—EMBARGOED—
UNTIL
FEBRUARY 5, 2018 11:30 AM (Beijing)
FEBRUARY 4, 2018 10:30 PM (DC)

THE US-CHINA BUSINESS COUNCIL
美 中 贸 易 全 国 委 员 会

OPTIMIZING CONNECTIVITY: Updated Recommendations to Improve China's Information Technology Environment

February 2018

Since China's Cybersecurity Law came into effect in June of 2017, the government has implemented a series of cybersecurity regulations with wide-ranging consequences for foreign and domestic companies operating in China.

Eighty-two percent of US-China Business Council (USCBC) members are concerned about China's approach to information flows and technology security, as reported in USCBC's 2017 member survey. This is largely due to the impact these new cybersecurity policies have on companies' ability to conduct day-to-day business. Chinese policies concerning investment, data export, product security reviews and critical information infrastructure affect the operations of both foreign and domestic companies in ways unseen in other markets. These policies constrain companies' use of global best practices, and limit their ability to employ technology solutions that combine operational efficiency with globally-proven technological safeguards. These policies also make it difficult for companies to exchange information used to combat security threats, creating conditions that make both consumers and businesses less safe.

USCBC has developed recommendations aimed at addressing the specific obstacles companies face when using information technology in China. These recommendations are based on extensive interviews with company technology officers and provide potential solutions that balance operational and security needs. They are meant to constructively address the concerns of the Chinese government and enterprises in a practical manner. USCBC appreciates the chance to put forward these recommendations and would welcome the opportunity to discuss them further with Chinese regulators.

Challenge 1: DATA FLOWS AND LOCALIZATION

China's data policies disrupt communications between a company's China facilities and its other global operations; stifle cross-border innovation; and increase costs by requiring the installation of duplicative IT infrastructure. These policies also affect the implementation of China's development plans such as Internet+ and the National Big Data Strategy. These restrictions impact foreign and domestic Chinese companies' ability to operate global platforms, carry out ecommerce, and perform cutting edge research and development (R&D) in China.

During interviews with USCBC, technology executives said that China's policies on data flows and localization make it difficult to use big data analytics. This affects product support, security, and innovation. For example:

- Energy companies that operate wind turbines in China need their fleets to be in constant communication with global headquarters, so their global teams can respond to power outages and prevent accidents.

- Companies that provide high-tech, internet-connected equipment used in "smart manufacturing" facilities require access to data from their devices so that they can remotely maintain or repair them.
- Companies that sell industrial vehicles for infrastructure development need to access telemetric and performance data to provide their customers with machine performance and preventative maintenance information.
- Financial services companies analyze data across borders to predict consumer trends, provide targeted services to customers, and identify potentially illegal transactions.

Overly restrictive data regimes impede these and other essential operations, hurting both businesses and the customers they serve.

The goal of data flow regulations is, in many cases, to safeguard the security of citizens' personal information and other important data. In practice, however, regulations mandating data localization or security review for cross-border flows or requiring the use of domestic technologies do little to achieve that goal. The strongest international standards to protect data privacy are determined by industry consensus, draw on global best practices, and are largely blind to where data is stored or transferred. Cybersecurity experts agree that cyberattacks most commonly result from inadequately protected systems, engineering errors, and carelessness on the part of users. Limiting choice only to service providers with infrastructure in China instead of those with proven privacy and security practices globally creates circumstances in which the security of personal information and important data is ultimately more likely to be undermined.

The inability to link global and China-based networks also creates security risks. Local software or local vendors may be unable to troubleshoot or communicate problems that come up in the use of global technology. When maintenance issues, technical problems, or criminal infiltration of networks occurs, a fractured global communications network limits companies' ability to rapidly respond.

Ensuring the free flow of data across borders is an essential part of an innovative digital economy, the development of which China has made a priority. Initiatives like the 13th Five-Year Plan, Made in China 2025, and Internet+ emphasize the development of smart and internet-based technology. Senior Chinese officials regularly emphasize the importance of an open and interconnected internet both within China and under the G20 framework.

To foster this openness and ensure data security, China should look to the best practices and expertise offered by international companies and developed through global standards setting processes, which integrate traditional business practices with global information networks. Allowing certain information to be globally accessed by companies, support teams, and interactive products is a key component of "smart technology" — a goal of the 13th Five-Year Plan — and is necessary for successful high-level policy plans across sectors, such as Internet+, the Big Data Promotion Plan, and development plans for greater energy efficiency via smart cities or China's financial industry.

Recommendations

- China should use a very narrow definition of national security and "state secrets" to ensure that companies do not unintentionally violate regulations regarding the storage and transfer of such information. This definition should be limited in scope to only include information that has direct bearing on national security.

© 2018, The US-China Business Council

- China should clarify that only original personal information and "important data" must be localized in China. China should also allow copies of data to be sent abroad for analysis and processing to ensure operational efficiency and encourage big data innovation. This would preserve territorial jurisdiction over the data while still allowing important business functions to be conducted. China should also clarify and affirm that only personal information and important data collected by CII operators is subject to data localization and data export security review. Network operators should be exempt from these requirements.

- China should affirm that "implied consent" is a sufficient standard for outbound data transfer. Requiring explicit personal consent before information can be transmitted across borders imposes significant regulatory burdens on Chinese and foreign companies that operate or communicate internationally. Data subjects are implicitly aware that their information might be utilized when they participate in ecommerce markets, subscribe to financial services, or generally engage in online activity. Formally recognizing the "implied consent" standard will eliminate duplication with existing data protection measures and ensure industry can be in full compliance with China's policies.

- Chinese policymakers should, in consultation with international industry, develop and implement policy based on global best practices for secure data management and regulatory transparency, pursuant to China's international commitments obligations to maintain regulatory transparency. China's bilateral and multilateral cyber dialogues with other governments should expand beyond cyber-crime to include discussion with industry stakeholders that can speak to the operating challenges posed by emerging cyber threats and evolving regulatory concerns. In addition, China should engage in bilateral and multilateral discussions regarding information exchange mechanisms for related to law enforcement efforts to ensure the resolution of international jurisdictional issues.

- China should become a party to the APEC Cross Border Privacy Rules System (CBPRS), which was developed to build consumer, business, and regulator trust in cross border flows of personal information. We also recommend that compliance with the APEC CBPR system be recognized as a basis for transfer of data out of China.

- China should publish a clear system of appeals for decisions in data export security review processes. China should also clarify if CAC's role is limited to coordination and guidance or if its authority extends to overruling the decisions made by relevant industry departments and regulatory authorities. We recommend the State Council CAC clarify whether the relationships and respective responsibilities of competent industry departments, regulatory authorities, and CAC are hierarchical, and how it will process review appeals. China should limit the frequency of mandatory data export security review audits to ease the disruptive administrative burden on industry stakeholders. We recommend that mandatory reviews occur once every three years to ease the administrative burden on industry stakeholders and regulators. China should eliminate requirements for industry stakeholders to justify that a country or region is sufficiently secure to protect transferred data. This is a process better managed by governments and goes far beyond the capabilities of industry.

Challenge 2: MARKET ACCESS AND GLOBAL SOLUTIONS

Chinese and foreign companies are unable to use many innovative cloud computing solutions in China due to China's overly restrictive licensing regime. These policies complicate the cost, efficiency, and information security considerations for both foreign and domestic company operations in China.

© 2018, The US-China Business Council

For example, the 2015 Telecommunications Services Catalogue released by the Ministry of Industry and Information Technology (MIIT) set licensing requirements for basic telecommunications services (BTS) and value-added telecommunications services (VATS) for foreign and Chinese companies. While the Catalogue does not use the term "cloud computing," it does cover elements of cloud computing as part of VATS, an approach not used in other markets. Consequently, to provide cloud solutions in China, companies must obtain three different certifications -- Internet Data Center (IDC), Internet Service Provider (ISP), and sometimes Internet Content Provider (ICP) licenses. Foreign companies are required to have partnerships with local players to obtain these licenses. While foreign companies may control up to 50 percent of such operations, some international companies have been unable to apply for or receive any of these licenses. Therefore, many foreign cloud services are unavailable in China, forcing Chinese and foreign companies that use them outside of China to use different systems for their China operations.

Companies that purchase global cloud products and services have reasonable expectations of using them wherever they do business — one of the core purposes and benefits of cloud-based solutions. This affects the efficient communication between China-based and international teams, which in turn affects the use of cloud-based client-relationship management (CRM) software; the sharing of business documents between internal teams and with external clients; and the application of cloud technology used for hosting data and providing development platforms for R&D purposes.

While there are a number of local Chinese cloud solutions available, few of these solutions have a global presence, creating a similar impediment to the use of Chinese cloud technology around the world that China's policies create for the use of global cloud products in China. Consequently, China's policies may create significant players in its domestic market, but fail to create global technology leaders – something competition with global industry leaders at home would remedy.

Ultimately, these restrictions run contrary to the goals of policies such as Internet+ and the 13th Five-Year Plan, which seek to capitalize on cloud computing to upgrade China's economy, allowing other markets instead to benefit from the efficiencies and security of global IT networks.

Recommendations

- China should allow both foreign and domestic companies to provide cloud computing services. Specifically, we recommend MIIT re-evaluate China's regulatory approach to cloud computing, using international approaches that generally categorize cloud computing as a computer service rather than a value-added telecommunications service (VATS). Such a change would align China's approach with international best practices.

- As long as cloud computing services are defined as a VATS under the 2015 MIIT Telecom Services Catalogue, Chinese regulators should issue Internet Content Provider (ICP) licenses and Internet Data Center (IDC) licenses to wholly-foreign owned enterprises (WFOEs) and Sino-Foreign JVs seeking to offer cloud computing services in China. We also recommend that the foreign investor in a JV be permitted to retain ownership and control of software and other proprietary technology licensed to the JV or partner, to ensure the proper protection of intellectual property and incentivize the use of the best technologies in China.

- China should enhance transparency within the IDC, ISP, and ICP licensing approval process so foreign companies can proactively work with regulators to address concerns about risks and security requirements.

© 2018, The US-China Business Council

- China should allow industry stakeholders to utilize legally registered virtual private network (VPN) services to maintain unfettered access to the global internet for legitimate business purposes. In VPN registration processes, China should require only accounting for the number of users of the VPN and not require the specific personal information of users of the service.

- As products move to solutions that provide information via the internet directly to customers, such as onboard display systems in vehicles, China should provide clear definitions of the types of services that qualify as internet content providers (ICPs).

Challenge 3: Secure and Controllable Technology & Overly Broad Cybersecurity Review Regimes

Companies use global technology systems to ensure the highest level of security possible for their customers to protect their data, including personally identifiable information (PII), from misuse or theft. To that end, policies mandating the adoption or use of unique "secure and controllable" technologies may in fact be detrimental to security goals.

USCBC companies report that local procurement tenders for IT products still call for the use of "secure and controllable" technology, and are implemented in a way that gives preference to local products over foreign technology based solely on nationality, rather than on technical assessment.

USCBC and our members appreciate that CAC has clarified that both foreign and domestic technology can qualify as "secure and controllable" technology, and we hope these principles are rigorously implemented as products and services undergo security review.

Over the past several years, China has implemented cybersecurity review regimes for ICT products without releasing necessary details on testing guidelines, product scopes, required documentation, timelines, or other licensing procedures. Consequently, it is unclear how these regimes will interact with existing review assessments such as the multi-level protection scheme (MLPS), other non-public review mechanisms, or the cybersecurity review mechanisms outlined in the Cybersecurity Law.

Additionally, some draft and enacted regulations have called for the use of local encryption algorithms, an approach that is inconsistent with global best practices and creates security concerns. Multinational firms use international encryption standards, tested extensively by international experts for security vulnerabilities, to minimize problems and ensure client data is well-protected— something financial industry regulations in particular require. Adopting different encryption standards for Chinese and global networks, which may be incompatible with each other, could create vulnerabilities in China-specific networks. These risks work against China's overall goal of enhanced IT security and would hamper Chinese companies from becoming global players that sell into the world's largest markets.

Ultimately, the use of technology systems unique to China will limit the ability of companies to apply global solutions and best practices within China to the benefit of Chinese consumers. Furthermore, local sourcing mandates may mean the use of equipment that is incompatible or inferior to the security standards companies set for their global operations. Decisions to contract IT globally or locally should be determined by company risk assessment needs rather than government directives that may inhibit companies from optimizing their security.

Recommendations

© 2018, The US-China Business Council

- The Cyberspace Administration of China (CAC) should ensure that "secure and controllable" technology requirements, when implemented, are non-discriminatory and will not require or give preference to the procurement or use of Chinese-origin products, technologies, intellectual property, or standards. If a network product or service security review is required to qualify as a "secure and controllable" product, the scope of qualified products should be narrowly tailored to products and services which—if compromised—pose a specific and substantiated risk to national security. Technology users not designated as CII operators should be fully exempt from requirements to procure secure and controllable technologies.

- China should streamline its cybersecurity review mechanisms into a single, clear regime that sets narrow parameters for the types of products under the scope of its review, and provide details on licensing requirements, timelines, testing procedures, and other information to facilitate company compliance. This regime should be transparent and formulated in consultation with international industry to ensure that China will benefit from the experience of existing security review mechanisms already utilized in other markets. Any cybersecurity review regime should also clarify its interaction with existing security mechanisms, such as MLPS. This would ensure more efficient processes, reduce business costs, and reduce international concerns regarding the potential for discrimination in such procedures.

- China should prohibit potential conflicts of interest and continue to enhance trade secret protection mechanisms in cybersecurity review processes which include third-party experts. CAC should also establish rules prohibiting posting experts with clear conflicts of interest to applicants' expert panels and requiring those with a conflict of interest be removed. China should also institute a formal process for applicants to dispute expert panel nominations where conflicts of interest exist. This process should include a public timeline for consideration, review, and resolution of the dispute to minimize disruptions in the investment process. To aid in that process, we also recommend companies undergoing cybersecurity review be allowed to provide input on expert panel nominations. To that end, CAC should provide updated and complete lists of approved experts to companies and allow them to nominate a certain number of experts to the panel. Finally, CAC should require experts to support information requests with substantiated facts, commercial experience, and sound science.

- China should allow companies to use single, global technology platforms and to procure IT solutions and products that best fit their corporate and security needs, based on considerations such as global network integration, risk-based cybersecurity frameworks, and global security standards based on industry consensus practices.

- China should consult with foreign companies and industry associations as it continues to draft technology security standards to ensure that global best practices are being incorporated to integrate Chinese and global IT security regimes. Draft standards on technology security should not contain mandates for the disclosure of source code, use of local encryption standards, mandate secure and controllable or indigenous innovation, or otherwise impose other burdens that would compromise intellectual property usage and protection.

- China should require that draft standards on technology security reflect its commitments at the 2015 Joint Commission on Commerce and Trade and the 2016 Strategic and Economic Dialogue that technology security should not inherently be linked to product nationality, and should be ascertained via technological assessment of security functions and processes.

© 2018, The US-China Business Council

- The State Council should require that all new technical standards undergo a minimum 60-day comment period with no mandates for domestic preference.

© 2018, The US-China Business Council