Photo byMichael Traitov on Shutterstock

LEXOLOGY
Getting The Deal Through

Market Intelligence

PRIVACY & CYBERSECURITY 2023

Global interview panel led by WilmerHale

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by WilmerHale, this *Privacy & Cybersecurity* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Post-covid trends
Cloud hosting
M&A risks
Selecting counsel

START READING

© Law Business Research 2023

Photo by Weiming Xie on Shutterstock

China

Jingyuan Shi is the key contact for the Shenzhen office of Simmons & Simmons, and a partner leading the TMT practice in the Greater China region. She is a PRC-qualified lawyer and a practising solicitor in England and Wales.

Jingyuan specialises in data and technology laws. She has supported a large number of telecoms, media and technology (TMT) companies, strategic and financial investors in the TMT industry, asset managers, financial institutions, fintech companies and life science companies on an impressive selection of mandates, including without limitation data compliance, PE/VC and M&A transactions, regulatory and intellectual property.

Jingyuan is regularly invited to speak at industrial events. She is also a regular contributor to the Simmons & Simmons website and WeChat account, and for the China chapters of Lexology Getting The Deal Through: *Fintech* (2017–2023), *Telecoms & Media* (2017–2021), and *Market Intelligence*: *Privacy and Cybersecurity* (2021–2022).

Yuchen Lai is a legal executive in our Shenzhen office and a PRC qualified lawyer. She works extensively for international and Chinese telecoms, media and technology (TMT) companies, strategic and financial investors, financial institutions, asset managers, FinTech companies as well as life science companies. She advises on a wide range of compliance issues such as data and wider regulatory compliance, as well as corporate transactions. Yuchen has a strong focus on China data advice and has in-depth knowledge and rich experience in Chinese and global data compliance projects.

© Law Business Research 2023

QUESTIONS

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

Over the past year, we have seen material regulatory updates in relation to cybersecurity matters in China, which, for the purpose of this chapter only, refers to mainland China, without taking into account the laws and practice in Hong Kong SAR, Macau SAR and the Taiwan region. The one with the widest influence is the implementation of two regulations in relation to cross-border data transfer (CBDT).

Restrictions on CBDT was introduced by China's Cybersecurity Law that took effect on 1 June 2017, which is the first legislation in China to comprehensively regulate the country's cyber networks. It applies to the construction, operation, maintenance and use of networks, as well as to cybersecurity supervision and management within the territory of China. Under the Cybersecurity Law, if an operator of 'critical information infrastructure' (CII) wishes to transfer personal information or 'important data' out of China, it must first clear the 'security assessment' (Security Assessment) organised by the Cyberspace Administration of China (CAC).

When the Personal Information Protection Law (PIPL), China's first comprehensive law on personal data protection, took effect on 1 November 2021, the Security Assessment requirement was extended to personal information processors (ie, equivalent to 'data controllers' under the General Data Protection regulation (GDPR)) that trigger certain data volume thresholds as determined by the CAC, though the PIPL itself does not clarify such thresholds.

However, the Security Assessment mechanism had not been officially implemented until 1 September 2022, when the Regulation on Security Assessment for Data Export (Security Assessment Regulation) was finally enacted, which clarifies that the following situations will be subject to the Security Assessment requirement: (1) any data exporter to transfer 'important data' out of China; (2) any CII operator to transfer personal information out of China; (3) any personal information processor that processes the personal information of more than 1 million individuals to transfer personal information out of China; (4) any personal information processor that has transferred the personal information of 100,000 individuals or the sensitive personal information of 10,000 individuals out of China since 1 January of the previous year to transfer personal information out of China.

The Security Assessment is, in essence, a process of administrative approval. The substantial documents required for the process include an application form, a self-assessment report on data export risks and the legal document to be entered into by the data exporter and the overseas recipient. The data exporter needs to disclose to the CAC

© Law Business Research 2023

detailed information about its business operations, data assets and processing activities, information systems and data centres involved in the intended CBDT, internal data security and privacy policies and procedures, as well as details of the overseas recipient. Further, the self-assessment report must also evaluate the data protection laws and practices in the destination jurisdiction, which is similar to the post-Schrems II 'transfer risk assessment' in the GDPR context.

Our observation is that in practice, the CAC applies very high standard when reviewing the application documents. According to official statements from provincial-level cyberspace administrations (PCAs), market players that have passed the Security Assessment by the end of May 2023 include Beijing Friendship Hospital, China Airline, Mazda, Sephora, HIK Vision and EZVIZ, etc.

The other important legislative update on CBDT is the Regulation on the Standard Contract for Personal Information Outbound Transfer (Standard Contract Regulation) as well as the annexed Standard Contract (China SCCs), which took effect as from 1 June 2023. Market players not subject to the Security Assessment obligation may use the China SCCs to transfer personal information out of China. The China SCCs share a fair amount of similarities with the EU's Standard Contractual Clauses for international data transfer (EU SCCs), whereas maintaining significant unique features, which international entities should note when implementing them and coordinating multi-jurisdictional data compliance.

For example, both the China SCCs and the EU SCCs are invariable fixed-form template contracts, the data exporter and the overseas recipient may only agree on limited additional clauses, which are not in conflict with the SCCs. Another example of the similarities is that both the EU SCCs and China SCCs are accompanied with the requirement of conducting impact or risk assessments on the proposed data transfers, which may be a challenging task to complete in practice.

Photo by Lili.Q on Shutterstock

As for the key divergences, the China SCCs in general do not differentiate different 'modules', except that a few clauses have set out different obligations for the overseas recipient, depending on whether it is a personal information processor or an entrusted party (ie equivalent to 'processor' under the GDPR). The Standard Contract Regulation also requires that the executed China SCCs along with the personal information protection impact assessment report shall be filed with the relevant PCA within 10 working days of the effective date of the executed China SCCs.

Another notable regulatory trend is that sectoral regulators in China are actively formulating or amending sector-specific rules in accordance with the principles under the Cybersecurity Law, the PIPL and the Data Security Law (effective as from 1 September 2021). To name a few, the new regulations issued over the past year include, among others, the Administrative Measures on the Cybersecurity of Medical Institutions, the Administrative Measures on the Cybersecurity of the Electricity Industry, the Administrative Measures on the Cyber and Information Security of the Securities and Futures

QUESTIONS

© Law Business Research 2023

QUESTIONS

"In addition to mandatory regulations, over 20 recommendatory national standards in relation to cybersecurity were also published over the past year ."

Industry, and the Interim the Administrative Measures on Data Security in the Areas of Industry and Information Technology.

In addition to mandatory regulations, over 20 recommendatory national standards in relation to cybersecurity were also published over the past year. Though they are not legally binding, such standards may provide practical guidance for cybersecurity, data security and privacy practices relating to some specific sectors and application scenarios, including facial recognition, security protection of CII, instant messaging, e-commerce, online payment, cloud computing, edge computing, blockchain, notification and consent for personal information processing, etc.

Looking at the enforcement side, key regulators including the CAC, the Ministry of Public Security (MPS), the Ministry of Industry and Information Technology (MIIT), and the State Administration of Market Regulation (SAMR) continue to carry out regular enforcement against cybersecurity and privacy misconducts.

In July 2022, China's ride-hailing conglomerate Didi Global Inc (Didi) was fined 8.026 billion yuan by the CAC for violations of cybersecurity and data related laws. The cybersecurity review on Didi was initiated in July 2021. According to the official statement by the CAC, Didi's illegal conducts starting from June 2015 have 'imposed significant risks to the country's cybersecurity and data security', and 'seriously infringed the privacy and personal information rights of users'. The CAC also commented that Didi's violations involve an enormous amount of data (over 64.7 billion pieces), multiple types of sensitive personal information and various applications and processing activities, and the fine was based on the nature, duration and damage of Didi's illegal activities.

In March 2023, China's Cybersecurity Review Office (CRO) initiated an investigation on US semiconductor manufacturer Micron. The CRO stated in May 2023 that Micron did not pass the cybersecurity

© Law Business Research 2023

review because it has 'severe cybersecurity problems' that could pose significant security risks to China's CII supply chain.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The Cybersecurity Law requires network operators to notify competent regulators of cybersecurity incidents including personal information breaches, but it does not go on to provide details about the key factors to be assessed. A set of lower-level regulations and standards provide guidelines in this regard (including a new standard to take effect on 1 December 2023, of which the full text has not be published as of the date of this note). The reportable incidents usually include cyberattacks, hacking, malware, virus and human or equipment failure that may cause significant damage to the society and general public. Subject to the affected areas and degree of damage, there are different categories of reportable breaches. The key factors or impact of an incident that an organisation must assess include: (1) internet access in geographic areas (eg, single or multiple provinces, or even the entire country); (2) operation of major websites or platforms (eg, e-commerce websites with millions of active users); (3) number of users affected (a minimum of 100,000 users should ring alarm bells); (4) loss, theft or falsification of state secrets, important or core data that may cause significant damages; and (v) a catch-all scenario applicable to other factors, judged by the discretion of the organisation suffering the breach incident.

Upon initial assessment, if an organisation believes any of the above factors is met, it should immediately report such breaches to regulators. If a breach incident is likely to cause severe harm to the lawful rights and interests of individuals (eg, where sensitive personal information is leaked), the organisation shall inform the affected individuals of such breach incident.

Photo by Eric007 on Shutterstock

The PIPL requires the personal information processors (note the definition of personal information processor under Chinese law is essentially equivalent to the concept of a 'data controller' under the GDPR) to notify the competent regulator and relevant individuals once a personal data breach is detected. If the processor can take measures to effectively avoid the damage caused by data breaches, then it may decide not to notify the affected individuals. However, if the data protection regulators find the breaches may cause damage to individuals, they can request the processor to notify the affected individuals regardless. There is so far no general hard time requirement on when such report must be done under the PIPL, but we recommend data processors to report as soon as possible if initial assessments point to a report.

In addition, note that there are likely sectorial rules with more specific timing requests on this issue. For example, for financial

© Law Business Research 2023

institutions, according to the Implementation Measures for Protecting Financial Consumers' Rights and Interests, which took effect on 1 November 2020, reports to consumers and the regulators must be made within 72 hours. The Measure for Supervising the Risks of Information Technology Outsourcing Activities by Banking and Insurance Institutions, which took effect on 30 December 2021, provides that banks shall report to China Banking and Insurance Regulatory Commission or its local counterparts within 24 hours of any client personal information breach or data damage/loss during the IT outsourcing activities. The Measures on Reporting, Investigation and Handling of Cybersecurity Incidents for Securities and Futures Sector, which took effect on 4 June 2021, provide that securities and futures institutions must report cybersecurity incidents immediately, and in the event of a severe incident the report shall be updated every 30 minutes. So, in addition to general reporting obligations, an organisation shall closely monitor and follow industry-specific regulations in order to comply with reporting obligations.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

When hit with a data security incident, companies must be able to multitask on many pressing issues at the same time. The biggest issues include, but are not limited to, assessment of severity and scope of damage; determination of whether to report the incident to regulators and affected individuals; technical rectification measures to control the incident to minimise damage; complete and swift internal review and investigation of the breach; coordination with outside legal, forensic, technical or public relations counsel to prepare for subsequent actions; cooperation with directives from regulators and the police (if necessary); responses to customer inquiries or complaints; and responses to media reports or coverage.

"An organisation shall closely monitor and follow industry-specific regulations in order to comply with reporting obligations."

Any of these issues, if not handled properly, may easily morph into a situation that is out of control, especially in today's social media age. Such an incident is the true test of a company's response strategies, internal policies, management structure, designated staff as well as technical capabilities. The ultimate goal is to manage potential liabilities on all fronts, manage potential reputational damages, resume normal operation and prevent recurrence of similar incidents.

That said, out of these pressing issues, from a privacy protection perspective companies must concentrate resources to assess damages that may be caused to the privacy of affected individuals and take effective measures as a first priority to contain and control such damage while completing all legally required reporting and other obligations.

© Law Business Research 2023

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Following in the footsteps of the GDPR, China has made tremendous legislative efforts in data and cybersecurity related laws and regulations. Some high-profile pieces of legislation and investigation cases have conveyed strong messages to companies operating in China. We have seen many leading companies make good progress with regard to improving their cybersecurity preparedness.

First and foremost, the best practices are to comply with governing laws and regulations. Therefore, it is advisable to assess a company's actual compliance work against the laws and regulations and take measures to fix any gaps.

In addition to the mandatory laws and regulations, a company may need to comply with national and industry specific cybersecurity standards, including some technical standards as guidelines for their cybersecurity work. Typical examples include the Information Security Technology standards formulated by the National Information Security Standardization Technical Committee (almost all new standards mentioned in the previous sections fall within this series).

The Cybersecurity Law encourages companies to take security certifications. By going through the certification process, a company can evaluate its own practices against the certification standards and make changes accordingly to improve cybersecurity. Internationally recognised certifications, including without limitation ISO/IEC 27001, are being widely adopted by Chinese organisations as well.

As the regulatory framework in China on cybersecurity is still at a nascent stage, it is advisable to closely monitor the legislative process and implementations of the laws and regulations and potential impact over a company's business operations.

"By going through the certification process, a company can evaluate its own practices against the certification standards and make changes accordingly to improve cybersecurity. Internationally recognised certifications, including without limitation ISO/IEC 27001, are being widely adopted by Chinese organisations as well."

© Law Business Research 2023

Photo by ESB Professional on Shutterstock

In terms of implementation of cybersecurity measures, companies need to mobilise resources to cover different areas. For example, they need to upgrade their IT infrastructure to maintain a high degree of cybersecurity; employ sufficient qualified technical staff; draft and implement necessary internal policies, especially an incident response policy; adjust the governance structure by appointing a data protection officer or similar roles; and seek readily available legal, forensic, technical and public relations advice in both the case of an incident and in their daily operation.

If any incident has escalated to a certain degree, companies tend to form special task forcse with in-house legal and technical staff and, if necessary, outside counsel as well, to address such incidents. It will help diffuse the situation in a professional and efficient way before it gets out of control.

QUESTIONS

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

Cloud services are one of the fastest growing areas in China in recent years. There are many factors for a company to consider and evaluate before it makes a decision to move data to a cloud hosting environment. These factors include, but are not limited to, security, flexibility, expansion capability, performance, cost, legal compliance, etc. If a company decides to go the cloud, the general recommendation is to assess the possibility of constructing the company's own private cloud system or to deploy hybrid cloud, and only if both are unrealistic, consider the public cloud.

With respect to special data security and privacy concerns, a company should evaluate such concerns in a larger context to determine the most suitable cloud service. As public cloud services cover a huge volume of users and multiple business models, they are more vulnerable to hacking. Hardware sharing is common for the public cloud. This means competitors using the same cloud services may share the same server. Further, the public cloud may not always meet certain compliance requirements, such as local storage of data. In contrast, a private cloud allows a company to deploy appropriate security measures as it sees fit, which will offer a higher degree of security. It is comparatively easier to meet compliance requirements using a private cloud. But the cost for a private cloud is also higher than the public cloud. Therefore, a company must strike a balance between the competing values of relevant factors in choosing cloud services. It is worth noting that two national standards related to cloud computing will take effect on 1 December 2023, which are the Security Guidance for Cloud Computing Services and the Security Capability Requirements for Cloud Computing Services, of which the full texts are not available as at the date of this chapter.

© Law Business Research 2023

"Another notable concern is that cloud services are not entirely open for foreign investors in China. Foreign cloud service providers may need to cooperate with local partners to step into the China market."

In China, leading public cloud service providers include Alibaba, Tencent, Huawei, China Telecom and AWS. Although private cloud service providers, such as Huawei and Lenovo, are also available, the main users of private-only cloud services are comparatively limited to financial institutes in China. Companies with data security and privacy concerns tend to separate data into different categories based on the security grades. For example, a customer's credit card number will be stored on the private cloud with higher security protection. In contrast, official website content can be stored on the public cloud with less security protection. Such a hybrid cloud solution may also help the company to meet balace various compliance requirements with cost concerns.

A company shall closely monitor sector-specific regulations and standards with respect to cloud deployment. For example, the MIIT has published multiple recommendatory standards (non-binding) for the telecoms sector since mid-2021. The People's Bank of China has also published three recommendatory standards regarding cloud computing for financial institutions in late 2020.

Subject to its business model, a company shall closely monitor data security and privacy related laws and regulations. It shall design its core products or services from the beginning of its operation with a concept of categorised separation of data in accordance with applicable laws and regulations. This will prove more efficient and cost-effective for the company when it decides to go on the cloud later.

Further, cross-border transfer of data could be a key concern when considering cloud deployment. Pursuant to the relevant regulations, storing data overseas is deemed as a form of CBDT, hence companies will need to go through the Security Assessment or enter into the China SCCs with their cloud solution providers, if the cloud servers are located outside of China. In addition to generally appliable laws and regulations, companies in certain sectors (eg, financial

© Law Business Research 2023

institutions, credit business agencies, insurance companies, medical institutions, ride-hailing service providers and smart cars) are also subject to sectoral data localisation requirements.

Another notable concern is that cloud services are not entirely open for foreign investors in China. Foreign cloud service providers may need to cooperate with local partners to step into the China market. Therefore, users of cloud service providers with a foreign background need to consider the business model of the service provider and consider whether it will have any impact on the services requested.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The Chinese government takes serious cybersecurity threats and criminal activity seriously.

The CAC is the main regulator with first-hand knowledge of market trends and cybersecurity threats through law enforcement activities, based on which it will lead the promulgation of new or amended regulations to address such concerns.

Owing to the rapid development of mobile technologies, CAC and other competent regulators such as the MIIT, the MPS and the SAMR have focused their law enforcement efforts in regulating mobile applications in recent years. These regulators have the authority under the law to request application stores to suspend or remove download channels for illegal applications. In the meantime, other sectoral regulators have also initiated special campaigns over the past year to urge relevant market players to identify and rectify non-compliant practices, such as the former China Banking and Insurance Regulatory Commission's campaign against banks and

Photo by askarim on Shutterstock

insurance companies, and the State Postal Administration's campaign targeting at delivery companies.

If any criminal offence leads are discovered during their investigation or review, such cases will be referred by the relevant regulators to the police to initiate criminal investigations. Individual citizens or entities, especially those victims of cybersecurity threats, are also encouraged to report crimes to the authorities, while providers of network products are legally obliged to report verified cybersecurity loopholes to the MIIT.

Law enforcement actions against cybersecurity threats are increasing. Civil lawsuits and public interest lawsuits against cybersecurity breaches are also increasing. According to statistics of the Supreme People's Procuratorate (SPP), over 6,000 public interest lawsuits for personal information protection were filed by procuratorates at various levels in 2022.

There are likely to be criminal liabilities for data violations. According to China's Criminal Law, criminal penalties for computer

© Law Business Research 2023

"The SPC and provincial high courts regularly publish model cases in relation to cybersecurity crimes to raise public awareness and deter future offences. Although China does not have a case law tradition, to some degree these model cases also serve as precedents for lower-level courts to rule on cases."

hacking-related offences range from three- to five-year, or even longer, imprisonment sentences. For other crimes (eg, fraud, theft and embezzlement) conducted via cybersecurity breaches, penalties for the same crimes (conducted in a traditional offline matter as set out in the Criminal Law) will also apply. In addition, the Law on Anti-Telecom and Internet Fraud took effective on 1 December 2022. This new Law aims at preventing and combating relevant crimes by telecoms, finance and internet regulations.

The Supreme People's Court (SPC) and the SPP jointly issued the Judicial Interpretations on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to the Information Network, which took effect on 1 November 2019. These judicial interpretations include quantified thresholds for punishable criminal offences, which provide guidelines to the police and prosecutors nationwide. The SPC and provincial high courts regularly publish model cases in relation to cybersecurity crimes to raise public awareness and deter future offences. Although China does not have a case law tradition, to some degree these model cases also serve as precedents for lower-level courts to rule on cases. As cybersecurity crimes tend to involve a large number of victims, the police and procuratorates usually take priority in handling these crimes.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

The risk factors vary for different M&A deals. For asset or equity deals with high privacy and data security concerns (eg, purchase of software with heavy collection of user data or the equity of a hotel chain with large customer check-in data or equities of a manufacturer with a large number of employees worldwide, among many other examples)

© Law Business Research 2023

privacy and data security liabilities should be a key, if not a deal-breaking, factor.

There are several steps to follow to minimise potential risks. First, a proper legal and technical due diligence must be done by the buyer. This is especially important for foreign investors who are not necessarily familiar with the relevant data implications in the China market. Often this exercise should be done against not only the Chinese law, but also the relevant laws to all the jurisdictions involved (eg, the portfolio companies have a cross-border structure established for capital financing reasons, or the investors have limited partners from different jurisdictions), which may trigger, among other things, cross-border data transfer concerns (again China has strict rules around cross-border data transfer). Note the due diligence findings may prove a no go, and if that is the case, of course, the earlier the finding is made, the better for both parties.

Second, subject to the due diligence findings, some rectification measures shall be taken either before signing, or as closing conditions or post-closing covenants (depending on circumstances). The buyer should consider requesting a reduction in the valuation of the target, escrow arrangement, etc, to hedge against potential liabilities. Certain representations and warranties should be customised with certain carve-outs to reflect the due diligence findings.

Third, subject to the magnitude of potential legal liabilities due to violations of privacy and data security, the buyer may insist on special compensation (which can be as severe as, for example, reversing the deal or down to the personal liabilities of the individual sellers) or offset of remaining payments (in the case of a payment schedule in several tranches with some payable after closing).

Fourth, the buyer should consider relevant insurance policies to cover liabilities for privacy and data security violations.

From the seller's perspective, it is important to shortlist credible buyer candidates. Once serious negotiations have commenced with selected buyers, the seller shall provide full disclosure to the buyers under a satisfactory confidentiality agreement. Properly documented full disclosure is the right defence for any subsequent buyer claim after closing. Further, as a general rule in M&A deals, the seller should consider setting certain time limits to provide any compensation, including for privacy and data security violations. Needless to say, operating in a compliant way (especially navigating the dynamic Chinese data law) from day one is important for the seller.

Jingyuan Shi
jingyuan.shi@simmons-simmons.com

Simmons & Simmons
Shenzhen
www.simmons-simmons.com

Yuchen Lai
yuchen.lai@simmons-simmons.com

Read more from this firm on Lexology

© Law Business Research 2023

QUESTIONS

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Each law firm has its own focused practices. Clients should seek cybersecurity advice from lawyers who have a long-term track record of experience in navigating cybersecurity and data protection with a legal and a sectorial eye where relevant to the client. As cybersecurity often goes beyond national borders and, more importantly, nowadays data legislation from the key economies globally is influencing each other so heavily (especially the GDPR's impacts globally), lawyers with international practice and experience can offer more solid advice and input from a comparative perspective. Good lawyers are always on top of the latest legal developments. Last but not least, reputation or comments on lawyers generated from previous deals may also be key attributes clients should look for.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

There are multiple layers of laws and regulations on cybersecurity and privacy in China. Some have only recently been adopted and without sufficient implementation rules, some may be in the draft stage, and the cybersecurity and privacy related legal framework is evolving at extremely fast pace, with new legislations or drafts coming out almost every month. We anticipate that this trend will continue in the next couple of years. In addition, multiple regulators may be in charge of the supervision of the same issues from different perspectives. Therefore, a client needs expert advice to help correctly analyse their case and navigate in the complex legal and regulatory framework for cybersecurity and privacy compliance in China.

How is the privacy landscape changing in your jurisdiction?

The triangulated safeguard for data regulation (ie, thee Cybersecurity Law, the Data Security Law and the PIPL) are all in place. Lower-level implementation regulations and recommendatory national standards are being drafted or amended accordingly. Key regulators will finalise their internal guidelines on law enforcement where applicable. Regional regulations on data and privacy are also emerging. All of these changes will shape the privacy and data protection regime in China. Businesses, especially multinational business undertakings with a China presence or selling products or services to China, would need to review their privacy approach to comply with these changes. Regulators are bringing enforcement up to speed with this new wave of legislation.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

Business should be particularly aware of cybersecurity incidents that may cause massive data loss, paralyse internet access in wide geographic areas, affect a significant number of users, involve sensitive personal information, involve data (regardless of it being personal or non-personal data) in key sectors, stir up social unrest or involve state secrets, public interest or national security concerns.

© Law Business Research 2023

About Market Intelligence

Respected opinion, expert judgement

Lexology GTDT: Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes in major jurisdictions around the world. Through engaging, easily comparable interviews, the series provides the legal profession's thought leaders with a platform for sharing their views on current market conditions and developments in the law.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most interesting cases and deals.

Read more Market Intelligence topics

This publication is intended to provide general information on law and policy. The information and opinions it contains are not intended to provide legal advice, and should not be treated as a substitute for specific advice concerning particular situations (where appropriate, from local advisers).

Enquiries concerning reproduction should be sent to customersuccess@lexology.com.

Enquiries concerning editorial content should be directed to the Content Director, Clare Bolton – clare.bolton@lbresearch.com.

© Law Business Research 2023