CORPORATE COMPLIANCE INSIGHTS
THE PREMIER GLOBAL NEWS SOURCE FOR COMPLIANCE, ETHICS, RISK & INFORMATION SECURITY

The China Syndrome: Competing Regimes Make Due Diligence a Tall Task

In the world's second-largest economy, corporate investigations are increasingly challenging, but be warned: Skipping out on due diligence is worse

by Bradley Dizik and Akiko Goldberg — August 16, 2023 in Financial Services

The U.S.-China relationship has never exactly been a great one — remember the spy balloon? But recent escalations on both sides of the divide have corporations with business interests in China caught in the middle. Guidepost Solutions' Bradley Dizik and Akiko Goldberg discuss the strain on due diligence investigators.

While reliable information from China has always come at a premium, recent restrictions on previously available business intelligence as well as Chinese enforcement actions against foreign investigative diligence firms are particularly concerning for corporations with businesses and investments in China.

Meanwhile, U.S. lawmakers, regulators and law enforcement are tightening their scrutiny of companies with interests in China more than in previous decades. Sanctions against Chinese individuals and entities, export and import controls on goods to and from China, including the extensive ban on goods from Xinjiang, money transfer license and anti-money laundering requirements, and FCPA are only a few recent examples.

Companies with business interests and investments in China are well advised to reinforce their compliance and risk management programs to account for these new challenges by conducting **effective diligence** in China and of Chinese individuals and companies.

'Comprehensive national security'

As noted by Chinese Communist Party (CCP) leader Xi Jinping's message to his top national security officials to think about the "worst case" scenarios and prepare for "stormy seas" at the party's National Security Commission at the end of May, the CCP has shown extraordinary willingness to sacrifice continuous economic growth for national security, even as the country's economy struggles to recover from its zero-Covid lockdown measures.

Xi's concept of "comprehensive national security" covers just about everything — politics, economics, culture, defense and **cyberspace**. His recent legal reform and enforcement efforts demonstrate his intention to restrict any information outflows perceived to be threatening to national security.

In April, China expanded its law against espionage beyond the illegal handling of "state secrets" to cover any "documents, data, materials or items related to national security and interests." This law, which took effect July 1, also provided search and seizure powers to state security agencies. This followed a data-security law passed last year giving the government more oversight of **cross-border data transfers**.

In China, legal language is often vague, and the newly expanded anti-espionage law is no exception. For example, the law does not define what falls under China's "national security and interests." The ambiguity not only makes it difficult to draw a clear line as to what is and is not permissible, but it also allows much room for arbitrary enforcement by Chinese authorities.

Even before the expansion of the anti-espionage law took effect in July, Chinese authorities raided the Beijing office of the Mintz Group, a New York-based investigative due diligence firm. This led to the detention of five Chinese nationals who worked for the company and subsequent closure of the company's Beijing and Hong Kong offices. In April, employees in the Shanghai office of U.S. consulting firm Bain & Co. were questioned by Chinese authorities. And in May, consulting firm Capvision, which was founded in China but is now partly based in the U.S., was raided by police in an action broadcast on a state-owned television channel.

Despite what appears to be targeted actions against these diligence consulting firms, for now, most due diligence work is continuing as usual, especially where it can be conducted

through open-source research, such as publicly available or proprietary databases, albeit with some noticeable apprehension around collection of information via human sources on the ground in China.

While it is impossible to determine what prompted the aforementioned raids and questioning, it does not take a stretch of imagination to see that any probe into politically sensitive areas deemed off-limits by China has become even more challenging as U.S.-China tensions continue to rise. Indeed, before the raid, Mintz Group had reportedly engaged in corporate due diligence work examining the possible use of forced labor in supply chains linked to the Xinjiang region.

In further restriction of foreign access to information, China also instructed its state-owned companies to shun U.S. big four auditors in favor of local and Hong Kong auditors. It has cut access to online sources, including decisions from court cases and procurement documents. More recently, a Chinese data provider, Wind Information, which has been widely relied upon by investors and analysts, began restricting overseas subscribers from accessing certain information including satellite images.

While Beijing's tightening control over business intelligence access is making it difficult for foreign corporations to conduct meaningful due diligence, Washington is creating more needs for it by reinforcing its sanctions and export and import control regimes, as well as FCPA and anti-money laundering enforcements.

For example, U.S. lawmakers are demanding tougher enforcement of the **Uyghur Forced Labor Prevention Act of 2021** that blocked many imports from Xinjiang. In addition to Washington's restrictions on high-end chip exports to China, the number of Chinese companies under its export controls has been rapidly increasing.

Even if a company's products and supply chain partners are not subject to these regimes, its subsidiaries and distribution channel's conduct may still be found in violation of U.S. laws. In May, Netherlands-based medical device company Koninklijke Philips N.V. agreed to pay the SEC $62 million for alleged FCPA violations by its Chinese subsidiaries, distributors and sub-dealers. FinCEN and state regulators are shoring up AML scrutiny over cryptocurrency exchanges and money transfer licenses particularly as they relate to China. And most recently, President Joe Biden issued an **executive order** banning new U.S. venture capital and private equity investment in semiconductors, microelectronics, quantum computers and some AI applications.

Despite these developments, few compliance professionals are confident in their organizations' compliance and risk management strategies in China. While conventional wisdom may suggest mitigation of non-financial risks is in conflict with maximizing profits,

recent legislative and enforcement trends indicate otherwise. By creating concrete consequences to previously somewhat abstract concepts like forced labor and strictly enforcing sanctions and anti-corruption regimes, Washington has clearly raised the stakes of a corporation's noncompliance with its political and national security agenda, especially as it relates to China.

In light of the increasingly murky business environment in China for U.S. and other foreign companies and individuals, combined with increasingly tougher U.S. enforcement in relation to China, companies must closely scrutinize their compliance practices and reinforce their policies, programs and oversight.

They must ensure partners and agents in their supply chains, distributors and sales agents, and trading, joint venture and M&A counterparts both in and outside China are aware of, trained on and strictly adherent to all company policies based on updated laws and regulations. In addition, companies should take note that Chinese laws and regulations are often vague and applied inconsistently; their risk mitigation strategies should allow for flexibility and agility.

Finally, even under a challenging and at times hostile information gathering environment in China, companies must not neglect conducting sufficient due diligence on their counterparts and on their own internal entities, employees and executives. Open-source intelligence remains a powerful tool for companies to protect themselves from potential U.S. enforcement with increasingly serious legal, pecuniary and reputational consequences.

Bradley Dizik and Akiko Goldberg

Bradley Dizik is executive vice president, emerging issues and technology at Guidepost Solutions, a security and investigations firm. He is a member of the Washington D.C. and New York bars and is regularly called on to advise board directors and executive officers in response to their most public and private crises.

Akiko Goldberg is a managing director at Guidepost Solutions. She is a multilingual attorney with over 14 years of experience managing complex multijurisdictional and cross-border investigations and litigation.

Originally published by *Corporate Compliance Insights* – Republished with permission