Llinks Client Alert — June 2025
Data breaches may be inevitable, but here's a roadmap to proper response

Former Cisco CEO John Chambers once said, "There are only two types of companies: those that have been hacked and those that don't know they have been hacked". In recent years, as more companies rely on digital operations and network technology continues to develop, this statement has become increasingly proven true. Recently, several internationally renowned brands have experienced personal information ("PI") breach incidents of varying scales, once again sounding the alarm for companies to prioritize data security incident response.

In this month's Client Alert, based on our long-term experience in assisting clients with data security incidents, we will address the top 3 concerns for companies.

I. Should individuals be notified after a data security incident occurs?

If PI held by a company is leaked, does the company have an obligation to notify the PI subjects? The answer is, not necessarily.

According to Article 57 of the *Personal Information Protection Law* ("*PIPL*"), if a "PI processor (note: equivalent to the concept of "data controller" under the GDPR) takes measures that can effectively avoid harm caused by data leakage, tampering, or loss, the PI processor may choose not to notify individuals". This means that whether a PI processor has an obligation to notify individuals depends on whether the data security incident has harmful consequences.

1. How to assess the harm of a data security incident to individuals?

How to evaluate whether a data security incident is harmful to individuals? You might have thought of a similar mechanism (also a compliance obligation) under the *PIPL*: PI Protection Impact Assessment ("PIA").

According to the *PIPL*, PI processor should conduct a PIA before engaging in "PI processing activities that have a significant impact on personal rights and interests". The purpose of PIAs is to assess the risks and impacts of PI processing activities on the rights and interests of PI subjects. Although a data security incident is not a PI processing activity, the assessment logic and methods of PIA can be fully applied to assess whether a data security incident will cause harm to individuals.

In a simplified PIA assessment model, the harmful consequences are usually assessed from the following 4 aspects: (1) data sensitivity; (2) possibility of risk; (3) severity of harm; and (4) effectiveness of remedial measures. For example, suppose in a data security incident, the PI leaked by the company includes employees' names, positions, and work emails. Then the assessment process is as follows:

- Data sensitivity: The above PI does not involve sensitive PI, so its sensitivity is low.
- Possibility of risk: Assuming the leaked information is plaintext and has been obtained or accessed by hackers, then there is a risk possibility.
- Severity of harm: Because the leaked information is non-sensitive and limited to work-related fields, without other PI, the possibility of causing harm to personal life, health, property safety, or dignity is low, so the harm severity is low.
- Effectiveness of remedial measures: If the company can promptly fix the loopholes that led to the data leakage after the data security incident and strengthen employees' awareness of the potential harmful consequences after the data leakage (e.g., specific notifications and training for potential phishing emails), then these measures can be considered effective in preventing harm to individuals from data leakage.

After the above assessment and taking corresponding security measures, if it can be determined that the data security incident will not cause harm to individuals, the company may be exempted from notifying the PI subjects. However, it should be noted that in practice, regulatory authorities usually have stricter standards for judging the effectiveness of "avoiding harm", and in any case, regulatory authorities have the power to mandate companies to fulfill their notification obligations after assessment. Therefore, companies must be cautious when judging whether to apply this exception clause to avoid misjudgment and expanded risks.

2. How to notify individuals?

Conversely, if, after assessment, the data security incident may cause harm to individuals, then the company has an obligation to notify individuals, or if regulatory authorities believe that the data security incident may cause harm to individuals, they will also require the company to notify individuals.

In this case, how should a company notify individuals?

In principle, the company should notify each individual affected by the data security incident. Generally, it is recommended that companies use written and traceable methods for notification, such as email, SMS, APP pushes/notifications, etc. Currently, SMS notification is relatively common.

If one-on-one notification is not feasible, the company should take reasonable measures to publicize the notification, such as making an announcement within its APP or through media platforms.

When notifying individuals, the following content should be provided:

- A brief description of the security incident;
- Types and fields of PI leaked;
- Impact of the security incident on individuals;
- Disposal measures already taken or to be taken by the company;
- Suggestions and guidelines for individuals to prevent and reduce risks themselves;
- Remedial measures or compensation provided to individuals;
- Contact information of the company's PI protection officer and protection agency.

II. Should regulatory agencies be notified after a data security incident occurs?

1. When is it necessary to report to regulatory agencies?

Many companies that experience data security incidents ask us whether there is a "threshold" for the number of people for reporting data security incidents to the government. Unfortunately, the *PIPL*'s statement regarding the government reporting obligation for data security incidents is: "If PI leakage, tampering, or loss occurs or may occur, PI processor shall immediately take remedial measures and notify departments performing PI protection duties". It can be seen that the *PIPL* does not set a "threshold" for reporting data security incidents.

Among the existing laws and regulations, the closest provision to a "threshold" is the "general incident", being the lowest level of data incidents stipulated in the *Emergency Plan for Public Internet Network Security Incidents*, whose standard is: "leakage of PI of more than 100,000 Internet users".

In addition, the *Measures for the Administration of Network Security Incident Reporting (Draft for Comment)* ("*Draft Reporting Measures*") released by the Cyberspace Administration of China in December 2023 divide network security incidents into 4 categories: "Critical", "Highly severe", "Moderately severe", and "General". Among them, one of the criteria for determining a "Moderately severe" incident is "leakage of PI of more than one million people". It is worth noting that the *Draft Reporting Measures* do not specify whether "General" level network security incidents that do not meet this standard (i.e., leakage of less than 1 million PI) also require mandatory reporting. At this stage, it is recommended that companies still follow the requirements of the *PIPL*. That is, once PI leakage occurs, regardless of the quantity, it should be reported to the regulatory authorities. To balance efficiency and compliance, companies can first briefly explain the situation to the regulatory authorities by phone or other means, and then supplement and improve the materials according to the instructions of the regulatory authorities (such as requiring submission of a written report).

2. What is the time limit for reporting to regulatory agencies?

The *PIPL* requires companies to "immediately" take remedial measures and notify relevant regulators when a security incident occurs, but it does not provide a specific time definition for

"immediately". The *Draft Reporting Measures* elaborate on this, requiring companies to complete reporting for "Moderately severe" and above security incidents (including situations involving the PI leakage of 1 million or more people) within 1 hour of the incident.

Accordingly, if a security incident involves the leakage of 1 million or more PI, it is recommended that companies report to the regulatory agencies within 1 hour; for security incidents with a scale of less than 1 million, although there is no clear mandatory time limit, based on the principle of "immediate" notification in the *PIPL*, it is recommended that companies report as promptly as practically possible. Generally, if a company can report within 24 hours, it can usually be considered to meet the time limit requirements.

3. Is there no concern for domestic entities if the leakage occurs overseas?

It should be noted that in scenarios involving cross-border data transfer, even if the data leakage occurs overseas, the reporting obligation of domestic entities cannot be exempted. In other words, even if PI is transferred abroad through compliant means such as SCCs, if the PI is leaked due to security loopholes of the overseas recipient (e.g., group headquarters), the domestic entity that initially collected and exported the PI is still responsible for the entire data lifecycle. During investigations, regulatory authorities have the right to require domestic entities to explain their due diligence when selecting overseas partners, the content of bilateral data export agreements (such as SCCs), technical and management measures deployed to ensure data export security, and the coordination and response with overseas parties after the incident.

III. How should companies prevent data security incidents?

No company can 100% avoid data security incidents, but by taking the following measures, companies can minimize the probability of data security incidents occurring.

1. Build a data security protection system

Effective risk management outweighs passive crisis response. Companies should start from ex-ante prevention, in-process monitoring, and ex-post response to build a comprehensive data security and PI protection system.

1) Systemic Measures

From the perspective of institutional construction and organizational assurance, companies should focus on building and improving the following management mechanisms:

- **Improve internal management systems:** Formulate security policies covering the entire lifecycle of data collection, storage, use, transmission, and destruction, and refine data

classification and grading standards, access control policies, and network security emergency plans.

- **Clarify data security responsibilities and management bodies:** Establish dedicated data security officers and management teams, and grant them sufficient authority and resource support to implement data security strategies.
- **Conduct data security training:** Regularly organize dedicated training for all employees, especially those in positions processing core or sensitive data, to enhance their security awareness and practical protection skills, and help employees identify and prevent security risks in daily work, such as phishing.
- **PIA:** For high-risk data processing activities such as processing sensitive PI, using PI for automated decision-making, providing or publicly disclosing PI on a large scale, and transferring PI abroad, companies must proactively conduct a PIA before initiation. This is not only a statutory requirement but also an important means for companies to identify, assess, and take measures to mitigate potential data security risks.
- **Implement data minimization:** In all aspects of data processing, strictly adhere to the principle of data minimization, ensuring that PI collection and processing activities are strictly limited to the minimum necessary scope for specific processing purposes that have been informed to users and for which their consent has been obtained (or which comply with other statutory legal basis), resolutely avoiding excessive collection and unnecessary processing, thereby reducing the impact of potential data breaches at the source.

2) Technical Measures

At the technical level, companies need to deploy multi-layered protective measures. Combined with industry best practices, key technical measures usually include:

- **Access Control:** Establish strict identity authentication and permission management mechanisms, adhering to the principles of “least privilege” and “separation of duties”, to ensure that different roles can only access the data required for their duties.
- **Encryption and De-identification:** For sensitive data, whether in storage or transmission, appropriate strength encryption technology should be adopted for protection; when providing data to external parties or performing internal data analysis, de-identification or anonymization techniques should be used as much as possible to reduce the risk of PI being re-identified.
- **Security Audit and Log Recording:** Record all key data processing activities and conduct regular security audits to effectively trace the cause in the event of a security incident.
- **Vulnerability Scanning and Penetration Testing:** Regularly conduct security vulnerability scans and penetration tests on information systems and applications to promptly discover and fix potential security flaws.
- **Intrusion Detection and Prevention Systems:** Deploy firewalls, intrusion detection/prevention systems (IDS/IPS), Web application firewalls (WAF), and other

network security devices to monitor, identify, and effectively defend against internal and external network attacks in real time.

- **Data Backup and Recovery:** Establish reliable backup mechanisms and regularly drill data recovery procedures to ensure rapid and complete data recovery in case of accidents and to maintain business continuity.

2. Vendor Management

Based on our experience, many data security incidents do not occur within companies but originate from data breaches of third-party vendors or service providers. Therefore, effective management of external Vendors is an important part of a company's prevention of data security incidents. Specifically, companies should focus on the following aspects:

1) Prudent selection of vendors

At the beginning of cooperation, prudent selection of Vendors is the first hurdle. Companies must conduct comprehensive due diligence, examining their internal management systems, technical protection capabilities, industry qualifications related to data security (such as ISO 27001/27701 international standard certifications), past data security incident records, maturity of emergency response mechanisms, and (if applicable) their own compliance operations.

2) Sign data processing agreements

After selecting a partner, a clear, comprehensive, and well-defined data processing agreement should be signed. The agreement should clarify the roles and responsibilities of both parties in data processing activities, detailing the purpose, duration, and methods of data processing, the types and scope of PI involved, the security measures both parties need to take (which should be no less than the company’s own standards and legal and regulatory requirements), data confidentiality obligations, notification and cooperation mechanisms in the event of a data breach (e.g., requiring the vendor to report to the company within a specified time), the company’s audit rights over the vendor, restrictions on the vendor’s re-entrustment (i.e., conditions and procedures for subcontracting to sub-vendors), liability for breach of contract, and requirements for data deletion or return after the cooperation ends.

3) Continuous supervision and audit

Vendor management is not a one-time effort. Companies must establish and implement a dynamic supervision and audit mechanism covering the entire vendor cooperation cycle. This includes regularly requiring vendors to submit documentation of their data security status, such as the latest security assessment reports, compliance certifications, or third-party independent audit opinions, to dynamically assess their security protection level. At the same time, the

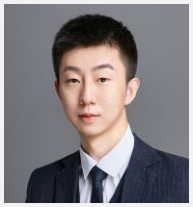
company’s audit rights over the vendor’s data processing activities should be clearly stated in the data processing agreement, so that when necessary, through questionnaires, remote system checks, and even on-site inspections (while adhering to confidentiality and minimal disruption principles), it can verify whether the vendor continues to comply with the agreement and regulatory requirements. In addition, for situations where vendors may subcontract the data entrusted to them to sub-vendors, companies should establish strict prior approval and continuous supervision mechanisms. It is usually required that the vendor must obtain the company’s clear written consent before any form of sub-contracting and ensure that the main vendor, through binding contractual terms, effectively transmits and binds the sub-vendor with data protection standards and obligations no less than those in the main contract.

Our legal services related to data security incident response include:

- Assist clients in establishing the policy and procedural framework for responding to data security incidents.
- Assist clients in establishing a Crisis Management Team (CMT) and defining CMT personnel responsibilities.
- Grading security incidents according to applicable regulatory classification and grading standards, and initiating corresponding disposal guidelines and operating procedures.
- Assist clients in fulfilling statutory reporting obligations in China and other jurisdictions.
- Provide legal services regarding network security and service procurement during the emergency transition period.
- Analyze the impact of security incidents on relevant business contracts of the company (whether it constitutes force majeure, change of circumstances) and assist in negotiating with contract counterparts.
- Analyze the impact of security incidents on other external stakeholders (e.g., affected individuals) and assist clients in communicating with relevant parties.
- Assist clients in negotiating with hacker attackers on ransom extortion and other matters.
- Assist clients in claiming compensation from insurers for cybersecurity insurance.
- Assist clients in responding to inquiries and challenges from the media and other third parties.
- Provide legal services to clients for legal disputes arising from security incidents (initiating lawsuits, responding to lawsuits, and data export security assessments).
- Assist clients in responding to on-site inspections/investigations by regulatory authorities.

If you are in need of any of our legal services, please feel free to contact us:

David Pan
+86 21 3135 8701
david.pan@llinkslaw.com



Nigel Zhu
+86 21 3135 8683
nigel.zhu@llinkslaw.com

SHANGHAI	BEIJING	SHENZHEN
19F, ONE LUJIAZUI 68 Yin Cheng Road Middle Shanghai 200120 P.R.China T: +86 21 3135 8666 F: +86 21 3135 8600	30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli, Chaoyang District Beijing 100020 P.R.China T: +86 10 5081 3888 F: +86 10 5081 3866	18F, China Resources Tower 2666 Keyuan South Road, Nanshan District Shenzhen 518063 P.R.China T: +86 755 3391 7666 F: +86 755 3391 7668
HONG KONG	**LONDON**	
Room 3201, 32/F, Alexandra House 18 Chater Road Central, Hong Kong T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE United Kingdom T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD