THE NATIONAL LAW JOURNAL
JULY 2017
An ALM Publication
THE PRACTICE | Commentary and advice on developments in the law

China's New Cybersecurity Law Is a Start

BY NICK AKERMAN AND DAN GOLDBERGER

ON JUNE 1, CHINA'S NEW CYBERsecurity law took effect. The new law applies not only to domestic Chinese companies but has wide-ranging implications for U.S. and other foreign companies doing business in China.

Since its passage last November, the cybersecurity law has faced heavy criticism from the international business community, primarily due to the burdens it places on multinational companies operating in China that use, store and move data in and out of China. The law has also faced criticism over its ambiguous language. Even the most seasoned China watchers cannot say with any certainty how the Chinese government will enforce it.

The cybersecurity law applies to businesses in all sectors of the Chinese economy and creates a national approach to protecting data. It regulates the data that companies may store, and where and how they store it. It also heavily restricts what a company may do with personal data collected and stored in China.

However, the law is ambiguous in many respects, which has created significant uncertainty for businesses operating in China. For example, operators of "Critical Information Infrastructure," an undefined term in the law, are subjected to heightened security obligations. Because the term is not defined, we cannot be sure which companies qualify as these operators.

Despite the unease and uncertainty over the new law, there are positives, as well. The law adopts data regulatory standards from the European Union and the U.S. Thus, at least with respect to data security compliance, multinational companies operating in China will not need to develop a new framework from the ground up. Instead, they likely have the building blocks in place with their current data compliance programs operative in the U.S. and EU.

In the U.S., the trend has moved away from a reactive approach of dealing with data breaches after they occur to a more proactive approach of preventing data breaches through a seven-step data security compliance program.

In drafting its new cybersecurity law, China has adopted the criteria of what has become the gold standard in the U.S. for an effective data security compliance program.

OSTILL/SHUTTERSTOCK.COM

U.S. compliance, based on the seven steps in the Federal Sentencing Guidelines, requires companies to promulgate data security policies and procedures that are consistently enforced through high-level oversight, periodic audits to ensure the compliance plan's effectiveness and mechanisms for reporting and responding to violations. However, the "national standards" referenced in the China law have not yet been promulgated, and until they are, compliance with these articles remains aspirational.

Under the law, companies must identify the relevant persons responsible for corporate data security oversight and ensure that those individuals do not pose a risk for unethical behavior. Without adequately trained compliance personnel, the policies and procedures obviously cannot be effectively enforced.

Importantly, periodic audits are also mandated by the law to ensure enforcement of policies. Testing the efficacy of its data compliance program enables a company to assess its effectiveness before a data breach has occurred.

The new law also requires companies to establish mechanisms for reporting data security violations and relies on company employees to do so.

Though China now has the building blocks in place for data security compliance, the government hasn't been clear enough about its new cybersecurity law and how it will interpret it. This creates uncertainties and unknown risks for companies doing business in China.

For now, China has created an effective framework for data security compliance. The devil will be in the details.

NICK AKERMAN *and* **DAN GOLDBERGER** *are partners at Dorsey & Whitney. Akerman's practice focuses on civil and criminal trials and data protection. Goldberger's practice focuses on complex commercial litigation, intellectual property litigation and data protection.*