DORSEY
DORSEY+WHITNEY LLP

China Adopts Tough and Sweeping Cybersecurity Law

December 8, 2016 – The TMCA
by Daniel Goldberger, Ray Liu Esq., Nick Akerman, Frank Hong, and Peter Corne

On November 7, 2016, the Standing Committee of China's National People's Congress promulgated the Cybersecurity Law of the People's Republic of China, a law James Zimmerman, chairman of the American Chamber of Commerce in China calls "a step backwards for innovation in China that won't do much to improve security." The law becomes effective on June 1, 2017 and will apply to businesses in every sector of the economy. While the law purports to create an overall national cyber security plan, its provisions, some of which are vague, create significant potential uncertainties for companies doing business in China. Below are some of the noteworthy provisions of the law. Full details regarding the law can be found on Dorsey's Computer Fraud and Data Protection Blog here.

- Makes local storage mandatory and eliminates the option of storing business data outside of China, if (1) the company falls within the definition of an operator of "critical information infrastructure" ("CII"), and (2) there are personal information and "important data" collected and generated in China.
- For certain "important" sectors enhanced security obligations will be triggered. These include public communications, information service, energy, transport, water conservancy, finance, public service and e-government, as well as other CII.
- Companies will be required to have clear policies and procedures to protect data and information, and those policies and procedures must comply with national standards.
- Companies must establish high-level corporate oversight, including at the board of directors level, which must provide adequate funding of the program in proportion to the size of the company and the risk. Companies must identify and empower the relevant stakeholders and place overall control of data security in the hands of an individual or a small group of individuals.
- Companies must carefully select and scrutinize the individuals in charge of data security compliance. Not only must they not pose a risk for unethical behavior, they must be trained and certified with a cybersecurity expertise.
- Companies must have clear standards and procedures that are communicated effectively to the entire workforce.

Related People

- Daniel Goldberger
- Ray Liu Esq.

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

- Conduct must conduct periodic audits of the effectiveness of the data security compliance program.
- Companies must consistently enforce the policies and establish mechanisms for reporting violations

The law is broadly drafted, filled with ambiguities and creates significant potential uncertainties for companies doing business in China in terms of maintaining and protecting competitively sensitive and personal data. Going forward, the Chinese authorities will be interpreting and applying the many ambiguous and vague terms in the new regulations and implementing rules that will directly impact how companies conduct business in China. For businesses to grow in global markets like China, companies must support seamless mobility with the ability to conduct transactions on any device or platform in any country. It remains to be seen whether this law will enhance security of data in China and how difficult compliance may become.