGO Law includes the following, rather vague definition of a foreign NGO: "non-profit, non-government social organisations that have been legally established outside China, such as foundations, social organisations, and think tanks, etc."<sup>2</sup> Particularly unhelpful is the inclusion of "etc." as part of the definition.

Although the Foreign NGO Law also introduces a carve-out as provided under Article 53 (Carve-out Provision),<sup>3</sup> with the scope broadened compared to the previous draft, it can still end up leaving more questions than it resolves. Instead of simply exempting foreign schools, hospitals and research institutions and academic organisations from the definition of foreign NGOs, the Carve-out Provision only specifically lists exchange and cooperation activities between foreign and domestic schools, hospitals, natural science and engineering research institutions or academic organisations.

Thus, foreign schools, hospitals, natural science and engineering research institutions and academic organisations with a domestic counterpart in compliance with applicable PRC laws can take some comfort that they do not require registration as a foreign NGO's representative office, nor do they need to secure an approval and record filing for temporary activities from the relevant government agencies under the Foreign NGO Law. However, at the same time, they must refrain from engaging in or providing financial support to for-profit activities, political activities and illegally supporting or sponsoring religious activities. More troubling is whether any other activities of foreign schools, hospitals, research institutions or academic organisations that are not engaged in exchange or cooperation with a domestic counterpart, or research institutions or academic organisations that are engaged in exchanges or cooperation that fall outside of the scope of "natural sciences or engineering"—even when they have a domestic counterpart—are subject to the substantive requirements of the Foreign NGO Law.

These ambiguities remain even after the release of the *Registration Guidelines* and the *National Catalogue* (as well as some *Local Catalogues*). In particular, the *National Catalogue* lists education as one of those nine areas, and is further divided into four sub-areas, each covering certain main projects (Education Section). The Ministry of Education and its local, provincial departments (collectively, the MOE) are listed as the main supervisory authority for the Education Section.

<sup>2</sup> See Article 2 of the Foreign NGO Law.

<sup>3</sup> Article 53 of the Foreign NGO Law provides: "The exchange and cooperation between foreign schools, hospitals, natural science and engineering research institutions or academic organisations and domestic schools, hospitals, natural science and engineering research institutions or academic organisations shall follow and comply with the relevant regulations and rules of the state. If the foreign schools, hospitals, institutions or organisations referred to in the preceding paragraph violate the provisions of Article 5 herein when they conduct their activities in China, they shall be subject to legal liabilities in accordance with law."

Certain activities and projects listed under this section, such as “conducting joint research projects”, “promoting bi-directed overseas studies”, and “cooperation in carrying out academic exchanges” has given rise to concern and confusion, as, to our understanding, these activities should have already been carved out under the Carve-out Provision if these activities are between a foreign university, hospital or academic institute and its Chinese counterpart. We have sought advice from the relevant authorities in a number of different jurisdictions (both the MPS and the MOE) and received contradictory and inconsistent guidance in this regard. However, at least in different situations the answers given by officials from the national MPS are consistent, i.e. exchange and cooperation between two organisations of the same type—for example between a foreign school and a Chinese school, or a foreign hospital and Chinese hospital—are covered under the Carve-out Provision.

## Implementing rules

Although these two sets of implementing rules for the Foreign NGO Law are now available, their release was quite close to the Foreign NGO Law officially taking effect which leaves very little time for foreign NGOs to prepare and plan their RO registration applications or temporary activities, not to mention that there are still outstanding questions and issues. For example:

1. Does the *National Catalogue* apply to a Foreign NGOs’ temporary activities as well?

This is still unclear. One possible interpretation is that these catalogues only apply when foreign NGOs seek to set up ROs in China, but do not apply to their temporary activities. Some MPS officials at both national and provincial level hold this view.

2. What is a Foreign NGO’s status after 1<sup>st</sup> January, 2017, before its successful registration/filing with MPS?

On 8<sup>th</sup> November, 2016, a representative from the MPS’ Foreign NGO Management Bureau indicated at a briefing held in Shanghai that the MPS will not grant an official ‘transition’ or ‘grace period’ with respect to enforcement of the Foreign NGO Law. As of 1<sup>st</sup> January, 2016, they expected applicable Foreign NGOs to start submitting their application documents and complying with the law. However, as there will be lead times for the approval process before a foreign NGO completes the registration of its RO or record-filing for its temporary activities, many foreign NGOs have concerns over whether they are prohibited from engaging in any activities until after they have received such registration or record-filing. Many MPS officials we spoke to through anonymous telephone inquiries answered in the affirmative. As far as we know, many foreign NGOs have adopted a wait-and-see attitude and have suspended their

current operations in China until they obtain the registration or filing with the MPS or have better information on which to base a decision.

3. What is the intent of the prohibition on for-profit activities?

The Foreign NGO Law specifically prohibits foreign NGOs from engaging in or providing financial support to for-profit activities and political activities, and illegally conducting or sponsoring religious activities.<sup>4</sup> While the restrictions on political and religious activities have long been in effect, no guidance has been provided as to what types of activities will be deemed as either carrying out or sponsoring for-profit activities in China. For example, given the general inability to register a non-profit subsidiary in China in the past but the desire to be able to hire employees, rent space and conduct activities in China, many foreign NGOs have set up subsidiaries in China as for-profit legal entities (usually in the form of a wholly foreign-owned entity, (WFOE)), either as a direct subsidiary, or perhaps within a holding company for its overseas operations. Due to the prohibition on for-profit activities and the language of Article 9,<sup>5</sup> which applies restrictions on direct or indirect activity, it is not clear whether these existing WFOEs will be permitted to continue their operations in China under grandfather approval rules, and whether the WFOE is still an available option for a foreign NGO to enter into China with its overseas for-profit holding company. Based on anonymous phone inquiries with the MPS and its provincial arms, officials have advised that a foreign NGO will not be allowed to act as direct shareholder of a WFOE but its affiliate established offshore as a for-profit entity can still invest and set up a WFOE in China. **Eb**

**Hogan Lovells** is a global legal practice with over 2,800 lawyers in more than 40 offices including three offices in Greater China, five offices in the rest of Asia and 17 offices in Europe. The Beijing, Shanghai and Hong Kong offices provide a full range of services covering antitrust/completion law, intellectual property, media and technology, banking and finance, corporate and contracts, dispute resolution, government and regulatory, projects, engineering and construction, real estate, and restructuring and insolvency.

<sup>4</sup> Article 5 of the Foreign NGO Law provides: “Foreign NGOs that conduct activities within China shall comply with the law of China; shall not threaten China’s national unity and safety and the unity of all ethnic groups of China; shall not jeopardise China’s national interests, societal public interests or the legitimate rights and interests of the citizens, legal persons and other organizations. Foreign NGOs shall not engage in or provide financial support to for-profit activities or political activities within China. They are also forbidden to illegally conduct or sponsor religious activities.”

<sup>5</sup> Second paragraph of Article 9 of the Foreign NGO Law provides: “A Foreign NGO that has not established and registered a representative office or has not completed the record-filing for conducting temporary activities is not permitted to directly or indirectly conduct activities within China, and shall not directly or indirectly entrust and sponsor any unit or individual within China to conduct activities within China.”



# LEVELLING THE PLAYING FIELD FOR SMEs IN CHINA

## European Chamber's recommendations included in revised China SME Promotion Act

First coming into effect in 2003, the SME Promotion Act underwent a recent revision in late 2016. The Chamber's **InterChamber SME Working Group** took this opportunity to proactively feed into the revision process, providing recommendations taken from its position paper. This positive advocacy approach resulted in all four of the recommendations being included in the revised draft, which could go a long way to levelling the playing field for SMEs operating in China.



## Status quo, economic significance and policy developments

As in other major world economies, small and medium-sized enterprises (SMEs) now make up the overwhelming majority of businesses in the Chinese economy. According to data released by the National People's Congress (NPC) Fiscal and Economic Committee, by the end of 2015, the total number of businesses registered with the State Administration for Industry and Commerce (SAIC) reached 21.86 million, the majority of which were SMEs. Significantly, SMEs accounted for 99.6 per cent of businesses in the industrial sector.

Their contribution to economic growth, job creation and innovation has been increasingly recognised by Chinese policymakers. During a press conference at the Third Session of the 12<sup>th</sup> People's Political Consultative Conference National Committee in 2015, Mr Lv Xinhua highlighted their importance. He stated that SMEs contribute to over 65 per cent of GDP, 75 per cent of employment and 50 per cent of tax revenues. Over the 12<sup>th</sup> Five-Year Plan period, he said, registration of SMEs' intellectual property rights achieved 53 per cent growth year-to-year.<sup>1</sup>

In acknowledgment of the crucial role played by SMEs, policymakers are making greater efforts to identify the key challenges that they face, with the goal of creating a more favourable policy environment for them. In the *2015/2016 Blue Book on the Development of SMEs in China*, the Ministry of Industry and Information Technology (MIIT) discussed some of the most prominent obstacles hindering their development and also laid out some opportunities that can arise from recent, positive policy developments.

Obstacles to SME development	
Unfair competitive environment	Compared to large businesses: <ul style="list-style-type: none"> <li>• More restricted market access</li> <li>• Greater difficulties in key economic resources</li> </ul>
Lack of channels for talent acquisition	<ul style="list-style-type: none"> <li>• Mismatch between the skills supplied by China's education system and those demanded by SMEs</li> </ul>
Lack of affordable channels for financing	<ul style="list-style-type: none"> <li>• Limited access to direct financing (venture capital, debt and equity financing)</li> <li>• Cumbersome and expensive indirect financing</li> </ul>
Burdensome public finance system	<ul style="list-style-type: none"> <li>• Heavy tax and social security contributions</li> <li>• Opaque system of fees and administrative charges</li> </ul>
Weak capacity building	<ul style="list-style-type: none"> <li>• Low mobility out of traditional industries in decline</li> <li>• Dwindling profitability from the traditional business model of low quality, low technology and low price</li> </ul>

<sup>1</sup> Lv Xinhua: Work of Political Consultative Conference believed to bring relief to medium-sized, small and micro enterprises, Xinhua, 2<sup>nd</sup> March, 2016, viewed 22<sup>nd</sup> December, 2016, <[http://news.xinhuanet.com/politics/2015lh/2015-03/02/c\\_127534833.htm](http://news.xinhuanet.com/politics/2015lh/2015-03/02/c_127534833.htm)>

Positive policy developments and their implications	
Internet+	<ul style="list-style-type: none"> <li>• Facilitate the improvement of production efficiency</li> <li>• Contribute to the construction of a coherent credit evaluation system by leveraging Big Data</li> <li>• Promote affordable Internet financing</li> </ul>
Belt and Road Initiative	<ul style="list-style-type: none"> <li>• Act as a vehicle for SME internationalisation</li> <li>• Provide a wider range of financial products for SMEs in internationalisation</li> </ul>
China Manufacturing 2025	<ul style="list-style-type: none"> <li>• Promotes clustering</li> <li>• Promotes differentiation in terms of business models, products and technologies</li> </ul>

## Revision of the SME Promotion Act and Chamber Advocacy

The SME Promotion Act first came into effect in 2003, with the objective of ensuring a fair and healthy legal, policy and market environment for the development of Chinese SMEs. After more than a decade, its inadequacy to serve the stated objective has become increasingly obvious, reflected in particular by its failure to keep up with the new challenges facing SMEs and by its weak enforceability.

To address these problems, the NPC initiated the revision of the SME Promotion Act in October 2016, followed by a month-long public consultation starting mid-November.

Over the years, through dialogues with both Chinese and European SMEs and other stakeholders, the European Chamber identified a number of common difficulties and obstacles that affect Chinese and European SMEs alike. The Chamber was also aware that Chinese lawmakers and policymakers have long been looking to economies with more developed legal and policy frameworks for input on how to promote the development of SMEs. With this in mind, the Chamber reached out to the key SME policymaker—the MIIT SME Bureau—which also acts as a key advisory body for the NPC Legislative Affairs Committee (LAC) for the development of the SME Promotion Act.

The Inter-Chamber SME Working Group shared EU experience in protecting and helping SMEs. In September 2016, the latest *Position Paper* had been presented to both the director general of the MIIT SME Bureau and its research coordinator. The working group had also been enhancing its visibility among Chinese authorities by becoming actively involved in initiatives and activities organised by the MIIT SME Bureau.

In October 2016, the NPC LAC began revising the SME Promotion Act. The Inter-Chamber SME Working Group reacted by providing business recommendations via the call for comments and during official meetings with the MIIT SME Bureau and other relevant experts and officials. The working group's recommendations related to access to finance, burdensome administrative work, late payment issues and IPR protection were all incorporated. The following table


Key recommendations (KRs) from the Working Group Position Paper 2016/17	Chapters and articles in the first revised draft of the SME Promotion Act
<b>KR 1 - better access to financing</b>	<b>Chapter 3 – SME financing promotion</b>
<ul style="list-style-type: none"> <li>Implement key performance indicators (KPIs) to encourage banks to issue loans to SMEs.</li> </ul>	<ul style="list-style-type: none"> <li>Article 15 demands that banking regulators devise dedicated supervision policies for SME banking services and encourage bank financing for SMEs.</li> <li>Article 17 encourages banks to set up specialised entities to provide dedicated SME financial services.</li> </ul>
<ul style="list-style-type: none"> <li>Develop focused credit risk assessment procedures/systems suitable for the provision of SME loans.</li> </ul>	<ul style="list-style-type: none"> <li>Article 24 encourages credit rating agencies to develop SME-focused credit evaluation services and encourages the set-up of third-party independent SME credit rating agencies.</li> </ul>
<b>KR 2 – simplifying regulatory and administrative requirements for SMEs</b>	<b>Chapter 8 SME Rights Protection</b>
<ul style="list-style-type: none"> <li>Further develop official platforms to provide comprehensive and coherent information to SMEs.</li> </ul>	<ul style="list-style-type: none"> <li>Article 25 requires government bodies at and above the county level to provide free legal and policy consulting and public information services to SMEs regarding administrative, taxation, financing, hiring, production safety and social security.</li> </ul>
<ul style="list-style-type: none"> <li>Alleviate the administrative burdens for SMEs by reducing government approvals and simplifying the remaining approval and filing procedures.</li> </ul>	<ul style="list-style-type: none"> <li>Article 27 requires the State to optimise administrative approval procedures and facilitate the acquisition of licences and permits for small and micro businesses</li> <li>Article 30 requires the State to simplify the procedure for cancelling registration to facilitate the exit of small and micro businesses.</li> </ul>
<b>KR 3 – tackling late payments</b>	<b>Chapter 8 SME Rights Protection</b>
<ul style="list-style-type: none"> <li>Issue guidelines to ensure that government and state-associated institutions (incl. SOEs) respect contractual payment terms.</li> </ul>	<ul style="list-style-type: none"> <li>Article 53 prohibits the violation of contractual payment terms and payment deferrals by government bodies and large businesses and lays out the procedure for SMEs seeking rights protection.</li> </ul>

provides a comparison between the working group's recommendations and how they appear in the revised draft of the SME Promotion Act:

## Looking forward

The Inter-Chamber SME Working Group believes that the revision of the SME Promotion Act will have far-reaching implications on SME development and hopes that it will contribute towards positively strengthening SME competitiveness and their presence along the global value chain.

As the most fundamental law for protecting and helping SMEs, the act will serve to guide more concrete legislative and policymaking efforts of government bodies at all levels. It is likely that over the coming years we will see a wave of pertinent laws, regulations and policies coming out in the spirit of the SME Promotion Act.

Providing SMEs with a well-designed legal and policy framework that stands in when the market fails to allow the full potential of SMEs will be crucial for the sustainable growth of the Chinese economy. The Inter-Chamber SME Working Group remains committed to continuing to contribute to the improvement of the Chinese market and policy environment for European and Chinese SMEs alike. 

*The **Inter-Chamber SME Working Group** is the advocacy platform of the EU SME Centre, which focuses on helping European SMEs dealing with the challenges and difficulties related to the China market. The Inter-Chamber SME Working Group is a joint SME community from six European chambers of commerce: the China-Britain Business Council, the Benelux Chamber of Commerce in China, the China - Italy Chamber of Commerce, the French Chamber of Commerce in China, the European Union Chamber of Commerce in China and EUROCHAMBRES.*

*The European Union Chamber of Commerce is the leading chamber on policy advocacy. We carry out quarterly working group meetings, policy meetings and seminars, involving stakeholders from different chambers of commerce, the European Union Delegation to China and the 28 European Union member embassies in Beijing. From 2015 to 2016, the European Chamber has represented Inter-Chamber SME Working Group at the 6<sup>th</sup> and 7<sup>th</sup> EU-China SME Policy Dialogue, the EU-China Industrial Dialogue, the APEC Vietnam Workshop and the B20 Hangzhou Summit.*

*For information, please contact Deputy Head of Government Affairs Xavier Sans-Powell at [xsanspowell@european-chamber.com](mailto:xsanspowell@european-chamber.com).*



# SELLING YOUR WARES

## Entering the software business in China

European SMEs are traditionally strong in the development of new technologies and providing related services. Although China is a challenging market to enter in terms of regulation of technology and intellectual property rights (IPR) enforcement, it still holds a great deal of promise for companies bringing innovative solutions and technology. In this article the **EU SME Centre** looks at the software business in China, explaining common ways of operating such businesses and the regulations that should be heeded.



Software is a special product, the development of which does not usually require any special conditions such as natural resources or manufacturing facilities. It could therefore theoretically be developed either in China or abroad before being brought to the Chinese market. However, it should be noted that in China, software is subject to various regulations and more vulnerable to infringement of intellectual property.

Therefore it is of utmost importance to carefully consider your desired goals when drafting your business plan, as well as the risks associated with selling software to China. Your entry mode should then be based on this analysis.

## Direct investment into China

*Example: A medium-sized company active in the software industry in the EU (Company A) is interested in establishing a subsidiary in China and employing local staff.*

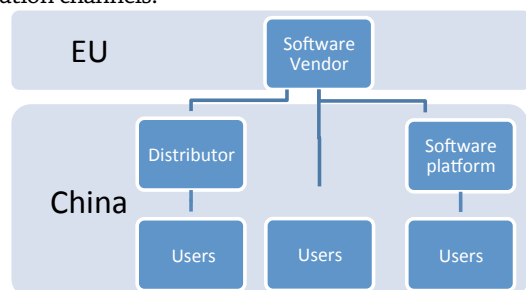
Manufacturing and development of software products falls under the 'encouraged' category in the latest version of the *Catalogue for the Guidance of Foreign Investment* issued in 2015. There are no substantial regulatory barriers preventing Company A from establishing a subsidiary engaged in manufacturing and development of software in China and the Chinese subsidiary in this industry may enjoy preferential treatment, e.g. less approval procedures and tax concessions.

Nevertheless, Company A will still have to conform to the other Chinese legislation governing the software business (e.g. the *Administrative Measures for Software Products*). Moreover, although the manufacturing and development of software products is generally encouraged by the Chinese Government, the distribution of certain software products is restricted or even prohibited under Chinese law (e.g. online games).

## Sale of software products to China

*Example: A small-sized software vendor (Company B) based in the EU identifies opportunities in the rapidly growing Chinese market, but finds setting up a local subsidiary in China too costly.*

Foreign companies may distribute their software products to Chinese users via various channels without direct investment into China. Below is an overview of the common distribution channels:



## Websites located abroad

The advantage of this option is that software products and their transactions will not be regulated by the Chinese Government, as the transaction occurs outside Chinese territory. The disadvantage is that the Chinese Government can easily block access to a certain foreign website using the Great Chinese Firewall.

It is advisable to create Chinese language web pages, and enable purchasers to use Chinese credit cards or Alipay (a popular online payment platform in China, similar to PayPal).

## Cooperation with Chinese software platforms

A foreign company may submit their software products to the Chinese market by entering into an Online Platform Service Agreement with a Chinese online software platform. The developer would be directly responsible for the content of the software. Before the software can be published on the platform, though, the online platform will review the software, to check whether it contains any illegal or improper information. For example, Tencent will review whether the software contains information such as pornography, gambling or defamatory content. It will also review the function of the software to be published, e.g., whether it will 'steal' customer information, or whether it contains improper advertisements.

Transactions occurring online in China are governed by relevant Chinese laws and regulations.<sup>1</sup> Software products are supervised by both online platforms and the relevant Chinese government authorities.

Online platforms may have the discretion to impose certain admittance standards for the software products. For instance, Baidu's software platform will require the submitter to provide proof that he/she is the copyright owner of the software being submitted. It should be noted that the agreement between the platform and the software owner are, in most cases, prepared by the platform. Software owners have limited bargaining power on the designing of these service agreements.

## Distribution via Chinese agents

It is common practice that software products are mostly traded by means of licensing. Trading of software products in China also follows this trend. The copyright owner of a software product makes profit by authorising others to use the software according to commercial conditions agreed by both parties. The following are some examples of licensing types:

- End users are licensed to use a copy of software products.
- A publisher/distributor is licensed to copy, distribute

<sup>1</sup> The *Decision of the Standing Committee of the National People's Congress on Internet Security Protection*; the *Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection*; and the *Administrative Measures for Internet Information Services*.






and publish software products.

- A software and/or hardware producer is licensed to pre-install a software product inside software/hardware.

A distribution licence agreement has to be arranged between foreign software vendors and local Chinese distributors, authorising the distributor to sell and distribute software products within a defined territory via certain distribution channels.

## Tax considerations

If the end user is going to download the software directly from the website of Company B, there will be no customs clearance involved and thus no duties nor 17 per cent import VAT will be levied. However, payment of royalties<sup>2</sup> to a foreign resident will be subject to withholding tax<sup>3</sup> and six per cent VAT.<sup>4</sup> 

*If you would like to learn more on how to sell software to China or have any questions on this subject, contact the EU SME Centre at <http://www.eusmecentre.org.cn/expert>.*

*tre at <http://www.eusmecentre.org.cn/expert>.*

*The **EU SME Centre** in Beijing provides a comprehensive range of hands-on support services to European small and medium-sized enterprises (SMEs), getting them ready to do business in China.*

*Our team of experts provides advice and support in four areas – business development, law, standards and conformity and human resources. Collaborating with external experts worldwide, the Centre converts valuable knowledge and experience into practical business tools and services easily accessible online. From first-line advice to in-depth technical solutions, we offer services through Knowledge Centre, Advice Centre, Training Centre, SME Advocacy Platform and Hot-Desks.*

*The Centre is funded by the European Union and implemented by a consortium of six partners - the China-Britain Business Council, the Benelux Chamber of Commerce, the China-Italy Chamber of Commerce, the French Chamber of Commerce in China, the EUROCHAMBRES, and the European Union Chamber of Commerce in China.*

*To learn more about the Centre, visit website [www.eusmecentre.org.cn](http://www.eusmecentre.org.cn)*



<sup>2</sup> There is a clear definition of 'royalties' under Chinese tax law, and the difference between the 'software usage fees' and 'royalties' has been widely discussed. The central tax administration has provided certain clarification: regarding the granting of use rights to software (not including any license of IPR), if such granting is subject to a set of restrictive terms (scope of use, means and term), the usage fees will be deemed as 'royalties' for tax purposes.

<sup>3</sup> The specific rate depends on the Double Tax Treaty between China and the country where Company B resides.

<sup>4</sup> China's VAT system uses multiple VAT rates rather than a single VAT rate for all goods and services: commonly used rates are 3%, 6%, 11%, 13% and 17%.

# EURObiz APP OUT NOW



**\*Available for  
iPhone and iPad**



**THE HOTTEST TOPICS FOR EUROPEAN  
BUSINESS IN CHINA ALWAYS AT YOUR  
FINGERTIPS**

[www.eurobiz.com.cn](http://www.eurobiz.com.cn)





# CHAMBER ANNUAL CONFERENCE 2016: IS GLOBALISATION IN RETREAT?

Held on 14<sup>th</sup> December, the Chamber's annual conference, *Globalisation in Retreat: Risks and Opportunities for China*, was an intriguing event. Speakers that included ambassadors, business leaders, economists and academics guided the 180 attendees through the complex causes and effects of recent political developments, and presented some possible outcomes. One thing became apparent over the course of the morning – it is too simplistic to reduce the tendencies that have emerged over the last couple of years to a single concept of 'anti-globalisation'.

As the conference panels were conducted under the Chatham House rule, the following summarises some of the key discussion points and does not represent complete views of any of the panellists who participated.



Ulrich Weigl, Head of Trade and Investment, EU Delegation to China

## Keynote speeches

In his opening speech, HE Hans-Dietmar Schweisgut, EU Ambassador to China, listed the key issues in 2016 that have mapped the future global outlook, including Brexit, Trump's election—both prevalent themes in all panel discussions—the G20, and, to a lesser extent, the Italian referendum.

“Populist-fuelled discontent has become a major factor in the political discourse,” said the ambassador, explaining that for the first time the growing backlash to globalisation was addressed at length during the 2016 G20 Summit. Expanding on the EU-China relationship, Ambassador Schweisgut called for reciprocity in trade and investment, as it would confirm China's commitment to fair and open trade and “would answer the concerns of those who fear that globalisation is a one-way street.”

Also delivering a keynote speech, Chamber President Jörg Wuttke conveyed a more personal narrative. Having grown up in post-war Germany, which surrendered parts of its sovereignty in the pursuit of globalisation, he lamented, “Sometimes, we should not take things for granted, like globalisation.”

On China's position, President Wuttke noted that while “China has been the biggest beneficiary of globalisation this century”, the future relies on openness and full implementation of the rule of law. “China should not make the mistake of relying on past EU openness,” he cautioned.

## Panel 1: Away from the Washington Consensus?

Contemporary China has many faces—or devils on its

shoulder, if you prefer—each of which, while taking China in a slightly different direction, come together to make up the complex nation it has become.<sup>1</sup> China as the ‘principled pluralist’ sees that Trump is threatening to reduce multilateral cooperation and is poised to fill the vacuum – as the US steps back, China will step forward. China as the ‘herald of the high frontier’ sees the US regressing to the pre-enlightenment era, while China itself clings to science – its stance on climate change is a good example of this.

While globalisation does show some signs of retreating, it has been responsible for bringing the world rapidly forward since World War II. China has not only made great contributions to the world since its accessions to the WTO, with its global GDP contribution expanding from 0.4 per cent to 20 per cent today, it has also benefitted a huge amount.

But while US-China relations were already heading for a reset—regardless of a Trump or Clinton presidency—China may well be surprised by the strength of reaction from the US business community – it is fully prepared to push back against China until reciprocity comes into play.

Alongside this, the US are abandoning the TPP, and look set to do the same with the TTIP, giving China an opportunity to upgrade its trade relationships with other regions and become a leader on trade agreements. This could be the time for China and the EU to cement their trade relationship before globalisation as we know it goes further south.

<sup>1</sup> These were identified as follows: 1) the ‘self-sufficient civilisation’ – generating our own values, we march to our own drum; 2) the ‘most humiliated nation’ – conquered and despised for a century, but no more; 3) the ‘sovereign survivor’ – leave us to survive as a communist power; 4) the ‘leader of the developing world’ – responsible, developing major power; 5) the ‘last man standing’ – the West is in decline, we have deep pockets; 6) the ‘principled pluralist’ – we will end the era of unilateral Western hegemony; and 7) the ‘herald of the high frontier’ – we share in, and protect, the global commons





Sharing a joke: European Chamber President Jörg Wuttke and HE Hans-Dietmar Schweisgut, EU Ambassador to China

Putting aside the Washington Consensus, there exists a 'Beijing Consensus', which can be basically characterised as China's commitment to globalisation. This form of globalisation, with Chinese characteristics, increasingly sees Chinese enterprises going out into the world – China manufacturing is even beginning to travel, and the FTAP, the AIIB and OBOR could potentially help to drive the world economy for the next 30 years.

This is where China's 'self-sufficient civilisation' rears its head – there is a clash between the 'global norm' and what China sees as a normative basis – China does not accept reciprocity on US terms, as there is a suspicion that the concept of 'reciprocity' has been predicated on US' interests. Working in tandem with this is China's 'most humiliated nation' which feels the need to now claw something back for itself.

It is highly significant that with OBOR a preference has emerged for China to invest in jurisdictions where there is strong rule of law – there is a natural inclination to make investments where a return can be guaranteed. This lesson is something that can inform China in terms of its own institutional reforms.

## Panel 2: The forces of anti-globalisation and the impact of economic nationalism on business

Essentially it is too early to know what will happen as a result of Brexit or of Trump's election, but these disruptive phenomena have both turned up the anti-globalisation vol-

ume.

For Trump's part, he will soon be exposed to a whole new world, and we will see how he deals with it. There has never been so much uncertainty over fundamental policy in Washington as there is right now. Therefore we need to look to those who Trump appoints as his top advisors if we are to glean an indication of where US policy is heading. Whatever happens, the US needs to recalibrate, come up with new ideas and decide which direction it is going to go in with China. There is also no absolute certainty that TPP is dead in the water – we could see Trump resuscitating it somewhere down the road and putting his own unique stamp on it.

In terms of finding solutions to the increasing prevalence of anti-globalisation sentiment and economic nationalism, it is important to put aside the elitist language being used at the political level and hold conversations with those who feel disenfranchised. Without addressing the root causes it will continue to grow. Political leaders need to acknowledge that what matters most to people is the immediate, the local and the personal.

If things are to get back on track, trust among different stakeholders will play an extremely important role. The process could be accelerated by a convergence of global interests, where multilateral cooperation is demanded. In the not-too-distant future this could happen in the area of climate change – if the current situation continues to deteriorate, it could become a major source of popular discontent.

So what is the future of bilateral trade and investment



HE Max Baucus, US Ambassador to China

agreements? While it is significant that China's State Development Research Centre has acknowledged that reciprocity is a fair principle, it does not exist at the moment. But perhaps the most interesting point is that China's ODI has outstripped FDI, and this has introduced new pressures. China investing in jurisdictions that enshrine rule of law should have a positive effect, as they can learn and grow from these experiences and take them back home, but there also a need for compromise on both sides – it should not necessarily be for China to make the first move.

Leading up to the next Party Congress there will be a huge focus on domestic stability, which will present an enormous challenge to President Xi. How they will deal with Trump is still completely unknown—even the other Republican candidates couldn't fathom him—but we could see the hand of the hardliners being strengthened – uncertainty tends to breed conservatism after all.

### Panel 3: Macro Outlook: The L-shaped 'new normal'

China's natural instinct to intervene and stabilise its economy resulted in a pull-back on reforms – the instability of 2015/2016 saw it move to deal with both equity and currency markets. Further capital controls can be expected, despite how bad this is for business. This is just a reality that will need to be faced in the medium term – China's measures to stabilise have come at the expense of the markets.

It is believed by some that the so-called 'new normal' and the 6.7 per cent growth figure are incompatible, and that growth is actually more in the region of three to four per

cent. But three to four per cent growth, it has to be said, it not bad, it is the sign of a maturing economy. This represents good and bad news – although the growth is slower than we have been led to believe, it is much more in line with what business has actually been experiencing, and as we are now closer to the floor, it won't hurt as much if we do fall.

Despite continued overall growth, though, China has 'recessionary pockets', like Liaoning Province, which need to be dealt with. Places such as these, where China's economy is heavily reliant on manufacturing by highly polluting enterprises, will suffer. In these areas the workforce needs to be re-educated and labour mobility needs to improve.

Going forward, there will continue to be a lot of push and pull between government and markets and it could be a case of one step forward, two steps back. This, on top of Trump and currency manipulation, could even signal a move away from globalisation on China's part, as policies could become a lot more inward looking.

In terms of how Brexit is being viewed by China business and leaders, and how they will engage with the UK and the EU going forward, there is a still a great deal of uncertainty – many Chinese companies are sitting and waiting to see how the situation develops. There could also be some further political repercussions in the EU, with a number of elections taking place in European countries next year, and this is adding to the overall sense of uncertainty. [Eb](#)

***We would like to thank our sponsors Huawei, Sanofi and Sennheiser.***

# EUROPEAN CHAMBER IN THE MEDIA

## Chamber comments on the newly released Cyber Security Law

### China passes controversial cybersecurity law

Ben Croxley  
AFP November 7, 2016



1 / 2

China's new cybersecurity law requires companies to verify a user's identity, effectively making it illegal to go online anonymously

The Cyber Security Law of China was passed on 7<sup>th</sup> November, 2016, by the National People's Congress (NPC). The European Chamber participated actively in both its first public consultation in July/August 2015 and second public consultation in August 2016. The Chamber's major concerns focused on data localisation requirements as well as the lack of clarity over 'critical information infrastructure'. The Chamber engaged with the Cyberspace Administration of China (CAC) and the NPC to voice industry concerns.

saying in a statement that the 'overall lack of transparency over the last year surrounding this significant and wide-reaching piece of legislation has created a great deal of uncertainty and negativity in the business environment'.

*"The European Chamber of Commerce disagreed,*

## President Wuttke urges a level playing field for foreign companies in China

THE EUROPEAN BUSINESS DAILY  
**Handelsblatt**  
GLOBAL

Companies & Markets Finance Politics Opinion

EXCLUSIVE STORIES [Light Budget Surplus in 2016](#) / [Former VW CEO to Appear Before German Parliament](#) / [World Economic Forum: Trump](#)

TRADE RELATIONS

### Turning China from Partner to Rival

German companies have long felt treated unfairly in China but refrained from speaking out. But now that Economics Minister Sigmar Gabriel is calling on Beijing to level the playing field on trade, they are speaking out in support.

Article options



Share This Article



When German Economy Minister Sigmar Gabriel visited China, his major task was to advocate for reciprocity between the two countries. President Wuttke's comments on the need for a level playing field were included in this article.

"One of them is Jörg Wuttke, president of the European Union Chamber of Commerce in Beijing. 'Does Germany truly want to let itself be nationalized through the back door?' he asked. 'Germany and Europe need to develop a mechanism to react to government takeovers.' He said Europeans should pay better attention to how the Americans, Canadians and Australians deal with these issues, noting that takeovers are sometimes blocked in those countries."

## Chamber speaks out about SAFE's window guidance on controlling capital outflow

**FINANCIAL TIMES**

US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

China Business [Add to myFT](#)

### Foreign companies in China hit by new exchange controls

Several European groups unable to make dividend payments abroad



Read next

China curbs use of foreign players in top tier football

Business



The *Financial Times* reported that some European companies in China have been unable to remit dividends abroad following the new exchange controls that were introduced on 28<sup>th</sup> November. The State Administration of Foreign Exchange (SAFE) instructed about 20 foreign and domestic banks on new 'window guidance' on foreign capital flows, which requires companies to obtain SAFE approval for capital outflows above USD 5 million.

*"Concerning this new measure, President Wuttke stated: 'The unpublished window guidance on the control of capital outflow is disruptive to EU companies' regular business operations. It also*

*unnecessarily exacerbates uncertainties regarding the predictability of China's investment environment."*



## The launch of the European Chamber's Shanghai Position Paper 2016/2017



*China Daily* highlighted the paper's recommendation related to improving Shanghai's quality of life, i.e. that improvements to the quality of life and easing visa restrictions will increase Shanghai's competitiveness. The article used Shanghai Chapter Chairman Mick Adams' quote from the official press release.

*"Head of the Shanghai chapter of the European Chamber, Michael Adams, said remaining attractive to international talent was critical to Shanghai's success. 'Ensuring that it does so, will require raising the quality of life in the city and*

*further opening the regime for the issuance of visas, working permits and hukou,' Adams said. The paper discusses how Shanghai can increase its standing as a global innovation centre, foster its manufacturing competitiveness, become more important for global finance, improve its quality of life and gather the best global talent in the city. 'In order for it to succeed in its ambitious goal to be a global centre, Shanghai will need the strong support and participation of foreign businesses, investment and talent,' Adams said."*

## Southwest China Chairman Robin Niethammer discusses business environment with Chengdu mayor



*"The European Chamber of Commerce in Chengdu, for example, reports of a meeting with the mayor of the city. Before the meeting the Chamber had sent a list of problems to the city administration. The paper, the so-called satisfaction report of the European companies in the region, raised concerns about the chronic air pollution, the still-questionable conditions found in Chengdu's hospitals and slow Internet. 'And then the mayor of Chengdu immediately came to us and said, let's talk, we want to address these problems,' said Robin Niethammer, Chairman of the European Chamber of Commerce in Southwest China. 'Then he invited*

*us to meet and actually worked through all the problems we had listed, and he has already submitted proposals for improvement."*

## Chamber News

The European Chamber is a people-based organisation whose operational success depends on the hard work and dedication of its staff. We employ great people, who make it possible for the Chamber to grow sustainably through the retention of our loyal members.

We are particularly proud to honour those staff who are celebrating milestones in service to the Chamber. In this issue we recognise and thank:



**Anna Rudawska**  
Deputy Manager  
5 years of service.



# EUROPEAN CHAMBER EVENTS GALLERY

## BEIJING CHAPTER



1



2

### Dialogue with MOFCOM (1)

On 23<sup>rd</sup> November, 2016, the Chamber held a dialogue with Zhu Bing, Director of Industry Division, Department of Foreign Investment Administration, MOFCOM, who explained the newly adopted *Interim Measures for Record-filing Administration of the Incorporation and Change of Foreign-invested Enterprises*.

### Maintaining Standards: Standardisation Reform in China's High Quality Consumer Product Market (2)

On 24<sup>th</sup> November, 2016, the Chamber hosted a seminar on the continued development of standardisation reform in China. We would like to thank our sponsors LEGO.

### European Chamber Annual Conference 2016: Globalisation in Retreat: Risk and Opportunities for China (3)

The Chamber's Annual Conference took place on 14<sup>th</sup> December, 2016. We would like to thank our sponsor Huawei, Sanofi and Sennheiser. Please see page 38 for a full review of the conference.



3

## NANJING CHAPTER



1

### First Nanjing Position Paper Presented in Zhenjiang (1)

On 6<sup>th</sup> January, Nanjing Board Chairman Bernhard Weber met with Xue Feng, Director General of the Zhenjiang Economic and Technological Development Zone, to present the first *Nanjing Position Paper 2017*.



2

### Chamber Meets Nanjing Vice Mayor (2)

On 12<sup>th</sup> January, the European Chamber Nanjing Chapter met Nanjing Government leaders including Mr Huang Lan, Vice Mayor of Nanjing.

## SHANGHAI CHAPTER



1

**Shanghai Position Paper 2016/2017 Launch (1)**

On 13<sup>th</sup> December, 2016, the European Chamber's Shanghai Chapter launched the second *Shanghai Position Paper*.



2

**Shanghai Annual Dinner: Becoming a Global Centre (2)**

On 13<sup>th</sup> December, 2016, the European Chamber Shanghai held the Shanghai Annual Dinner: Becoming a Global Centre, with over 200 members and guests attending. We would like to thank our sponsors: Danone, Merck, Sanofi, TEDA, D'Andrea & Partners and Pernod Ricard.



3

**3<sup>rd</sup> CSR CEO Talk: CSR Versus Profitability with United Technologies (3)**

On 12<sup>th</sup> December, 2016, the Shanghai Chapter hosted the 3<sup>rd</sup> CSR CEO Talk.



4

**Top 10 CSR Trends: Perspective, Insights and Case sharing (4)**

On 12<sup>th</sup> January 2017, the European Chamber co-organised an event with the German Chamber, focusing on the top CSR trends for 2017.

## TIANJIN CHAPTER



1

**European Chamber's 2<sup>nd</sup> Education Roundtable in Tianjin (1&2)**

The European Chamber Tianjin Chapter hosted an exclusive educational tour of the Tianjin Haihe Education Park and the Tianjin Sino-German University of Applied Sciences followed by a roundtable on 2<sup>nd</sup> December, 2016.



2





EURObiz CSR

3<sup>RD</sup> CORPORATE  
SOCIAL  
RESPONSIBILITY  
AWARDS

Acknowledge  
CSR successes,  
raise sustainability  
awareness and share  
CSR experience



# THE EUROPEAN CHAMBER'S 3<sup>RD</sup> CSR AWARDS

On 25<sup>th</sup> November, 2016, the European Chamber Nanjing Chapter hosted its 3<sup>rd</sup> CSR Awards, gathering prominent leaders and CSR practitioners from all over China. The awards acknowledged CSR successes, raised sustainability awareness and shared the experiences of organisations, all of which are looking to further embrace corporate responsibility in China.

*"One strategic approach for societal value creation is to carefully assess the steps and partners in the value chain and establish policies and initiatives that reduce the potential negative impacts of the corporation's activities in the environment and in communities. That is the basis of the sustainability policies of corporations. The long-term orientation that it requires can create significant value for corporations, in terms of reduced future costs and increased resilience of value chains, in addition to*

*the value it creates for stakeholders and the environment."*

—Filipe Santos

Visiting Professor of Social Entrepreneurship, INSEAD

The European Chamber's 3<sup>rd</sup> CSR Awards introduced new award categories to make the awards more inclusive, sustainable and distinctive. The multinational corporation (MNC) category, included three new sub-categories: Employee Development, Responsible Value Chain Development and Environmental Protection and Sustainability. An

award category for SME Responsible Innovation was also added.

In order to increase participation and spread awareness among young people, high school and university students were also invited to submit their essays on the case study: 'A minority village after an earthquake'. Students exercised their analytical and creative skills to develop both disaster relief and long-term reconstruction solutions.

- **Siemens** took home the award for Employee Development thanks to the Siemens Employee Volunteer Association. This employee-managed organisation focuses on improving access to education, providing greater access to science and technology and sustaining the community.
- **Nestle** took first in Responsible Value Chain Development due to its initiative in Yunnan's coffee industry. Having introduced coffee into Yunnan over 30 years ago, Nestle has provided substantial support for the industry through training and technical assistance, developing new opportunities for the region.
- **Michelin China** took the award in Sustainable Growth and Environmental protection with their substantial progress in decreasing their environmental footprint. Having cut CO<sub>2</sub> emissions by 49.3% and water use by 76.7% since 2013, Michelin continues to establish more and more ambitious goals in its efforts to further minimise its environmental footprint.
- **First Respond** took the award in Responsible Innovation for an SME. First Respond was established to help people in China develop the skills and the will to save others in life-threatening situations. Having already trained more than 90,000 citizens, First Respond looks forward to further expansion.

### Panel 1

Chaired by Nanjing Chapter board member Petra Grandison, the first panel focused on the topic *Evolving from CSR as a set of principles to creating shared value throughout the value chain*.

Jonathan Dong, from Nestle China, kicked things off with an introduction to the expansion of value throughout the dairy production chain. Ms Chia-Lin Coispeau, co-founder of Maverlinn Impact Innovation, followed up with a presentation on how aspirational brands can create shared value, with examples that demonstrated the progress of CSR in China. She also discussed the link between a company's reputation and its stock value. The next presentation was delivered by Thierry Yvon, National Risk Prevention Director of Carrefour China. Mr Yvon applied the value of CSR principles to methods of developing sustainable trust with consumers. Carrefour has dedicated itself to assuring food safety throughout its operations, he said. Finally, Dr Monique Taylor, Campus Dean and Executive Director of the New York Institute of Technology campus in Nanjing, discussed several strategies for developing CSR principles

among college students so that they can take them into their careers. The first panel concluded with a Q&A session.

### Panel 2

The second panel was chaired by Xavier Durand-Delacre, Senior VP of Arkema Asia-Pacific and President of Arkema China. He gave a presentation on integrating CSR and innovation into company strategies to maximise social, economic and environmental impact. Next, Ms Yixing Hao, EP Manager of Michelin China, discussed ways that companies can approach environmental sustainability. The third presentation was delivered by Michael Rosenthal, President of Miss Earth China, on the theme *How green is the green revolution?* He highlighted many of the discrepancies that can be found within the green movement, and encouraged a more comprehensive view on evaluating green actions. The next discussion was led by Rolf H. Koehler, a Board Member of AHK Shanghai. Mr Koehler raised the issue of inclusion in our economic system, and used discussion points from AHK's More than a Market Forum to highlight excluded populations. Finally Catherine Chauvinc, Group Vice President of Aden Services, discussed various ways that CSR can be used to reinforce corporate culture. 

*"The EUCCC CSR awards in China allowed voices of corporations, universities, social entrepreneurs and not-for-profit organisations, wholeheartedly invested in CSR, to be heard. As social entrepreneurs, we would like to warmly thank the highly dedicated EUCCC executives, discussion panelists, judges and all participating organisations and students. This uniquely diverse and powerful cross-fertilising dialogue fostered CSR, responsible innovation and impact leadership for shared value creation and economic progress to ensure a bright future for the generations to come, in a well-preserved environment. Now is indeed time for action."*

—Chia-Lin Coispeau, Founder  
Maverlinn Impact Innovation (Shanghai)

We would like to extend our thanks to our distinguished panel of nine judges, who gave their time to review all entries: Julia Broussard, Country Programme Manager, UN Women China Office; Julia Güsten, Managing Partner, Sharehouse (Nanjing) Co Ltd; Dr Markus Hermann, HR Director, BASF-YPC Company Ltd; Rolf H. Koehler, Principal, Koehler and Co Ltd, Hong Kong; Pascal Marmier, CEO, Swissnex China; Professor Filipe Santos, President, Portugal Social Innovation; Ms She Hongyu, Assistant to Secretary General, Amity Foundation; Mr Hui Zhang, Director of UTC Sustainability & Corporate Responsibility and Chair, CSR Forum, European Chamber; and James Zhou, Charter President, Rotary Club, Hangzhou.

We would also like to thank our sponsors:

**BASF-YCP, Nestle and Maverlinn.**



## EXECUTIVE COMMITTEE OF THE EUROPEAN CHAMBER



President  
Jörg Wuttke  
BASF



Vice President  
Bertrand de la Noue  
Total



Vice President  
Patrick Horgan



Vice President  
Sara Marchetta  
Chiomenti



Vice President  
Mick Adams  
Somerley



Vice President  
Alberto Vettoretti  
Dezan Shira &  
Associates



Treasurer  
Lars Eckerlein  
ABB



States'  
Representative  
Massimo  
Bagnasco  
Progetto CMR



States'  
Representative  
Bruno Weill  
BNP Paribas



States'  
Representative  
Mats Harborn,  
Scania



Secretary  
General  
Adam Dunnett

## NANJING BOARD



Chairman  
Bernhard Weber  
BSH Home  
Appliances  
Holding (China)  
Co Ltd



Petra Grandinson  
Atlas Copco



Markus Hermann  
BASF-YPC



Andreas Risch  
Fette (Nanjing)  
Compacting  
Machinery Co Ltd

## SHANGHAI BOARD



Chairman  
Mick Adams  
Somerley



Vice Chairman  
Carlo D'Andrea  
D'Andrea &  
Partners



Vice Chairman  
Marcus Wassmuth  
Landesbank Baden-  
Württemberg



Serafino  
Bartolozzi  
MAHLE  
Technologies



Eduardo Morcillo  
InterChina



Andreas Odrian  
Deutsche Bank



Clarissa Shen  
Sanofi China

## SHENYANG BOARD



Chairman  
Harald Kumpfert  
Smartheat



Stephane  
Gonnertand  
ODC Marine



Maximilian Hauk  
BMW



Sarah Miller  
Michelin



Guido Milner  
Sofitel Shenyang  
Lido

## SOUTH CHINA BOARD



Chairman  
Alberto Vettoretti  
Dezan Shira &  
Associates



Vice Chairman  
George Lau  
TÜV Rheinland



Scott D'Alterio  
QSI International  
School



Vivian Desmonts  
DS Avocats Law  
Firm (Guangzhou)



Danny Hong  
BASF  
Polyurethanes  
(China) Co Ltd



Ivan Shang  
Siemens Ltd,  
China



Klaus Zenkel  
Imedco  
Technology  
Shenzhen

## SOUTHWEST BOARD



Chairman  
Robin  
Niethammer  
Bayer Healthcare



Vice Chairman  
Paul Sives  
Proton  
Products



Shirley Ling  
Deloitte Advisory  
Chengdu



Kevin M. Marin  
Oakland Capital  
GmbH (Chongqing  
Representative)



Iker Vergel  
ADIsports



Aimee Zhang  
UniGroup  
Relocation,  
Chengdu

## TIANJIN BOARD



Chairman  
Christoph  
Schrempp  
Airbus



Gabriele Castaldi  
Flexbo



Kelvin Lee  
PwC Consultants  
(Shenzhen) Ltd,  
Tianjin Branch

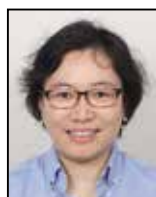


Michael Stengele  
Siemens

## EUROPEAN CHAMBER OFFICE TEAM



Beijing Office  
General Manager  
Maggie Xie



Nanjing Office  
General Manager  
Mei Zhang



Shanghai Office  
General Manager  
Ioana Kraft



Shenyang Office  
Office Manager  
Marine Chen



South China Office  
General Manager  
Francine  
Hadjisotiriou



Southwest China  
Office  
General Manager  
Sally Huang



Tianjin Office  
General Manager  
Kitty Wang



Secretary  
General  
Adam Dunnett

# CHAMBER NEWS

Every year both Chamber staff and management take a moment to recognise the outstanding work of their fellow colleagues. The Peer Awards are given to colleagues nominated by their peers, and selected by the Chamber's Management Committee. The Secretary General Award is based on nominations by the Chamber's Management Committee and chosen by the Secretary General. Winners of both awards receive a plaque and a gift from the Chamber.

## SECRETARY GENERAL AWARD



**Carl Hayward – Beijing Chapter**

Awarded for excellence and delivering a record breaking year in publications.



**Xavier Sans-Powell – Beijing Chapter**

Awarded for lobbying success with the InterChamber SME Working Group.



**Kinga Katus – Beijing Chapter**

Awarded for excelling on EU cooperation projects.

## PEER RECOGNITION AWARD



**Rui Gao – Beijing Chapter**

Awarded for her patient and thoughtful cross-chapter cooperation.



**Marine Chen – Shenyang Chapter**

Awarded for her determination and passion for the Chamber.



**Yefang Wang – Beijing Chapter**

Awarded for her work leading on Exclusive Dialogue events and her excellent communication skills.

# WILLEM BARENDSWAARD: A TRUE EUROPEAN

On 22<sup>nd</sup> November, 2016, we received the completely unexpected and devastating news of the untimely passing of Dr Willem Barendswaard (Wim), just two weeks after he had celebrated his birthday. Wim worked for SGS, and was a highly respected and influential board member of the European Chamber's Tianjin Chapter. He was held in the highest regard by his colleagues, fellow board members and European Chamber staff in Tianjin.

Wim constantly surprised us with his fresh ways of thinking, his ability to develop new ideas and to transform these ideas into action to drive the Tianjin Chapter forward.

He was fully dedicated to his work for the European Chamber and was worthy of being called a true European. He had been preparing himself to potentially step up as the next chairman of the Tianjin board, and now that he has sadly gone he will leave an enormous gap.



From L-R: Gabriele Castaldi (Tianjin Board), Kitty Wang (Tianjin GM), Michael Stengele (Tianjin Board), Willem Barendswaard (Tianjin Board), Kelvin Lee (Tianjin Board) and Adam Dunnett (Chamber Secretary General) at the Tianjin Gala Dinner, 2016

We will all miss his great kindness, his support and cooperation, and the way that he was able to go beyond any obstacles or resistance that faced him. His fantastic analytical abilities and his spirit have been of enormous value to the Chamber and we cannot overstate the contribution that he has made to our work.

Unfortunately, at the time of writing, we were unable to get in direct contact with his relatives and there was no chance for us in Tianjin to say a last, proper goodbye to Wim, so we can only pray for him. We are all very thankful that we had the opportunity to know this extraordinary person, who will always have a place in our hearts. We hope that his soul has found eternal peace at last.

Dr Christoph Schrempp

Chairman

European Chamber of Commerce in China, Tianjin

Jörg Wuttke

President

European Chamber of Commerce in China



# NEW DIMENSIONS OF CONFERENCING.



## TeamConnect Ceiling

Featuring a ceiling-mounted microphone installation with automatic beam-forming technology, the TeamConnect Ceiling conferencing system combines the advantages of wireless and wire-bound solutions, requiring minimal support, in any conference room.

[www.sennheiser.com/teamconnect-ceiling](http://www.sennheiser.com/teamconnect-ceiling)

**SENNHEISER**  
The Pursuit of Perfect Sound