China's Cybersecurity Law Calls for Mandatory Breach Notification and a Robust Incident Response Capability

pwc 普华永道

瑞栢律师事务所
Rui Bai Law Firm

Tiang & Partners
程偉賓律師事務所

Cyber breach incidents are on the rise. According to the results of the 2019 PwC China Unicorn CEO Survey, CEOs believe that data security and privacy protection are the external factors that will have the greatest impact on their companies in the next 1-3 years. While companies may choose to remain silent and keep things under wraps when cyber incidents occur, wherever possible, China's Cybersecurity Law ("CSL"), effective from June 1, 2017, sets out comprehensive requirements for cyber incident response and breach management, including mandatory breach notifications and penalties for failure to comply.

China Cybersecurity Law – A Comprehensive Cybersecurity and Privacy Protection Framework

The CSL establishes a broad range of management and technical requirements for all companies in China that own or operate a network.

These entities are defined as “Network Operators” (NO) and a subset of these entities in critical or sensitive industry sectors are defined as “Critical Information Infrastructure Operators” (CIIO). Article 76 (3) of the CSL defines NOs as network owners and managers or network service providers. In practice, every company which has basic IT equipment or facilities falls into this category. According to Article 31 of the CSL, the State shall carry out special protection of the important industries and fields, such as public communication and information services, energy, communications, water conservation, finance, public services and e-government affairs, critical information infrastructures that , once are damaged, disabled or encountered data breach, may endanger national security, people’s livelihood and public interest, on the basis of the multi-level protection scheme (MLPS) for network security.

Article 10 of the CSL requires all NOs to implement technical and other necessary measures to ensure safe and stable network operability. It also requires that NOs effectively respond to network security incidents, prevent illegal and criminal activities, and maintain the integrity, confidentiality and availability of the data running on the network. Article 21 and 34 respectively state that all NOs and CIIOs must include the following in their CSL compliance frameworks: security policies, roles & responsibilities for IT personnel, anti-virus or anti-cyberattack technical measures, network log retention, systems for data classification, active data backup and encryption for NOs, and additional obligations on CIIOs such as having dedicated security personnel (who are required to go through background checks), mandatory security training, data recovery policies, and incident response plans with regular penetration testing. Failure to effectively build up and implement a robust compliance framework may subject companies and the directly responsible persons to administrative penalties; where serious security incidents occur, criminal liabilities may follow at both corporate and individual levels.

CSL requirements can be grouped into 8 domains as shown in the diagram below:

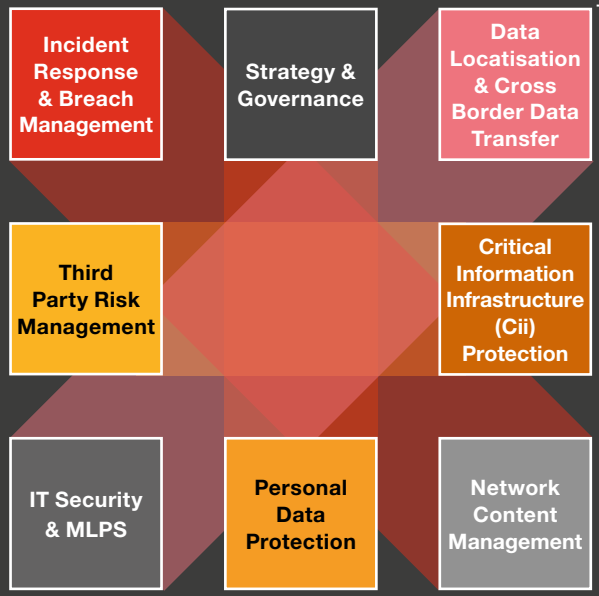
Cyber Security Law of the People's Republic of China

Strategy & Governance

Define an overarching program, policies, governance structure, roles and responsibilities designed to coordinate, design, implement and maintain the program that is aligned with CSL.

Incident Response & Breach Management

Develop and promulgate an incident response plan and conduct training drills. The plan should include steps to notify the authorities and affected data subjects, conduct investigations, supporting the authorities in any follow-up inquiries and remediation of issues identified from the investigation.



Data Localisation & Cross Border Data Transfer

Conduct data inventory, localise and/or perform cross-border data transfer security assessment for Personal and Important data.

Third Party Risk Management

Conduct due diligence procedures, impose privacy & security and confidentiality requirements on third parties to mitigate risks associated with access to the organization's information assets. Ensure 3rd party products and services are certified and approved.

Critical Information Infrastructure (CII) Protection

Identify critical information infrastructure, implement and operate required heightened security and control requirements.

Network Content Management

Establish protocols for web content creation, monitoring websites and user platforms to identify and filter any inappropriate content accessed or posted by users. Utilise licensed and approved VPN services.

IT Security & Multi-Level Protection Scheme (MLPS)

Implement MLPS designated management and technical controls to safeguard network and IT systems. Perform MLPS readiness including grading, registration, self and certified assessments.

Personal Data Protection

Establish a privacy framework with provisions and controls in place to protect personal data throughout the data lifecycle.

Key requirements related to Cyber Incident Response and Breach Management

Within the “Cyber Incident Response and Breach Management” domain, among the many comprehensive requirements, NOs have to notify relevant authorities in the event of a breach as well as affected data subjects whose data may have been leaked or stolen. According to Article 64 of the CSL, failure to comply may result in corporate fines up to RMB 1 million, and for the persons directly responsible, up to RMB 100,000. Companies and key individuals may also be subject to criminal prosecution, while key individuals may face imprisonment and/or be barred from assuming senior corporate roles and taking on professional responsibilities in the future.

Companies must therefore design and implement a robust Incident Response (IR) program to ensure that they are able to address these compliance requirements. Key requirements can be summarized as follows:

- **Incident Response (IR) Plan:** Formulate an IR plan, conduct regular drills. In the event of an incident, execute the plan to contain the threat and minimize disruption and impact (Article 25);
- **Breach Notification:** Notify the relevant authorities and affected data subjects whose data may have been leaked, in a timely manner and provide necessary assistance and support (Article 42);
- **Investigation and Remediation:** Perform a forensic investigation to identify the source and nature of the breach and promptly adopt remedial measures to fix all security issues. Provide necessary assistance and support to the authorities in the event that they conduct an independent investigation (Article 55).

Compliance with CSL requirements mandates a robust Incident Response (IR) Program

Prevent

- Take technical measures to guard against computer viruses and acts that jeopardize cyber security, such as cyberattacks and network intrusions (#21)
- Encrypt and make backups of important systems and data (#21, #34)
- Promptly remediate security flaws and vulnerabilities (#22)
- Formulate IR plan and deal with security risks in a timely manner (#25, #34)
- Regularly conduct emergency drills including those coordinated by relevant authority (#34, #39)

Detect

- Take technical measures to monitor and record network operation status and cybersecurity incidents, and retaining relevant network logs for not less than six months (#21)
- Conduct testing on, and an assessment of, the security of, and the potential risks existing in, its network at least once per year and report results and improvement measures to relevant authority (#38)
- Establish and publicise a complaint/whistle-blowing mechanism, and handle reports in a timely manner (#49)

Respond

- Promptly execute IR Plan upon detection of incident (#25)
- Report incident to relevant authority (#25)
- Notify users whose personal information have been leaked and relevant authority in a timely manner (#42)
- Conduct breach investigation, take measures to eliminate risk and spread of the incident, issue public advisory/warning in a timely manner (#55)

CSL Article number
 # Article number for CIIOs

Recover

- Promptly adopt remedial measures, including restore backups and fix all security issues (#25)
- Provide technical support and assistance to the authority in its activities of safeguarding national security or investigating crimes in accordance with the law (#28)

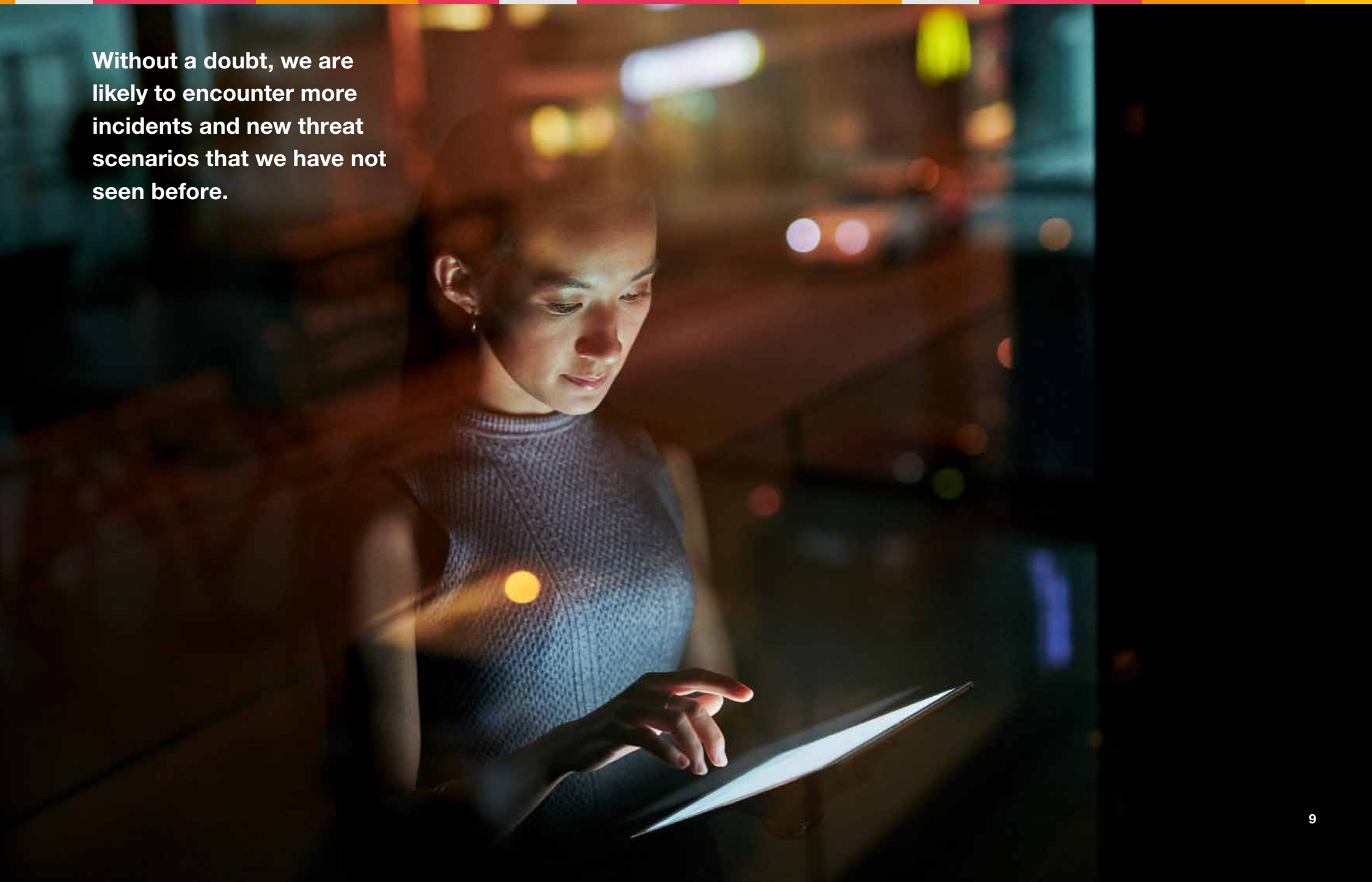
Depending on the company's status as an NO or CIIO, violations of incident response rules may result in corporate fines of up to RMB 100,000 or 1 million and individual fines of up to RMB 50,000 or 100,000. normally, the company in question will see rectification orders and warnings too. In extreme cases, criminal liabilities can be expected (#59, #64)

Work with the Cyberspace Administration of China (CAC) and other government depts. to implement an Emergency Plan for National Network Security Incidents《国家网络安全事件应急预案》

Digital Revolution and the Escalating Threat Landscape

The trend of ubiquitous technology, smarter systems and big data is resulting in a greater adoption and reliance on technology systems in industry, commerce and in our daily lives. The growing reliance on AI is an example of this trend: 60% of CEOs in China and the Asia-Pacific region believe that AI will displace more jobs than it creates, while only 2% of those CEOs are confident that the opposite will occur, according to PwC's 22nd Annual Global CEO Survey.

This increased reliance on technology is strongly linked to an escalation in cyber threats: according to PwC's 2020 Insurance & Beyond survey, the cyber insurance market will grow from $5 billion in annual premiums in 2018 to at least $7.5 billion by 2020. This increase in the cost of cyber insurance not only demonstrates the growing concerns over cyber attacks and incidents, but also the need for more robust incident response capabilities to mitigate their impact and ensure swift recovery.



Without a doubt, we are likely to encounter more incidents and new threat scenarios that we have not seen before.

Key Steps to Manage a Cyber Breach Incident in China

While companies should heavily invest in preventive measures to avoid incidents in the first instance, the notion of a perfectly secure system is idealistic and unrealistic. Therefore companies must be adequately prepared to deal with incidents as and when they arise, enrol the involvement of senior management and cross functional teams while ensuring that processes and methods are compliant with all relevant requirements.

In view of the legal and regulatory landscape in China, when a cyberattack does takes place, proper execution of the following steps will collectively assist in minimizing both first party and third party damages, as well as help to prevent other derivative damages.

Conduct an IT forensic investigation.

This exercise is intended to reveal the root cause, the timing, the existing and potential damages, as well as what parties may be accountable for a cyberattack. It is noteworthy that, similar to other investigations, companies cannot breach the laws and regulations or infringe upon the legitimate rights and interests of individuals when conducting cyber investigations. An “IT forensic” investigation can therefore be used to determine what devices were impacted or infected, enabling forensic specialists to trace back the steps of the attackers to identify how the attack took place. Doing so is crucial to prevent future attacks of a similar nature from reoccurring.

Retain evidence of the incident and of damages.

The retention of digital evidence is required for communicating with the authorities and with data subjects, as well as for insurance claims or other avenues through which affected parties might seek damages. Companies are advised to consider evidence retention while also keeping in mind the need to eliminate the negative effects of the cyberattack. For example, in scenarios where illicit content (such as pornography or terrorism-related information) is leaked online, webpage screenshots and network logs should be preserved to facilitate investigations, but the online content itself should be removed in a timely fashion to mitigate their negative impact. Acquiring forensic images of various devices – servers, PCs and cellphones – is oftentimes a helpful step in conducting the sort of deep-dive technical analysis that can uncover signs of illicit communications with external parties or attempts to remove proprietary data (e.g., intellectual property) from company premises without authorization. An understanding of evidence notarization, particularly for digital evidence, is also crucial for China-based court proceedings. It is highly recommended that any company looking to collect evidence work with their legal teams to determine whether or not notarization will be required, as the notarization of digital evidence is most valuable if it occurs when the evidence is first collected (as opposed to performing notarization after the data has been analyzed and sensitive information has been definitively identified).

Notify in-charge regulatory agencies and concerned data subjects.

Many cyberattacks are followed by virus diffusion, data breach and the spreading of illegally-obtained information to potential black market buyers. Therefore, notifying the appropriate supervisory agencies and data subjects would be helpful to contain the incident at national, regional and individual levels.
It is particularly recommended to include damage control and precautionary measures in the notification letter to data subjects. If data has (or may have) been stolen, hackers will often wait for a period of time, sometimes months, before trying to sell the stolen information on the black market. There are ways, however, to establish scans on black market websites (often only accessible via the dark web) so that companies will know if their data is being sold. Taking such measures is a step in the right direction to demonstrate to regulatory agencies that the data breach is being handled with all due seriousness and that real efforts are being made to mitigate damages.

Respond to government investigation and/or damage actions.

A cyberattack may result in administrative or criminal liabilities imposed by the authority or civil liabilities sought by third parties companies or data subjects. Properly responding to those potential risks is equally important to tackle the first party damage or business continuity issues.

Respond to media exposure.

Even the largest international corporations may struggle to manage the public fallout that occurs from a serious data breach. Identifying a public relations firm that specializes in managing the messaging strategy for cyber incidents is a key element to rebuilding consumer trust and minimizing business impact. Competent incident response and legal teams should also have experience providing public relations firms with the information they need to appropriately manage any media attention and negative public perception.

Notify insurance companies where relevant.

If there is an active cyber insurance policy in place at the time of the incident, it is strongly recommended that the subject of the attack notify the insurance company as soon as possible to verify whether any (or all) damages are covered by the insurance policy. Insurance companies often work in tandem with law firms, IT forensic and public relations firms, forming a cohesive team that can quickly jump into action when an attack is first identified and the policies would typically reimburse the fee for these service providers.

Seeking Restitution.

Seeking damages from third parties and employees that are whole or partially responsible for the consequence of a cyberattack will help minimize monetary loss and deter future noncompliant behavior. When it comes to cyber threats, financial impacts cannot be overstated: PwC's most recent Global Crisis Survey found that financial losses due to these attacks on average exceed USD 1 million, and 1% of all incidents exceeding USD 100 million. The financial impact of a cyber breach – lost consumer trust, fines, and professional service fees – are difficult to measure, but are both long-lasting and hard to mitigate. While cyber insurance can play a helpful role in easing the financial burden of a cyberattack, working with counsel to determine whether and how to seek damages is a critical step in reducing the impact on a company's bottom line.

Post-Incident Review and Lessons Learnt.

A review of the incident and steps taken to address the incident to identify lessons learned, will provide opportunities to improve systems, processes, tools and training to prevent re-occurrence and improve response. In practice, remediation actions should go beyond just implementing more security solutions and/or controls. Employee training is a critical component of cyber security, as many cyber incidents begin with careless employee behavior. In fact, PwC's 2019 Global Crisis Survey found that over two thirds of all cyberattacks originate from phishing emails (or from malware that is transmitted via the phishing email). These kinds of attacks can be prevented with sound employee training.

Keeping in-charge regulatory agencies updated.

Finally, keeping regulatory agencies apprised of remediation efforts is necessary to demonstrate that regulatory requirements are being taken seriously and that there is a genuine commitment to reducing the risk of future cyber incidents. It is recommended that companies implement recommendations from the relevant supervisory agencies, which are normally issued in the aftermath of a serious cyberattack. Companies should also maintain regular communication with these agencies, both during and after an incident. Post-incident reporting is particularly relevant with the development of the Chinese social credit system, whereby companies which have committed serious misconduct or have been blacklisted will be subject to public disclosure and punishment from a variety of government agencies.

Compliance with the CSL is not a simple undertaking for any company with operations in China. Design and implementation of a robust Cybersecurity program supported by a team of cybersecurity professionals, and being prepared to handle cyber incidents is critical to navigating the evolving cyber threat landscape. In the event of a cyber breach incident, various third parties, including IT forensic specialists, law firms and public relations firms can provide the required expertise to improve the outcome of a cyberattack. Companies must know, however, that ultimate responsibility for cybersecurity and prompt response to cyber incidents rests on their shoulders.

Contact us

PwC China

Ramesh Moosa
Partner, Cybersecurity, Privacy & Forensics
PwC
+86 (21) 2323 8688
ramesh.moosa@cn.pwc.com

Sean Pan
Director, Cybersecurity & Privacy
PwC
+86 (21) 2323 2693
sean.pan@cn.pwc.com

Steve Curnan
Senior Manager, Cybersecurity, Privacy & Forensics
PwC
+86 (21) 2323 8003
stephen.s.curnan@cn.pwc.com

Tiang & Partners

Martyn Huckerby
Head of Competition Law, Asia-Pacific
Registered Foreign Lawyer
Tiang & Partners
+852 2833 4918
martyn.huckerby@tiangandpartners.com

Rui Bai Law Firm

Annie Xue
Regulatory Compliance Senior Manager
Rui Bai Law Firm
+86 (10) 8540 4602
annie.xue@ruibailaw.com

www.pwccn.com

www.tiangandpartners.com

www.ruibailaw.com
