International
Comparative
Legal Guides

Practical cross-border insights into cybersecurity

Cybersecurity 2023

Sixth Edition

Contributing Editor:
Edward R. McNicholas
Ropes & Gray LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

China


Susan Ning


Han Wu

King & Wood Mallesons

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Under the *Criminal Law of the People's Republic of China* (the "**Criminal Law**"), cybercrimes are mainly provided in the section: "Crimes of Disturbing Public Order". Articles 285, 286, and 287 are the three major Articles that directly relate to cybercrimes. Moreover, Article 253(1) indirectly relates to cybersecurity and applies to cases involving internet-related personal information infringement acts. The punishments for violating Articles 285, 286, and 287 include imprisonment, detention, and fines. For example, in serious cases, the offender may be sentenced to up to seven years' imprisonment for illegally obtaining data from a computer information system. Entities may be convicted for violating Articles 285, 286, and 287, as unit crime has been provided for in all three Articles.

It is worth noting that Articles 286 and 287 set up the principle that if a person uses computers (for example, through hacking, phishing or other internet-related illegal action) to commit other crimes, i.e. crimes that traditionally had no relationship with the internet, such as financial fraud, theft, embezzlement, misappropriation of public funds and theft of state secrets, the offender shall be convicted of the crime for which the penalty is heavier.

Pursuant to Article 285 of the *Criminal Law*, activities that involve invading a computer information system in the areas of State affairs, national defence or advanced science and technology constitute the "crime of invading a computer information system". The offender shall be sentenced to a fixed-term imprisonment of not more than three years or detention. For activities of invading a computer information system other than those in the above areas, it may constitute a "crime of obtaining data from a computer information system and controlling a computer information system" and the offender shall be sentenced to fixed-term imprisonment of not more than three years or detention, or imprisonment for three to seven years in serious cases. If an entity commits those crimes, such entities shall be fined, and the persons who are directly in charge and the other persons who are directly liable for the offences shall be punished accordingly.

Article 285 of the *Criminal Law* further provides that whoever, in violation of the state provisions, intrudes into a computer information system other than that prescribed in the preceding paragraph or uses other technical means to obtain the data stored, processed or transmitted in the said computer information system or exercise illegal control over the said computer information system shall, if the circumstances are serious, be sentenced to a fixed-term imprisonment of no more than three years or criminal detention, and/or be fined; or if the circumstances are extremely serious, shall be sentenced to a fixed-term imprisonment of no less than three years but not more than seven years, and be fined.

For example, in the criminal case of "*Zhang, Huang and others*' illegal obtainment of data in a computer information system and illegal control over a computer system", the defendant Zhang obtained the data by using hacker technology, and illegally obtained foreign citizens' credit card information, including the country, name, region, mailbox, phone number, credit card number, security code, validity period and other information from foreign shopping websites. Zhang then passed it on to Huang to sell online. According to the final decision of Jinhua Intermediate People's Court in Zhejiang Province in September 2020, the defendant Zhang was sentenced to five years' imprisonment and fined RMB 140,000 for illegally obtaining computer information system data. Defendant Huang was sentenced to four years and 11 months in prison and fined RMB 135,000 for illegally obtaining computer information system data.

It is noteworthy that the use of web crawlers may be regarded as invading conduct in violation of Article 285 if a technical method is adopted to crack anti-crawling measures set by websites or to bypass identity check processes set in a computer server. This is supported by various criminal cases in China. According to the ruling of the Yancheng Intermediate People's Court of Jiangsu Province on the *Cheng Mao* case, the defendant Cheng Mao hired programmers to register batches of accounts of an online shopping website by using proxy pools or broadband dialling and changing IP addresses constantly to avoid the website's anti-crawling strategies and bypass the verification mechanism used in the account registration process. Then, the defendant sold such accounts and obtained illegal gains of RMB 3,277,735. The court found that Cheng Mao was guilty of illegally obtaining data from a computer information system and sentenced them to four years in prison and a fine of RMB 500,000.

Pursuant to Article 29(1) of the *Public Security Administration Punishments Law of the People's Republic of China* (the "**Public Security Administration Punishments Law**"), if a person, in violation of national regulations, invades a computer information system that causes harm to such system, he/she will be detained for not more than five days, and will be detained for more than five days but less than 10 days if the circumstances are serious.

Article 27 of the *Cybersecurity Law of the People's Republic of China* (the "**Cybersecurity Law**") prohibits any person from endangering network security, such as illegally intruding into any other person's network, interfering with the normal functions

of any other person's network, and stealing network data. According to Article 63, any violation of the provision, if not regarded as committing a crime, will be subject to administrative penalties, including confiscation of illegal income, detention of no more than five days, and a fine between RMB 50,000 and RMB 500,000. If the circumstances are relatively serious, the violator shall be detained for not less than five days but not more than 15 days, and may be fined between RMB 100,000 and RMB 1 million. Where an entity carries out any of the above conduct, the public security authority shall confiscate its illegal income, impose a fine of between RMB 100,000 and RMB 1 million, and punish its directly responsible person in charge and other directly liable persons in accordance with the provisions of the preceding paragraph. Article 63 of the *Cybersecurity Law* further provides that the person given a public security punishment due to his/her violation of Article 27 shall not hold a key position of cybersecurity management and network operation for five years; and a person given any criminal punishment shall be prohibited for life from holding a key position of cybersecurity management and network operation.

Denial-of-service attacks

Pursuant to Article 286 of the *Criminal Law*, denial-of-service attacks could constitute the "crime of sabotaging [a] computer information system", and a sentence of more than five years' imprisonment may be given in particularly serious cases.

Denial-of-service attacks may also lead to administrative penalties. Pursuant to Article 29(2) of the *Public Security Administration Punishments Law*, if a person, in violation of national regulations, deletes, changes, increases or interferes with the functions of a computer information system, making it impossible for the system to operate normally, an administrative penalty of detention of less than five days, or in serious cases, detention of more than five days but less than 10 days, will be imposed.

In terms of the *Cybersecurity Law*, a denial-of-service attack will also be regarded as endangering network security and will also be subject to penalties under Article 63 of the *Cybersecurity Law*.

Phishing

Phishing is usually performed to steal or otherwise acquire the personal information of citizens, which is considered the "crime of infringing a citizen's personal information" provided in Article 253(1) of the *Criminal Law*; up to seven years' imprisonment may be sentenced in serious cases. In addition, those who engage in fraudulent activities by way of phishing may also commit the crime of "fraud". If the amount involved is relatively large, the offender will be sentenced to three years or fewer in prison or put under limited incarceration or surveillance, in addition to being fined. Those who defraud extraordinarily large amounts of money and property, or who are involved in especially serious cases, are to be sentenced to 10 years or more in prison or even be given life sentences, in addition to fines or confiscation of property.

According to the judgment made by the Nanping Intermediate People's Court of Fujian Province in April 2021, the defendants Xie and Lin sent phishing QR codes to the victims after adding their WeChat accounts. After the victims have scanned the QR codes, and filled in their personal bank account numbers, passwords and other information, the defendants checked the personal bank information of the victims and inquired about the balance in their accounts. Then, based on the search results, the defendants used different methods to defraud. Finally, Xie, Lin, and other plaintiffs were convicted of fraud. Xie was sentenced to eight years in prison and a fine of RMB 80,000, while Lin was sentenced to seven years in prison and a fine of RMB 70,000.

Furthermore, as most phishing is conducted by spreading a computer virus, the administrative penalty for this is for detention of less than five days or, in serious cases, detention of more than five days but less than 10 days, pursuant to Article 29 of the *Public Security Administration Punishments Law*. Article 63 of the *Cybersecurity Law* may also apply.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

For intentional creation or dissemination of a computer virus or other destructive programs, including, but not limited to, ransomware, spyware, worms, trojans and viruses, which affect the normal operation of a computer information system, if serious consequences are caused, such activities constitute the "crime of sabotaging a computer information system" under Article 286 of the *Criminal Law*. The offender may be sentenced to five years' imprisonment in extremely serious cases.

In addition, anyone who installs the above destructive programs in order to control others' computers may commit the crime of illegally controlling the computer information system under Paragraph 2 of Article 285 of the *Criminal Law*. If the circumstances are serious, he/she will be sentenced to imprisonment of not more than three years or limited incarceration, and/or be fined; or, if the circumstances are extremely serious, he/she shall be sentenced to imprisonment of not less than three years but not more than seven years, and be fined.

For instance, in the case of Ling illegally controlling the computer information system, the defendant, without permission of the owner of the internet bar, installed the destructive Trojan horse program on the internet bar server, and illegally controlled the computer information system. According to the final judgment made by the Dongguan Intermediate People's Court in April 2021, the defendant Ling was sentenced to three years in prison, and fined RMB 5,000 for the crime of illegal control of the computer information system.

In addition, intentionally making up or transmitting such destructive programs that adversely affect the normal operation of a computer information system is illegal, pursuant to Article 29 of the *Public Security Administration Punishments Law*. The violator may be subject to detention of less than five days or, in serious cases, detention of more than five days but less than 10 days. Article 63 of the *Cybersecurity Law* may also apply.

Moreover, Article 48 of the *Cybersecurity Law* provides that electronic information sent by and application software provided by any individual or organisation shall not be installed with malware, and the violator, according to Article 60 of the *Cybersecurity Law*, will be ordered to take corrective action and be given a warning by the competent authorities. If the violator refuses to take corrective action, or such consequences as endangering cybersecurity are caused, it shall be fined between RMB 50,000 and RMB 500,000, and the directly responsible person in charge shall be fined between RMB 10,000 and RMB 100,000.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

If a person provides hardware, software or other tools specially used for invading or illegally controlling computer information systems, or if the person knows that any other person is committing the criminal act of invading or illegally controlling a computer information system and still provides programs or tools for such a person, he/she shall commit the crime of "providing program[s] or tools for invading or illegally controlling computer information systems", pursuant to Article 285 of the *Criminal Law*.

In addition, if a person intentionally makes up or transmits destructive programs such as computer viruses that adversely affect the normal operation of a computer information system, and if not severe enough to constitute a crime, he/she will be penalised according to Article 29 of the *Public Security*

Administration Punishments Law. Furthermore, Articles 27 and 63 of the *Cybersecurity Law* also prohibit provision of programs or tools specifically used for conducting any activity endangering cybersecurity, or provision of technical support, advertising promotions, payments and settlement services or any other assistance to any person conducting any activity endangering cybersecurity.

Possession or use of hardware, software or other tools used to commit cybercrime
If a person possesses or uses hardware, software or other tools to commit cybercrime as prescribed under the *Criminal Law*, depending on the crime committed, the offender may be convicted in accordance with the corresponding Article under the *Criminal Law*, such as the "crime of invading a computer information system".

There is also an offence, i.e. "illegal use of information networks", that involves activities that take advantage of an information network to establish websites and communication groups for criminal activities, such as defrauding, teaching criminal methods, producing or selling prohibited items and controlled substances. If the criminal activity also constitutes another offence, the offender shall be convicted of the crime that imposes a heavier penalty.

Identity theft or identity fraud (e.g. in connection with access devices)
Under the *Criminal Law*, for identity theft, if the offender obtains identities by stealing or otherwise illegally acquires the personal information of citizens, such activity may be convicted as the "crime of infringing a citizen's personal information", pursuant to Article 253(1). If a person uses the stolen identity of others as his/her own proof of identity, such behaviour may constitute the "crime of identity theft" under Article 280(1) of the *Criminal Law*; in case such person uses the stolen identity to commit fraud or other criminal activities, he/she should be convicted of the crime the penalty of which is higher.

The *Cybersecurity Law* protects network information security, including the security of personal information. Stealing or illegally acquiring the personal information of citizens may also cause administrative penalties if the violation is not severe enough to constitute a crime.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
If a current or former employee breaches confidentiality obligations and causes infringement of personal information, trade secrets, or state secrets, etc., the offender will be convicted pursuant to Article 287 and punished in accordance with the relevant provisions of the *Criminal Law*, such as the "crime of infringing trade secrets".

In the final judgment made by the Huizhou Intermediate People's Court in September 2020, the defendant Wang left Huaxing Company and started working for Chongqing Huike Company. Huike Company wanted to inquire about the reasons for the abnormal product experiment. After Wang knew this, he shared the undisclosed production process and technology reports, which he obtained from Huixing Company in the WeChat group of the department of Huike Company, resulting in the use of such technical information by Huike Company. The court finally ruled that the defendant Wang constituted the crime of infringing trade secrets.

Furthermore, the infringement of trade secrets, under the *Anti-unfair Competition Law of the People's Republic of China* (the "**Anti-unfair Competition Law**"), will be subject to administrative penalties, including being ordered to cease the infringing conduct, the confiscation of illegal income, a fine ranging from RMB 100,000 to RMB 1 million, and a fine ranging from RMB 500,000 to RMB 5 million if the circumstances are serious.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
Unsolicited penetration testing could be seen as an illegal invasion of another person's computer information system, without having prior permission or consent.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
If a person, in violation of laws and regulations, deletes, amends, adds or disturbs the functions of a computer information system and causes the computer information system's inability to work normally, or conducts operations of deletion, amendment or addition towards the data or application programs that are stored, disposed of or transmitted in a computer information system, and serious consequences result, such activities constitute the "crime of sabotaging [a] computer information system" under Article 286 of the *Criminal Law*. The offender shall be sentenced to a fixed-term imprisonment of more than five years if extremely serious consequences result.

If a person, in violation of national regulations, deletes, changes, or increases the stored, processed, or transmitted data and the application program of a computer information system, the person shall be detained for less than five days, or in serious cases, detained for more than five days but less than 10 days, pursuant to Article 29 of the *Public Security Administration Punishments Law*. Furthermore, any conduct, in addition to what is described above, that endangers network security will be regulated under Articles 27 and 63 of the *Cybersecurity Law*.

1.2 Do any of the above-mentioned offences have extraterritorial application?

All of the above-mentioned crimes have extraterritorial application. First, if the criminal act or its consequences take place within the territory of China, the crime shall be deemed to have been committed within the territory of China. Second, the *Criminal Law* is applicable to citizens of China who commit crimes prescribed in the *Criminal Law* outside the territory of China; however, if the maximum penalty of such crime prescribed in the *Criminal Law* is a fixed-term imprisonment of not more than three years, the offender could be exempted from punishment. Third, if a foreigner commits a crime outside the territory of China against the State or against Chinese citizens, the offender may be convicted pursuant to the *Criminal Law* if the *Criminal Law* prescribes a minimum punishment of fixed-term imprisonment of not less than three years; however, the *Criminal Law* shall not apply if it is not punishable according to the law of the place where it was committed.

The *Public Security Administration Punishments Law* is applicable within the territory of China (except where specially provided for by other laws), or to acts against the administration of public security committed aboard ships or aircrafts of China (except where specially provided for by other laws).

The *Cybersecurity Law* generally applies to the construction, operation, maintenance and use of the network within the territory of China. Where any overseas institution, organisation or individual attacks, intrudes into, disturbs, destroys or otherwise damages the critical information infrastructure ("**CII**") of China, causing any serious consequence, the violator shall be

subject to legal liability; and the public security department of the State Council and relevant authorities may decide to freeze the property of or take any other necessary sanctions measure against the institution, organisation or individual.

The *Anti-unfair Competition Law* does not explicitly provide that it has extra-terrestrial application. In principle, any conduct that disrupts market competition or harms the legitimate rights and interests of business operators or consumers will be regulated under this law.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

For the above-mentioned offences, there are no specific mitigation conditions prescribed by law. However, the mitigation conditions prescribed in the *Criminal Law* for all crimes are applicable. For example, if an offender voluntarily gives oneself up to the police and confesses his/her crimes or exposes others' crimes that can be verified, the offender would be given a mitigated punishment.

The *Anti-unfair Competition Law* provides in Article 25 that where a business operator who engages in unfair competition takes the initiative to eliminate or mitigate the harmful consequences of the illegal act, the administrative punishment shall be reduced or mitigated; where the illegal act is trivial and promptly corrected and does not cause harmful consequences, no administrative punishment shall be imposed. The *Law of the People's Republic of China on Administrative Penalty* (the "**Administrative Penalty Law**") generally sets out circumstances where the administrative penalties could be mitigated, including taking the initiative to eliminate or mitigate the harmful consequences of the illegal act, being coerced by another person to commit the illegal act, and performing meritorious deeds in coordination with the authorities to conduct an investigation, etc.

2 Cybersecurity Laws

2.1 *Applicable Laws*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The *Cybersecurity Law*, which came into force on 1 June 2017, is the law covering various aspects of network security and has laid the foundation for a comprehensive cybersecurity regulatory regime in China. So far, a series of specific measures aimed at facilitating the implementation of the *Cybersecurity Law* have already been enacted, such as the *Measures for Cybersecurity Review*, the *National Emergency Response Plan for Cybersecurity Incidents*, and the *Provisions on Protection of Children's Personal Information Online*.

The *Cybersecurity Law* recognises the graded cybersecurity protection as the basic legal system to ensure network security in China. While the *Regulation on Graded Protection of Cybersecurity* is still seeking opinions, relevant authorities have officially been promulgating recommended national standards regarding graded cybersecurity protection since May 2019 for guiding the graded protection. These national standards include, but are not limited to: the *Information Security Technology-Baseline for Classified Protection of Cybersecurity* (GB/T 22239-2019), which replaces GB/T 22239-2008; the *Information Security Technology-Evaluation Requirement for Classified Protection of Cybersecurity* (GB/T 28448-2019), which replaces GB/T 28448-2012; the *Information Security Technology-Technical Requirement of Security Design for Classified Protection of Cybersecurity* (GB/T 25070-2019), which replaces GB/T 25070-2010; the *Implementation Guide for Classified Protection Of Cybersecurity* (GB/T 25058-2019), which replaces GB/T 25058-2010; and the *Classification Guide for Classified Protection Of Cybersecurity* (GB/T 22240-2020), which replaces GB/T 22240-2008.

Meanwhile, the regulations and guidelines on the protection of CII, data processing, and security assessment of outbound data transfers have been released, including the *Regulations on the Security Protection of Critical Information Infrastructure* (the "**CII Regulations**"), effective from September 2021, the *Measures for Cybersecurity Review* (the "**Review Measures**"), effective from February 2022, and the *Administrative Provisions on Security Loopholes of Network Products (Draft for Comments)*.

It is worth noting that in June 2021, China promulgated the *Data Security Law of the People's Republic of China* (the "**Data Security Law**"), which governs the collection, storage, processing, use, supply, transaction and disclosure of various types of data. The *Data Security Law* has established a data classification and grading system, and relevant authorities will formulate catalogues of "important data" within their jurisdictions, and implement enhanced security measures to protect such important data. It also stipulates that data activities that may affect national security will be subject to security reviews organised by relevant authorities. As a specific industry regulation under the *Data Security Law*, five government agencies, including but not limited to the Cyberspace Administration of China (the "**CAC**"), and the National Development and Reform Commission, issued the *Administrative Provisions on the Security of Automobile Data (for Trial Implementation)* on 16 August 2021, which: define the basic concepts related to automobile data processing; and clarify the legal obligations of automobile data processors as well as the processing standards for important data and sensitive personal information. Moreover, the local regulations, such as the *Regulations of Shenzhen Special Economic Zone on Data*, previously released by the Shenzhen Municipal People's Congress, also set out rules of data processing and sharing, opening, utilisation of public data.

Furthermore, China has strengthened the regulations of personal information collection. On 20 August 2021, the *Personal Information Protection Law of the People's Republic of China* (the "**Personal Information Protection Law**") was released, which contained comprehensive rules on various matters to which attention should be paid in personal information processing. Regarding the regulation on the processing of personal information by app operators, several regulative documents or guidelines, including the *Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps*, the *Methods for Determining the Illegal Collection and Use of Personal Information by Apps*, and the *Guide to Self-Assessment of the Collection and Use of Personal Information by Apps*, etc., have been issued.

As the basic law in the field of civil law, the *Civil Code of the People's Republic of China* (the "**Civil Code**") also helps to maintain a safe cyber-environment, especially provided from Article 1194 to Article 1197, the Law lays down rules for tortuous liability concerning conducts endanger safe cyber-environments. Specifically, these Articles regulate rights and obligations of users as well as network service providers, providing that network users are entitled to notify service providers and ask the latter to take necessary measures to protect the users' rights when their legal interests are infringed via the network.

Moreover, several other laws also provide safeguards in the event concerning cybersecurity. For instance, the *Cryptography Law of the People's Republic of China* (the "**Cryptography Law**") came into effect in January 2020 and provides regulations on the management and use of cryptography. The *Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services* aims to promote the positive and good applications of algorithms and

prevents service providers from using algorithm-recommended services to engage in activities prohibited by laws and administrative regulations.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The *Cybersecurity Law* includes provisions on the security protection of the CII. For instance, Article 37 of the *Cybersecurity Law* stipulates that personal information and important data collected or generated by CII operators ("**CIIOs**") during their operations within the territory of the PRC shall be stored within the PRC. Under Article 31 of the *Cybersecurity Law*, the state shall, based on the rules for graded protection of cybersecurity, focus on protecting the critical information infrastructure in important industries and fields, such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs, and the critical information infrastructure that will result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage.

In addition, the *CII Regulations* further sets out requirements on the security protection of the CII. For example, CIIOs shall set up special security management departments, prepare contingency plans, and conduct regular contingency drills, network security inspections and risk assessments, etc.

Also, Article 27 of the *Cryptography Law* provides that for CIIOs, laws, administrative regulations, and relevant national regulations require protection by commercial cryptography; thus, the CIIOs thereof shall use commercial cryptography for protection and conduct a security assessment of commercial cryptography applications.

It is noteworthy that the *Review Measures* issued in December 2021 and effective from February 2022 requires that CIIOs purchasing network products and services, either of which affects or may affect national security, shall carry out a cybersecurity review according to the Measures. Specifically, Article 5 of the *Review Measures* further requires that in the event that a CIIO purchases network products and services, it shall anticipate the potential national security risks that may arise from the use of such products and services, and report the ones that may affect national security to the Cybersecurity Review Office for cybersecurity review. Moreover, as indicated in Article 1 of the *Review Measures*, one of the purposes of the newly established version of the *Review Measures* is "to ensure the security of the CII supply chain". Moreover, Article 1 stresses the *CII Regulations* as one of the legal bases of the Review Measures' formulation.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. The *Cybersecurity Law*, the *Data Security Law*, the *Personal Information Protection Law*, the *Administrative Provisions on the Security of Automobile Data (for Trial Implementation)*, the *Regulations on the Security Protection of Computer Information System*, the *National Emergency Response Plan for Cybersecurity Incidents*, and other relevant laws and regulations have provided for network operators' legal duties when facing cybersecurity Incidents, which in general could be categorised into the following:

(1) **Regular Preventive Work**: network operators must adopt regular measures to prevent cybersecurity Incidents, including adopting technical measures to prevent cybersecurity violations such as computer viruses, cyberattacks and network intrusions, monitoring and recording the network operation status and cybersecurity events, and maintaining cyber-related logs for no less than six months. Furthermore, network operators shall provide early warnings of abnormalities such as data leakage, damage, loss and tampering, etc. Important data processors and sensitive personal data processors shall also carry out regular risk assessments.
Moreover, under Article 58 of the *Personal Information Protection Law*, personal information processors that provide important internet platform services involving a huge number of users and complicated business types shall perform the following obligations: (a) establishing and improving the system of personal information protection compliance rules in accordance with the provisions issued by the state, forming independent institutions mainly consisting of external personnel to supervise personal information protection; (b) following the principles of openness, fairness and impartiality, developing platform rules, and clarifying the norms for the processing of personal information by product or service providers on platforms and the obligations to protect personal information; (c) stopping providing services to product or service providers on platforms that process personal information in severe violation of laws and administrative regulations; and (d) issuing social responsibility reports on personal information protection on a regular basis to be subject to public supervision;

(2) **Emergency Measures for Security Incidents**: network operators must develop an emergency plan for cybersecurity Incidents in order to promptly respond to security risks, to take remedial actions immediately, to notify affected data subjects, and to report the case to the competent authorities as required. In addition, several local regulations, such as the *Regulations of Shenzhen Special Economic Zone on Data*, stipulate in detail that data security contingency plans should classify data security Incidents based on factors such as the degree of harm and the scope of impact, and provide corresponding contingency measures; and

(3) **After-action Review**: to keep communication with and assist the authorities in finishing their investigation and review after an Incident, such as providing a summary of the cause, nature, and influence of the security Incident and improvement measures.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes, they are.

(1) The reporting obligation shall be triggered by the occurrence of an Incident threatening network security.

(2) Pursuant to the *Cybersecurity Law*, the *Data Security Law*, the *Personal Information Protection Law*, the *E-Commerce Law*,

and relevant regulations, network operators, personal information processors, and other relevant entities shall at least timely notify the responsible authorities, such as the local government, industry regulators, public security authorities and local cyberspace administrations. Where a data security Incident occurs during data processing, measures shall be taken forthwith and reports shall be made to the relevant departments as required. In addition, pursuant to the *Regulations of the People's Republic of China on the Security Protection of Computer Information System*, any case arising from computer information systems shall be reported to the public security authority within 24 hours. Moreover, if there is a possibility of information leakage related to national security, the national security authorities shall also be informed. For instance, where a major cybersecurity threat occurs to a CII, the CIIO shall report the threat to the protection department, which shall notify the national cyberspace administration that a particular serious cybersecurity threat exists. Furthermore, the *Administrative Provisions on Security Loopholes of Network Products* provides that network product providers shall notify the Ministry of Industry and Information Technology ("**MIIT**") two days after discovering the security loopholes.

(3) At least the following content is required to be reported: information of the notification party; description of the network security Incident; detailed information about the Incident; nature of the Incident; affected properties (if any); personal information being affected/breached (if any); preliminary containment measures that have been taken; and preliminary assessment on the severity of the Incident. As for the security loopholes, certain content is required to be reported, including the names, models, and versions of the network products with security loopholes, as well as the technical features, harms, and scope of influence of such loopholes.

(4) Nevertheless, if the publication of Incident-related information will jeopardise national security or the public interest, such publication shall be prohibited.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Under the *Cybersecurity Law*, in case of disclosure, damage or loss, or possible disclosure, damage or loss, of user information, the network operator is obligated to take immediate remedies and notify the affected users promptly. In addition, for any risk, such as a security defect or bug that is found in a network product or service, the product/service provider concerned shall inform the users of the said risk.

Pursuant to the *Data Security Law*, in data-processing activities, one shall make contingency plans, take disposition measures immediately, notify users, and report to the appropriate department in a timely manner as required when a data security event occurs.

Moreover, under the *Personal Informational Protection Law*, where leakage, or tampering of personal information occurs and protection authorities anticipate that the aforementioned situations may cause damages, the personal information processor is required to notify the data subjects.

Currently, relevant laws and regulations do not provide specific requirements regarding the nature and scope of information to be reported; according to the *Information Security Techniques – Personal Information Security Specification*, recommended standards formulated by the National Standardization Committee, operators shall at least inform data subjects of the general description of the Incident and its impact, any remedial measures taken or to be taken, suggestions for individual data subjects to mitigate risks, and contact information of the person responsible for dealing with the Incident, etc.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Any regulators identified under question 2.4 above to which network operators are required to report an Incident shall have the authority to enforce the requirements identified under questions 2.3 to 2.5 above. Specifically, the enforcement authorities include the CAC, the MIIT, the Ministry of Public Security ("**MPS**"), the State Secrecy Bureau, the State Encryption Administration and industry regulators, etc.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Pursuant to the *Cybersecurity Law*, in case of non-compliance, network operators may be given a warning, ordered to take rectification measures, and/or imposed fines by the relevant authorities. In case of refusal to make rectifications or in severe circumstances, further penalties such as suspension of related business, winding up for rectification, shutdown of websites, and revocation of a business licence may be imposed by the competent authorities.

Furthermore, under the *Personal Information Protection Law*, where a personal information processor processes personal information in violation of this law or fails to fulfil the personal information protection obligations as provided in this Law, the department performing personal information protection functions shall also confiscate its or his/her illegal income. Moreover, where any violation of laws as prescribed in this Law is committed, it shall be entered into the relevant credit record and be published in accordance with the provisions of the relevant laws and administrative regulations.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

On 2 July 2021, the Cybersecurity Review Office under the CAC initiated a cybersecurity review of an online car-hailing app and certain other online apps in accordance with the *Review Measures* (draft for comment). To cooperate with the cybersecurity review and to prevent the expansion of risks, the app operators were ordered to suspend the registration of new users during the period of review. However, the cybersecurity review brought public attention and became controversial since the draft-for-comment version of the *Review Measures* only subjects CIIOs to be possible subjects for cybersecurity reviews. To be designated as a CIIO, an entity typically must be in important industries and fields, such as public communications and information services, energy, transport, water conservancy, finance, public services or e-government affairs. An online car-hailing app company is unlikely to fit the aforementioned definition of CII, in which case, the opponents may challenge the initiation of the cybersecurity review for an unsolid ground. Nevertheless, several months after the initiation of the cybersecurity review, the CAC

issued the current version of the Review Measures, under which "online platform operators" was added as one of the potential entities that may be subject to cybersecurity reviews.

Moreover, each year, the CAC, MIIT, and MPS, together with the National Work Group for "Combating Pornography and Illegal Publications", initiate a special campaign called "*Jingwang*" (clean the internet), aiming at investigating and preventing illegal activities in cyberspace or cybercrimes.

This year, the "*Jingwang*" action focuses on screening online live streaming, social contact, forums and communities, online comics and other fields, and achieved phased results. By the end of January 2022, regulatory authorities had disposed of more than 4.55 million pieces of harmful online information, banned and closed over 16,400 illegal websites, and investigated and handled more than 62,000 cases of cracking down on online pornography and illegal publications.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
The use of Beacons may result in the collection and use of users' personal information. Pursuant to the *Cybersecurity Law*, organisations shall notify users and obtain their consent before collecting information. Considering the difficulty of obtaining consent when collecting information through Beacons, they are generally regarded as not complying with the basic requirements under the *Cybersecurity Law*.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Relevant laws and regulations do not explicitly prohibit organisations from using Honeypots to detect and deflect Incidents in their own network.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Relevant laws and regulations do not explicitly prohibit organisations from using Sinkholes to detect and deflect Incidents in their own network.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber attacks?

Monitoring or intercepting electronic communications may trigger privacy issues, as they usually involve a collection of private or personal communication information. For instance, the *Civil Code* explicitly prohibits individuals or organisations from infringing upon a natural person's right to privacy. Specifically, Article 1033 of the *Civil Code* provides that unless otherwise prescribed by the law or specifically agreed by the right holders, no organisation or individuals are allowed to deal with the private information of others.

Furthermore, Article 65 of the *Telecommunications Regulations of the People's Republic of China* (the "**Telecommunications Regulations**") provides that except for the inspection of telecommunications contents by the public security authorities, the national security authorities, or the People's Procuratorates in accordance with the procedures stipulated by the law for the purposes of national security or a criminal investigation, no organisation or individual shall inspect telecommunications contents for any reason.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber attacks?

Pursuant to Article 28 of the *Cryptography Law*, the commerce department of the State Council and the State Cryptography Administration shall implement import licensing for commercial cryptography that involves State Security and public interest and that have encryption protection functions. They shall implement export controls on commercial cryptography that involves State security and public interest or that involves the international obligations of China.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Although industries or sectors such as telecoms, credit reporting, banking and finance, and insurance have some specific requirements with respect to the collection and protection of information, the prevention of information leakage, and the emergency response to Incidents, these requirements are, in general, in line with those under the *Cybersecurity Law*, the *Data Security Law*, and the *Personal Information Protection Law* without deviations.

However, since 15 February 2022, upon the effectiveness of the Review Measures, entities or individuals who are subject to the *Review Measures* (the "**Subject Parties**") are imposed with obligations of anticipating whether national security risks may arise from their purchases of products and services. Therefore, for enterprise entities carrying out different types of business, with the establishment of the *Review Measures*, we believe that a trend of Subject Parties evaluating their own products and businesses in advance based on the standard of "affect or may affect national security" (which also known as the gist of cybersecurity review) will be seen. Moreover, such preliminary evaluation shall be in combination with the regulatory focus of their industries. For instance, for Subject Parties in the banking and finance industry, besides obligations imposed by strict legal requirements under Applicable Laws, the Subject Parties shall also pay close attention to the localisation requirement under regulatory rules to avoid a personal information breach that affects national security, especially in the cross-border data transaction scenario. In addition, in the context of increasingly stringent cybersecurity reviews, corporate entities increasingly intend to complete self-assessment and rectification concerning the compliance of their business in advance, in order to avoid triggering cybersecurity reviews.

4.2 Excluding the requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Yes, there are. For example, the *Provisional Rules on Management of the Individual Credit Information Database* are promulgated by the People's Bank of China to ensure the secure and legitimate use of personal credit information: the *Measures of the People's Bank of China for the Protection of Financial Consumers' Rights and Interests* (updated by the People's Bank of China in September 2020) obliges financial institutions to ensure the security of personal financial information, and the *Anti-Money Laundering Law*; and the *Administrative Measures for the Identification of Clients and the Keeping of Clients' Identity Information and Transaction Records by Financial Institutions* requires financial institutions to take technical measures to prevent the loss, destruction or leakage of their client's identity information or transaction data. In addition, pursuant to the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users*, telecommunication business operators or internet information service providers shall record information such as the staff members who perform operations on the personal information of users, the time and place of such operations, and the matters involved, to prevent user information from being divulged, damaged, tampered with or lost.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Under the *Cybersecurity Law*, if a company, as a network operator, fails: to fulfil the obligation of security protection to ensure that the network is free from interference, disruption or unauthorised access, and to prevent network data from being disclosed, stolen or tampered with; fails to satisfy the mandatory requirements set forth in the applicable national standards; or fails to develop an emergency plan for cybersecurity Incidents, a warning shall be imposed on the company, and a fine will be imposed on both the company and the responsible person directly in charge if such company refuses to make rectifications or causes threats to cybersecurity.

Furthermore, under the *Data Security Law*, where an organisation conducting data processing activities fails to conduct regular risk assessments, strengthen risk monitoring or take remedial measures after any data security defect, vulnerability, or other risk is discovered, the competent authority may impose a fine on the directly liable executive in charge or other directly liable person.

Moreover, where a personal information processor commits any illegal act as specified in the preceding paragraph with serious circumstances, the authority performing personal information protection functions at or above the provincial level shall: order it or him/her to take corrective action; confiscate its or his/her illegal income; and impose a fine, and may also: order the suspension of relevant business or suspension of business for an overhaul; notify the relevant competent department to revoke the relevant business permit or business licence; and impose a fine on any directly liable person in charge or other directly liable person, and may decide to prohibit them from serving as directors, supervisors, senior executives or persons in charge of the personal information protection of related enterprises during a certain period of time.

In addition, as mentioned in question 1.1 above, pursuant to Article 286(1) of the *Criminal Law*, if a network service provider fails to perform its duties of security protection on the information network as required by laws and administrative regulations, and refuses to correct their conduct after the regulatory authorities order them to rectify the non-performance, the network operator shall be fined, and the persons directly in charge and the other persons directly liable for the offences may be sentenced.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under the *Cybersecurity Law*, all network operators are required to designate a person in charge of cybersecurity, such as a chief information security officer ("**CISO**"), to establish an emergency plan for cybersecurity Incidents, and to take technical measures to monitor and record network operation and cybersecurity events. In addition, pursuant to Article 38 of the *Cybersecurity Law*, CIIOs are required to conduct, by themselves or entrusting a service provider, an examination and assessment of their cybersecurity and the potential risks at least once a year, and submit the examination and assessment results, as well as improvement measures, to the competent authorities in charge of the security of the CII. That is to say, periodic cyber risk assessments and vulnerability assessments are mandatory for CIIOs. Furthermore, critical network equipment and special-purpose cybersecurity products provided by third-party vendors should satisfy the compulsory requirements set forth in the national standards and shall not be sold or supplied until such equipment or product successfully passes security certification or security tests by a qualified organisation.

Under the *Data Security Law*, a processor of important data shall specify the person(s) responsible for data security and the management body, and implement the responsibility of data security protection. Moreover, under Article 30 of the *Data Security Law*, the processor of important data shall carry out regular risk assessment on their data processing activities and submit a risk assessment report to the relevant competent authority.

The *Personal Information Protection Law* also requires that a personal information processor that processes the personal information reaching the threshold specified by the national cyberspace administration in terms of quantity shall appoint a person in charge of personal information protection to be responsible for overseeing personal information processing activities as well as the protection measures taken, among others. Article 51 requires that all personal information processors shall take necessary measures, including but not limited to: developing and organising the implementation of emergency plans for personal information security Incidents; and conducting classified management of personal information to ensure that personal information processing activities comply with the provisions of laws and administrative regulations, and prevent unauthorised access as well as the leakage, tampering or loss of personal information. The Article 55 further stipulates that a personal information processor shall conduct an impact assessment on personal information protection beforehand in the following circumstances: (i) processing sensitive personal information; (ii) making use of personal information to make automatic decision-making; (iii) entrusting others to process personal information, providing other personal information processors with personal information, and publicising personal

information; (iv) providing personal information to overseas parties; or (v) other personal information processing activities that have a significant impact on personal rights and interests.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Please refer to the answers to questions 2.4 and 2.5 above.

In addition, listed companies may have the duty to disclose cybersecurity risks or Incidents to the China Securities Regulatory Commission or disclose such information in their annual reports, depending on whether such information is deemed as significant and required to be disclosed.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

From the perspective of individuals, if an Incident results in unauthorised access to or disclosure of personal information collected and kept by the network operator, the individuals affected could bring a lawsuit against such network operator for breach of security protection obligations or for disclosing personal information by negligence on the basis of tort pursuant to the *Civil Code* and the *Personal Information Protection Law*. In two private lawsuits brought by consumers in July 2020, the court of first instance gave its verdict that the defendants in both cases had infringed consumers' rights and interests regarding personal information.

Further, as confirmed by the decision in the *Sina/Maimai* case ruled by the Beijing Intellectual Property Court, user data/information is an important operating resource and confers competitive advantages to network operators. If a network operator "steals" data from its competitor by accessing the data of such competitor without authorisation, the aggrieved party could sue the infringing party for unfair competition on the basis of the *Anti-unfair Competition Law*.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

On 9 August 2017, the plaintiff, Shen, ordered two airline tickets through an online booking app Ctrip App. Shen then received a text message that his flight was cancelled due to mechanical failure and he would be given a refund and compensation. Shen called the "customer service phone number", and the "customer service" accurately identified the name of the passenger, flight departure time and flight number. After Shen transferred RMB 99,976 to the "customer service", he finally realised that he had been deceived.

On 29 December 2018, the Chaoyang District People's Court of Beijing announced the following judgment: Ctrip had breached its security obligation as a network operator, resulting in security maintenance loopholes in the protection of the user's personal information. Therefore, Ctrip shall compensate Shen RMB 50,000 for his economic loss and make an apology to him at the same time.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Please refer to the answer to question 6.1 above.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations may take out insurance against Incidents, provided that such insurance categories are within the permitted scope of insurance regulations and have been approved by or filed with the China Insurance Regulatory Commission ("**CIRC**"). Currently, in China, there are already several insurance agents providing insurance related to Incidents such as data leakage, hacking, etc.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

So far, we are not aware of any regulation that sets out limitations specifically on insurance against Incidents. Normally, the coverage of loss will be decided through private negotiation between the insurer and the applicant, as long as such coverage does not violate mandatory regulations in China.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. anti-terrorism laws) that may be relied upon to investigate an Incident.

In accordance with the *Cybersecurity Law* and other relevant regulations, generally there are several enforcement agencies that are entitled to have investigatory power regarding an Incident, such as:

(1) the CAC, which is responsible for the overall planning and coordination of cybersecurity work and the relevant supervision and administration; and

(2) the authority in charge of telecommunication, the public security authority and other relevant authorities of the State Council, which will take charge of protecting, supervising and administrating cybersecurity pursuant to the present regulations in China.

The specific investigatory power of the above enforcement agencies can be found in a number of laws and regulations. For example, as stated in Article 54 of the *Cybersecurity Law*, the relevant departments of the government at provincial level and above are entitled to take the following measures in case of an increasing risk of an Incident:

(1) require authorities, organs and personnel concerned to promptly collect and report necessary information;

(2) organise authorities, organs and professionals concerned to analyse and evaluate cybersecurity risks; and

(3) give warnings to the public about the cybersecurity risks and release prevention and mitigation measures.

Pursuant to Article 19 of the *Anti-Terrorism Law of the People's Republic of China* (the "**Anti-Terrorism Law**"), where a risk of terrorism may arise in an Incident, the CAC, competent

telecommunications department, public security department, as well as the national security department shall carry out the following actions in accordance with their respective duties:

(1) order the relevant entities to stop transmission and delete the information involving terrorism and extremism; and
(2) shut down the relevant sites and cease the related services.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

First, the *Cybersecurity Law* has made it clear that network operators shall provide technical support for the public security department and the national security department specifically on two matters: (1) safeguarding national security; and (2) investigation of crimes. Second, the *Anti-Terrorism Law* explicitly states that telecommunications operators and internet information service providers shall facilitate the relevant departments in terrorism cases, such as providing technical interfaces and decryption services. Moreover, for entities and individuals that engage in international network connections, public security departments may also ask them to provide information, materials and digital files on security protection matters when investigating crimes committed through computer networks connected with international networks. In several business sectors, such as the financial sector, there are also applicable laws or regulations requiring entities to coordinate with relevant industrial regulators in their investigatory activities. For example, the *Anti-Money Laundering Law* requires financial institutions to promptly report transactions of large amounts and suspicious transactions to the Anti-money Laundering Information Center. Additionally, several regulations lay down rules governing the entities and individuals involved in the provision of internet information services. For instance, Article 28 of the *Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services* provides that an algorithm-recommended service provider shall keep web logs in accordance with the law, cooperate with cyberspace, telecommunications, public security, market regulatory, and other relevant authorities in conducting security assessment and supervisory inspection, and provide necessary technical, data, and other support and assistance. Article 21 of the *Provisions on the Administration of Internet Users' Account Information* (the "**Provision on Users' Account**") requires that cyberspace administrations shall, according to the law, supervise and inspect the administration by internet information service providers of internet users' registration and use of account information. Internet information service providers shall cooperate on it and provide necessary technical and data support and assistance. It further provides that if it is found that an internet information service provider is exposed to a high risk of network information security, the cyberspace administrations at or above the provincial level may require it to take measures such as suspending information updates, user account registration, or other related services. An internet information service provider shall take measures as required to take corrective action to eliminate hidden dangers. The protection of users' account information is also one of the safeguards implemented in accordance with Article 24 of the *Cybersecurity Law*, which requires the users to provide true identity information as they assign for service agreements or register service accounts.

Susan Ning is a senior partner and the head of the Commercial and Regulatory Group. She is one of the pioneers engaged in the cybersecurity and data compliance practice, with publications in a number of journals such as the *Journal of Cyber Affairs*. Her articles include "New Trends of the US Personal Data Protection – Key Points of the New FCC Rules", "Big Data: Success Comes Down to Solid Compliance", "Does Your Data Need a "VISA" to Travel Abroad?", and "A Brief Analysis on the Impact of Data on Competition in the Big Data Era", among others. Susan is recognised as a "Tier 1 Lawyer" for Cybersecurity and Data Compliance in 2019 *LEGALBAND* China.
Susan's practice areas cover self-assessment of network security, responding to network security checks initiated by authorities, data compliance training, due diligence of data transactions or exchanges, compliance of cross-border data transmissions, etc. Susan has assisted companies in sectors such as IT, transportation, online payments, consumer goods, finance, and the Internet of Vehicles in dealing with network security and data compliance issues.

King & Wood Mallesons
18th Floor, East Tower, World Financial Center
No.1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
China

Tel: +86 10 5878 5010
Email: susan.ning@cn.kwm.com
URL: www.kwm.com

Han Wu practises in the areas of cybersecurity, data compliance and antitrust. He excels in providing cybersecurity and data compliance advice to multinational companies' branches in China from the perspective of data compliance in China. Han also has expertise in establishing network security and data compliance systems for Chinese enterprises going abroad in line with the requirements of the European Union (GDPR), the United States and other jurisdictions. Han was elected as one of "40-under-40 Data Lawyers" by *Global Data Review* in 2018. Han was also recognised as a "Next Generation Partner" by *The Legal 500* in 2021 and named one of the 2021 *ALB China* Top 15 TMT Lawyers.
In the areas of cybersecurity and data compliance, Han provides legal services including: assisting clients to establish a cybersecurity compliance system; assisting clients in self-investigation on cybersecurity and data protection; assisting clients to conduct internal training on cybersecurity and data compliance; assisting clients in due diligence in data transactions; assisting clients to design plans for cross-border data transfers; and assisting clients in network security investigations and cybersecurity Incidents, among others.

King & Wood Mallesons
18th Floor, East Tower, World Financial Center
No.1 Dongsanhuan Zhonglu, Chaoyang District
Beijing 100020
China

Tel: +86 10 5878 5749
Email: wuhan@cn.kwm.com
URL: www.kwm.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group