Understanding China's New Draft for Cybersecurity Incident Reporting Measures: A Practical Guide for Network Operators

CAI PENG

On December 8, 2023, the Cyberspace Administration of China (CAC) introduced *Administrative Measures for the Reporting of Cybersecurity Incidents (Draft)* ("Measures"). This significant draft, now open for public commentary, mandates specific reporting requirements for network operators in the event of a cybersecurity incident. It clearly outlines the categories of incidents that need to be reported, the information that must be included in these reports, and the consequences for failing to report. This Measures marks a critical enhancement in China's approach to managing and mitigating cybersecurity risks.

1. Identifying the Key Subjects: Who Does the Measures Apply To

The Measures specifically target key subjects within the PRC jurisdiction responsible for network-related activities. These subjects, when facing incidents that jeopardize network security, is obligated to report per the Measures. The primary subjects include:

Subjects	How to Identify
Network Infrastructure Builders	those involved in the construction of network systems within China
Network Service Providers	entities providing network services, including ISPs, data centres, etc
Network Operators	owners and administrators of networks and network service providers

above subjects will hereinafter be collectively referred to as "Operators"

Each of these Operators must promptly report any 'cybersecurity incident', defined by the Measures as events causing harm to networks or information systems due to human error, technical failures, natural disasters, and other similar causes.

2. Reporting Procedure: How Should the Cybersecurity Incident Be Reported

The Measures require Operators to adhere to specific reporting procedures, which vary depending on the severity of the cybersecurity incident. Each category of incident demands distinct reporting protocols, as outlined in the table below:

Incident Severity	Reporting Subject	Reporting Authority	Required Time	Additional Notes
General/Relatively Severe	Operators of Critical Information Infrastructures ("CII")	• Operators report to the cybersecurity protection departments within the CII. • Operators report to the industrial supervisory body, if any, per the reporting requirement of the supervisory body. • In case of suspected crime, Operators shall report to the Public Security Bureau as well.	within **1 hour** if relatively severe	Operators shall promptly activate the emergency response plan.
	Operators of the Networks and Systems under Central/State Organs	• Operators report to the cybersecurity departments within the Central/State Organs. • Operators report to the industrial supervisory body, if any, per the reporting requirement of the supervisory body. • In case of suspected crime, Operators shall report to the Public Security Bureau as well.		
	Other Operators	• Operators report to the local Cyberspace Administration. • Operators report to the industrial supervisory body, if any, per the reporting requirement of the supervisory body. • In case of suspected crime, Operators shall report to the Public Security Bureau as well.		
Severe/Extrem	• Operators of CII	• 1st line: Operators report to the Cybersecurity Protection	Within **1 hour**	Operators shall

Incident Severity	Reporting Subject	Reporting Authority	Required Time	Additional Notes
ely Severe	• the Cybersecurity Protection Departments of CII	Departments of the CII. • 2nd line: the Cybersecurity Protection Departments of the CII escalate the report to the CAC and the Ministry of Public Security upon receiving the first line report from Operators.	for both lines of the report	promptly activate the emergency response plan.
	• Operators of the Networks and Systems under Central/State Organs • the Cybersecurity Departments of the Central/State Organs	• 1st line: Operators report to the Cybersecurity Departments of the Central/State Organs. • 2nd line: the Cybersecurity Departments of the Central/State Organs escalate the report to the CAC upon receiving the first line report from Operators.		
	• Other Operators • Local Cyberspace Administration	• 1st line: Operators report to Local Cyberspace Administration. • 2nd line: Local Cyberspace Administration escalate the report to the next higher-level CAC upon receiving the first line report from Operators.		

This structured approach ensures that the right level of urgency and detail is applied to each incident, facilitating efficient and effective communication with relevant authorities.

3. Incident Classification: General, Relatively Severe, Severe and Extremely Severe

In accordance with the attached Cybersecurity Incident Classification Guidelines to the Measures, cybersecurity incidents are categorized into four degrees: General, Relatively Severe, Severe, and Extremely Severe. The classification of cybersecurity incidents is based on the incident's scale and impact. This framework is designed to ensure a consistent and effective approach to managing and responding to varying levels of cybersecurity threats. To be specific:

Categories	Description	Classic Scenarios
Extremely Severe	Key network system losses, state secret theft, significant national security threats, major social disruption, extensive economic loss, or mass illegal information spread.	• Provincial-level or higher party and government portal websites, and key news websites are inaccessible for over 24 hours due to attacks or malfunction. • The overall operation of CII is interrupted for over 6 hours or the main functions are interrupted for over 24 hours. • The work and life of more than 30% of the population in a single provincial administrative region are affected. • The water, electricity, gas, oil, heating, and transportation service of more than 10 million people is affected. • Important data is leaked or stolen, posing an extremely serious threat to national security and social stability. • Personal information of more than 100 million people is leaked. • Party and government portal websites, key news websites, and network platforms are attacked and tampered with, resulting in the widespread dissemination of illegal and harmful information. • Direct economic losses of more than 100 million RMB.
Severe	Serious system losses, notable data breaches threatening national security and social order, but less severe than	• City-level or higher party and government portal websites, key news websites are inaccessible for over 6 hours due to attacks or malfunction. • The overall operation of CII is interrupted for over 2 hours or the main functions are interrupted for over 6 hours. • The work and life of more than 30% of the population in a single city-level administrative region are affected. • The water, electricity, gas, oil, heating, or transportation service of more than 1 million people is affected.

	Extremely Severe incidents.	• Important data is leaked or stolen, posing a serious threat to national security and social stability. • Personal information of more than 10 million people is leaked. • Party and government portal websites, key news websites, and network platforms are attacked and tampered with, resulting in the widespread dissemination of illegal and harmful information. • Direct economic losses of more than 20 million RMB.
Relatively Severe	Substantial disruptions and data breaches, posing serious security and stability threats, but with lesser impact than Severe incidents.	• City-level or higher party and government portal website, key news websites are inaccessible for over 2 hours due to attacks or malfunction. • The overall operation of CII is interrupted for more than 30 minutes or the main functions are interrupted for more than 2 hours. • The work and life of more than 10% of the population in a single city-level administrative region are affected. • The water, electricity, gas, oil, heating, or transportation service of more than 100,000 people is affected. • Important data is leaked or stolen, posing a relatively serious threat to national security and social stability. • Personal information of more than 1 million people is leaked. • Party and government portal website, key news websites, and network platforms are attacked and tampered with, resulting in the relatively widespread dissemination of illegal and harmful information. • Direct economic losses of more than 5 million RMB.
General	Incidents posing threats to security, order, and public interest but not reaching the severity of the above categories.	

4. Reporting Items for Operators: Article 5 & Attachment of the Measures

According to Article 5 of the Measures and its attached Cybersecurity Incident Information Reporting Form, the following items shall be included in the report prepared by Operators:

Items	Description
Organization and Infrastructure Details	Name of the central/state organs or the enterprises where the incident occurred and essential details about the affected facilities, systems, and platforms.
Incident Discovery and Impact Assessment	Time and location of discovery, incident type, impact, measures taken, and their effectiveness. For ransomware, include ransom details.
Incident Development	Ongoing trends, potential future impacts, and harms.
Preliminary Cause Analysis	Initial assessment of the incident's cause.
Investigation and Analysis Requirements	Information needed for further analysis, including possible attacker details, attack paths, and vulnerabilities.
Response and Future Plans	Future response plans and support needs.
Site Protection Status	Current security conditions at the incident location.
Additional Information	Other relevant information as necessary

Initial reports should focus on the first two items if full details are not immediately available, with a comprehensive report due within 24 hours. Post-incident, a thorough analysis covering response measures, impacts, and lessons learned must be compiled within 5 days.

Service providers shall promptly notify Operators to report Relatively Severe, Severe or Extremely Severe Incidents. If Operators fail to report accordingly, service providers can report directly to the appropriate cyberspace administrations. Additionally, social organizations and individuals are encouraged to report

Relatively Severe or above cybersecurity incidents as well.

5. Penalties for Non-Compliance in Cybersecurity Reporting: Look for Superior Laws

The Measures indicates that if reporting obligations are not met, Operators will face corresponding legal consequences prescribed by various superior laws. For specific penalties, the Measures refers mainly to *the Cybersecurity Law* (CSL), *the Personal Information Protection Law* (PIPL), and *the Data Security Law* (DSL), among others. The CSL, for instance, imposes warnings and fines for general non-compliance, escalating to higher fines for serious violations. The PIPL specifies fines and potential business suspension for severe breaches. The DSL also details fines and potential business suspensions, while the *Regulations on the Security Protection of Critical Information Infrastructure* imposes fines for reporting failures, with increased penalties for repeated or grave offenses."

6. Compliance Strategies: Aligning with New Measures for Enhanced Vigilance

Under the new Measures, Operators are required to follow specific protocols both in preventing and responding to cybersecurity threats. The forthcoming chart details these vital measures we recommend, aligning with the Measures' objectives, to enhance Operators' cybersecurity vigilance and responsiveness:

Category	Compliance Area	Recommended Actions
Preventative Measures	Data Protection	Implement data classification, encryption, isolation, and masking to prevent data breaches.
	Emergency Response	Develop response plans, establish teams, and conduct regular exercises for internet incidents.
	Organizational Structure	Formulate and monitor cybersecurity policies, implement network security, and conduct information security training.
	Legal Compliance Audit	Regularly audit cybersecurity measures for regulatory compliance.
Remedial Actions	Post-Incident Management	Collect incident information, identify causes and effects, and take immediate actions to minimize harm.

	Reporting and Notification	Report incidents to authorities as required and inform affected individuals of personal data breaches.
	Documentation and Analysis	Maintain detailed records of incidents, actions taken, and analyze for future improvements.

Conclusions

The Measures represents a pivotal step to enhance China's cybersecurity framework. Aiming to reduce the repercussions of cybersecurity incidents and fortify national cyber defences, it is designed to work in tandem with China's current legal frameworks such as CSL, PIPL, and DSL. By establishing a unified reporting protocol, the Measures seek to streamline the process of incident reporting, thereby improving the overall effectiveness of cybersecurity governance in the country. We will closely track the legislative process upon this new Measures and update the readers with further analysis upon its official release.