LUCY AWARENESS

China Cybersecurity Law Amendments

(Effective 1 January 2026)

Regulatory signals and implications for organisational readiness

Overview

China has enacted the first substantive amendments to its Cybersecurity Law since the legislation came into force in 2017. Effective from 1 January 2026, the revisions significantly increase enforcement powers, expand regulatory reach, and align cybersecurity obligations with China's modern data-protection and AI governance framework

The amendments do not introduce prescriptive technical controls. Instead, they raise expectations around governance, accountability, and demonstrable risk management across organisations operating in, or digitally connected to, China.

Who is in scope

- Organisations operating networks, platforms, or digital services in China
- Foreign entities whose digital activities may affect China's cybersecurity or data environment
- Technology vendors, SaaS providers, and supply-chain partners supporting China-based customers

Key regulatory shifts

Stronger enforcement and liability

- Regulators may impose penalties **without prior warnings**
- Significantly higher fines for organisations and accountable individuals
- Expanded use of non-financial sanctions, including service suspension and operational restrictions

Closer integration with data and AI governance

- Direct alignment with the Personal Information Protection Law (PIPL) and Data Security Law
- Formal recognition of AI-related cyber risks, including misuse, automation, and synthetic content

Broader regulatory reach

- Explicit extraterritorial application where overseas activity impacts China's networks or data
- Wider interpretation of cybersecurity obligations across systems, services, and platforms

What regulators implicitly expect

Although the law does not mandate specific security controls or training requirements, enforcement trends indicate that organisations are expected to demonstrate:

- The ability of staff to recognise, handle, and escalate cyber risks correctly
- Consistent and repeatable incident handling and reporting processes
- Clear cybersecurity governance and internal accountability
- Ongoing improvement, not one-off compliance exercises
- Preventive measures that materially reduce human-led security failures

clifford.ang@lucysecurity.com www.lucysecurity.com +41 44 557 19 37

Commercial and operational relevance

01

Human-originated incidents

Human-originated incidents (e.g. credential misuse, social engineering, improper data handling) now present heightened legal and operational risk

02

Senior management

Senior management exposure increases the need to evidence “reasonable and proportionate” controls

03

Organisations

Organisations must be able to prove preparedness, not merely assert it

The Challenge

The 2026 amendments signal a clear regulatory shift away from checkbox compliance and toward demonstrable organisational readiness. As enforcement becomes faster, broader, and more personal in its accountability, the rationale for systematically addressing human cyber risk becomes significantly stronger.

In this environment, organisations that invest in improving how people recognise, respond to, and manage cyber threats are materially better positioned to reduce exposure, support defensible compliance, and withstand regulatory scrutiny

The Solution is Lucy

Lucy Security helps APAC organisations meet these new legal burdens in three specific ways:

Building "Affirmative Defenses" Through Training

Challenge

The new legislation introduces leniency provisions for organisations that proactively mitigate harm.

How we assist

By utilising Lucy’s automated security awareness training and phishing simulations, your organisation can establish a "culture of compliance." In the event of a breach, possessing a verified record of employee training serves as crucial evidence to support arguments for reduced penalties under the new "good faith" mitigation clauses.

Meeting AI Governance Standards

Challenge

With the update effective from 1 January 2026, AI technologies are now formally integrated into China’s cybersecurity framework, necessitating risk assessments and ethical oversight.

How we assist

Lucy Security’s platform includes specialised modules on AI Safety and Ethics. We facilitate your teams' understanding of the risks associated with Generative AI—such as deepfakes and data leakage—ensuring that your staff deploy these tools within the confines of the new regional regulations.

Protecting Against Extraterritorial Risk

Challenge

Given that the legislation now extends beyond China’s borders, any APAC employee managing Chinese data may constitute a potential liability.

How we assist

Our platform supports over 130 languages, including simplified and traditional Chinese. This capability enables you to implement standardised, high-quality security training across your entire regional workforce, thereby minimising the risk that "human error" in a satellite office could result in a substantial fine or shutdown of your operations in China

clifford.ang@lucysecurity.com www.lucysecurity.com +41 44 557 19 37