KOBRE & KIM | DISPUTES AND INVESTIGATIONS

A New Opportunity to Avoid Cyberattacks From the U.S.

The New York Department of Financial Services (NYDFS) imposed regulations requiring companies to certify compliance with their cybersecurity. For Chinese companies looking to comply with these new regulations, a nuanced understanding of the NYDFS and on-the-ground support in China is essential.

January 30, 2019

Rising cyber security breaches place global companies at risk. New York, as a global center of finance, is a proven target of increased cyberattacks.

In response, the New York State Department of Financial Services (NYDFS) recently imposed new regulations requiring companies to certify compliance with their cybersecurity programs by February 15 of every year.

To prevent a breach, noncompliance or litigation, Chinese companies with U.S.-incorporated subsidies ought to ensure their programs comply with these new regulations, which will require a nuanced understanding of cybersecurity policies and of the operations of the NYDFS, as well as on-the-ground support in China.

Make Your Policies Careful and Complete

NYDFS will require companies to write cybersecurity policies that address the numerous threats to digital information, including physical security, access controls and electronic device management. Without pre-emptive guidelines, companies will remain vulnerable to data breaches or disruptions to information systems.

Bring in a Dedicated Expert

Companies also must ensure that someone takes responsibility for implementing policies. Whether an employee or third-party provider, the NYDFS requires that a qualified Chief Information Security Officer (CISO), implements and enforces cybersecurity policies. These designated officers must also provide at least annual reports regarding a company's cyberrisks, the effectiveness of its policies and cybersecurity incidents.

Check in Regularly

To ensure the effectiveness of their cybersecurity policies, NYDFS has also mandated that companies perform regular assessments to mitigate the impacts of cyberattacks. Systemic scans of IT infrastructure for publicly known vulnerabilities will help IT personnel assess the strength of companies' policies. It is also imperative to maintain protocols in case of threats become real, including plans to determine where and how a breach occurred, and designating decision-makers.

A New Opportunity

Companies can take the NYDFS's regulations as an opportunity to ensure that their IT policies and procedures can withstand and anticipate future cyberattack from the U.S.

For Chinese companies with U.S.-incorporated subsidies it will be critical to maintaining pre- and post-breach system integrity across jurisdictions, which will require both a nuanced understanding of the NYDFS and on-the-ground expertise in China.

About Kobre & Kim's Financial Products and Services Litigation Team

Kobre & Kim is a conflict-free Am Law 200 law firm focused on disputes and investigations, often involving fraud and misconduct.

Our financial products and services litigation team contains experts who regularly engage with U.S. regulatory agencies in the financial services industry, such as the New York Department of Financial Services. Often working in tandem with our Information and Cyber Security Services team, we offer a range of information security services to help manage pre and post-breach environments. Taking a holistic and strategic approach, our experienced team of professionals offers risk mitigation, investigation and security solutions across multiple industries.

KOBRE & KIM

Frequently working with other law firms as special counsel, Kobre & Kim regularly represents China-based clients in cross-border government enforcement actions. The firm’s broader Asia-based team is led by several former U.S. government lawyers who have served in relevant US agencies.