Technology Security and IT in China: Benchmarking and Best Practices

July 2016

Executive Summary

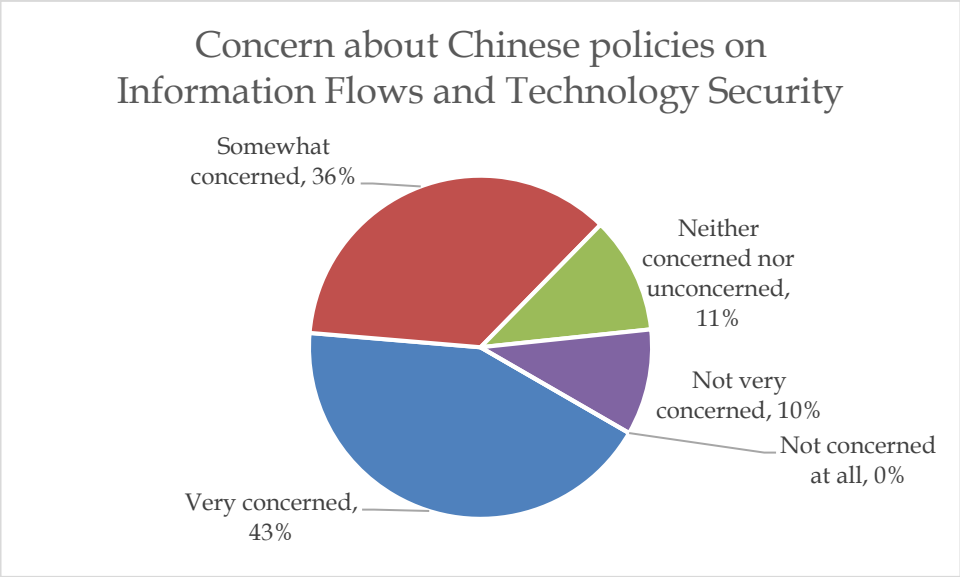
- Developments in information technology offer companies new channels for growth and innovation around the world. Though global policymakers implement a variety of regulatory methods for managing technological advances, China's regulatory framework restricts international companies in ways not seen in other markets.
- China's regulatory framework affects vendors of information and communications technology (ICT) products and services as well as companies that use digital information in sectors including aviation, finance, healthcare, manufacturing, and consumer goods. Technology security, cross-border data flows, and data privacy are top concerns as companies seek to develop internet- and information-based solutions for their traditional business models.
- Although Chinese policymakers are developing a better understanding of how to use technology to upgrade and enhance the economy, security objectives are outweighing a more pragmatic approach that would incorporate the best international products and services available. The Chinese government is promoting use of "indigenous," or domestic, information technology (IT) products, which are ambiguously defined as "secure and controllable" technology, and discouraging the use of foreign products and technologies.
- Chinese development plans such as Made in China 2025, Internet+, and the 13th Five-Year Plan emphasize the development of smart- and internet-based technology, which carry an implicit recognition of the benefits of global information networks. But formal regulations in the financial and healthcare sectors, as well as standards related to cloud computing, prohibit the flow of certain data across China's borders, thereby limiting the effectiveness of national development plans.
- The role of the Chief Information Officer (CIO) in China has expanded beyond maintaining basic IT operations to encompass digital strategy. This new scope requires traditional technical skills and knowledge of the policy environment. The rapidly changing environment requires CIOs to have a grasp of policies and regulations that can affect their everyday work. This understanding is vital in communicating to headquarters which technology solutions can and cannot be implemented in the China market.
- To better understand the challenges facing foreign companies under China's IT regulatory framework, the US-China Business Council (USCBC), in cooperation with the China CIO Alliance (CCA), interviewed CIOs, chief technology officers, and China or regional IT directors from more than 40 multinational companies. This report seeks to illuminate China-specific technology policy concerns and best practices faced by companies with manufacturing, retail, and services operations in the China market.

Introduction

Developments in information technology (IT) present companies with new channels for growth and innovation around the world, and few markets have greater potential for growth or innovation than China. Applications for big data are proliferating in services ranging from mobile payments to cloud computing and smart devices. As China transitions to consumer-driven growth, the country is primed to harness these technologies and position itself at the cutting edge of the tech frontier.

These technological advances are bringing to the forefront questions about how best to balance information flows, personal privacy, and national security. The Chinese government is placing an emphasis on national security, and is pursuing increasing control over digital information, data flows, and IT infrastructure procurement. This approach fundamentally shapes the market environment for all players—consumers, companies, and government regulators—in China. Just as China is a central arena for global technological innovation and development, so is it also a center of debate over the degree to which information technology and data should be regulated.

Perhaps no one is more attuned to this debate than foreign businesses operating in China. In the global marketplace, the rules of the road in key markets affect operations everywhere, and China's market dominance means companies may be beholden to China's regulatory developments even when conducting operations far beyond its borders. In a 2015 survey of member companies, the US-China Business Council (USCBC) identified information flows and technology security as top challenges facing companies in the China market. Again in 2016, companies expressed concerns about cross-border data flow restrictions, data localization requirements, mandatory use of unique Chinese technology standards, and the uncertainty over the use of corporate virtual private networks (VPNs).



Source: USCBC 2016 Member Company Survey Results

Technology plays an unprecedented role in the 21st century digital economy. More than ever, businesses' value chains depend on reliable IT infrastructure and information flow. Just as technology is constantly evolving, so too is the global regulatory and policy environment that governs it. Nimble adaptation is both a necessity and a particular challenge for companies with value chains that are complex and globally interconnected. As the Chinese market integrates into the global IT

environment, China's economic and security prerogatives pose sweeping repercussions for global IT infrastructure and the delivery of information. It is essential that companies take China's unique regulatory regime into account as they deploy new technologies or expand operations.

To shed light on policy concerns and operational best practices in China's IT regulatory framework, USCBC in cooperation with the China CIO Alliance (CCA), interviewed chief information officers (CIOs), chief technology officers, and China or regional IT directors of more than 40 multinational companies in sectors including industrial equipment, chemical manufacturing, healthcare, automotive, financial services, retail, and other services.

Our findings illustrate the numerous operational challenges that China's data/IT regulatory environment creates for companies across sectors, as well as the solutions they employ to keep their businesses running smoothly.

Data Regulatory Policies

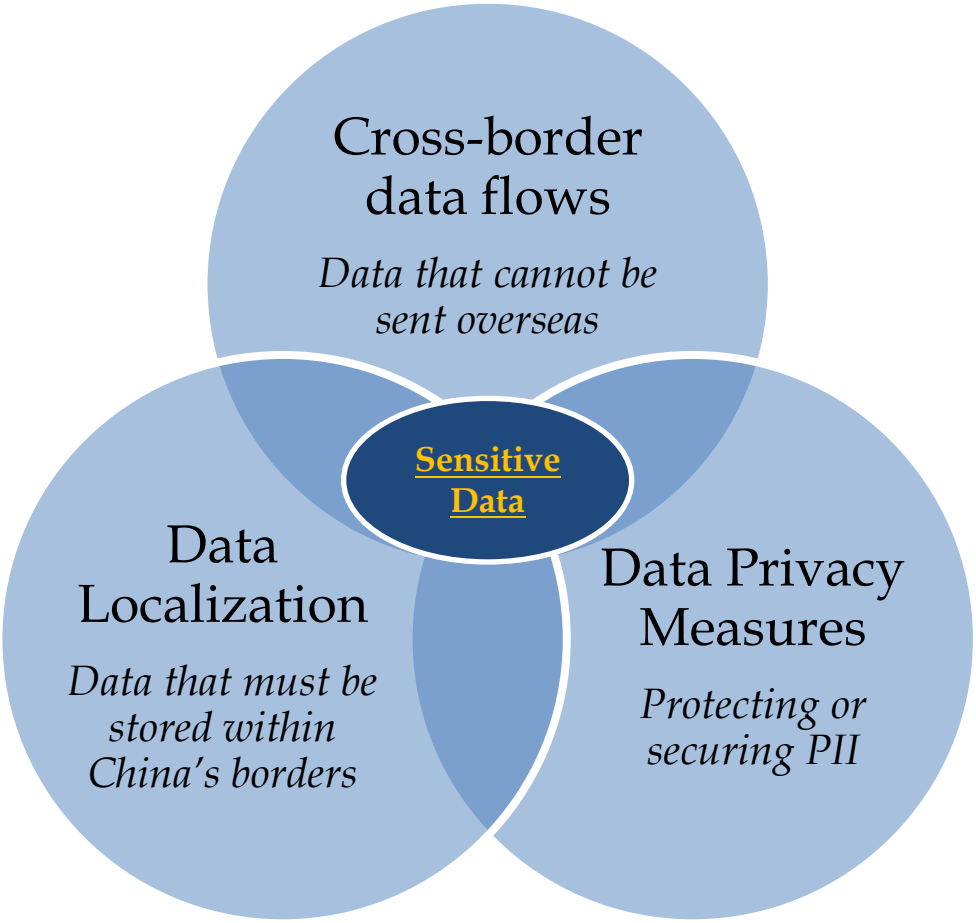
Big data—the harnessing of large sets of data to understand trends, patterns, and other useful information—allows companies to map out new customer segments, engage in targeted advertising, analyze key business trends, and provide customized services on a wide scale. Chinese leadership has aggressively promoted the use of big data to transform traditional industries.

But Chinese government agencies continue to promulgate policies that inhibit the use of big data, whether by mandating that certain data be stored within China's borders, prohibiting certain data from flowing overseas, or barring companies from analyzing data in ways commonly used in other markets. This policy environment creates compliance challenges for companies looking to use data to advance, expand, or otherwise enhance their China operations.

Existing literature on data regulation frequently confuses the concepts of data localization, data privacy, and cross-border data flows. A proper understanding of the Chinese regulatory framework requires a clear definition of these three policy terms:

- **Data localization** Data localization policies—also known as data residency—are geographic in nature, and stipulate that data must be stored within geographic boundaries. However, policies that require data localization may not automatically restrict data from leaving specified geographic boundaries, separating the concept from "cross-border data flows." Data localization policies can require companies to build location-specific infrastructure to store data, impacting company costs and strategic considerations.

  For example, the China Insurance Regulatory Commission (CIRC) released a notice in 2004, subsequently updated in 2011, governing the storage of data handled by insurance companies operating in China. The policy mandates that insurance company data, financial data, and other kinds of "important" data must be stored within mainland China—but there are no requirements prohibiting this same data from leaving China's shores.



- **Data privacy** Data privacy regulations aim to secure personal identifiable information (PII), and prevent its illegal sale or transfer. In some jurisdictions, such as the European Union (EU), data privacy laws forbid the transfer of information to any third party. Many data privacy regulations—such as those in the United States and in China—do not have a geographic restriction, separating this concept from "cross-border data flows."

  A China-specific example of data privacy can be found in the ninth amendment of the Criminal Law. The 2015 update forbids the sale or illegal provision of personal information to third parties without the consent of the individual in question. While this provision may include the transfer of data between in-country and overseas entities, it does not specifically distinguish between domestic-domestic transactions and domestic-international transactions.

- **Cross-border data flow** Cross-border data flow refers to the transmission of data overseas and across political borders. Data flow laws often overlap with data localization policies, mandating specific geographical data residency as well as prohibiting the flow of information overseas. These are the most restrictive geographic data regulatory measures and present the most pressing challenges for companies with global networks requiring instant communication.

A China-specific example of cross-border data flow restrictions is the Notice to Financial Institutions on Protecting Personal Financial Information issued by the People's Bank of China (PBOC) in January 2011. This regulation mandates that personal financial information of Chinese citizens be stored within China's borders and prohibits the flow of this information overseas.

Company case study: Data localization in the internet industry

Data localization requirements have existed in China for years.

In order to operate a website in China, companies are required to obtain an Internet Content Provider (ICP) filing or license. ICP filings, which are relatively simple to obtain for foreign companies and only require notification with relevant authorities, are necessary for "nonprofit" websites, such as company websites. ICP licenses, which are more difficult to obtain for foreign companies and require a more complex application process, are necessary for "profit generating" websites, such as ecommerce sites or sites that rely on advertising revenue. ICPs are governed by the Ministry of Industry and Information Technology (MIIT), and are outlined in separate regulations on telecommunications and internet information services.

Companies note that in conversations with Chinese officials, obtaining an ICP filing or license requires hosting websites on servers located within mainland China. This requirement serves as a de-facto localization policy—although there are no requirements to prevent certain data from leaving China's borders.

The common denominator among these three terms is the fact that they all regulate "sensitive data," a loosely-defined concept often left up to situationally-based interpretation by central or local authorities. Despite numerous policies focused on protecting PII, for example, only in early 2015 did the State Administration for Industry and Commerce (SAIC) define the term. Information including consumer names, genders, occupations, date of birth, national identity number, health status, and consumption habits, etc. is considered PII under the SAIC definition. Companies note that the "etc." at the end of the provision renders the breadth of the definition of PII open to interpretation. This linguistic ambiguity is not uncommon in Chinese regulations and results in a hazy compliance environment in which Chinese policies are functionally more restrictive than the international norm, whether or not they are intended to be.

Such vagaries are particularly problematic where there is potential overlap between commercial and criminal codes. The SAIC definition of PII, for example, also includes "personal consumption habits," data often collected by companies for targeted advertising and consumer analytic purposes. China's Criminal Law, meanwhile, prohibits illegally selling or providing information to third parties. Absent clarification as to when and whether the Criminal Law's prohibitions apply to "personal consumption habits" data, companies face not just civil compliance risks but also uncertainty as to whether practices they commonly employ in the global marketplace will expose them to criminal liability in China.

Existing Data Flow Restrictions

Despite a surge of recent attention, China has a long-established data regulatory regime.

A chart mapping the existing China data localization and data flow policies can be found in Appendix I. While the majority of these regulations are concentrated in sectors such as banking,

healthcare, insurance, and the internet, companies from a wide range of industries, including energy, aviation, and cloud computing, report challenges moving data across the borders of mainland China. Several companies note that many of these restrictions have existed for years.

The debate on how to regulate data in China is ongoing. Restrictive data policies stand in stark contrast to a flurry of centrally developed policies, such as Made in China 2025, the Three-Year Action Plan for Internet+, and the 13th Five-Year Plan. These policies all seek to leverage big data and "smart technology"—or devices that actively create data to provide services, ranging from sensors that can predict pollution patterns to watches that can function as payment platforms—to promote economic growth.

When the PBOC published restrictions on cross-border flows of personal financial information in 2011, it prompted questions as to how China could meet service industry goals while restricting basic information requirements. This concern was particularly acute in the case of Shanghai, a city the government hopes to develop into a "global financial center" by 2020. To offset these contradictions, the Shanghai branch of the PBOC published follow-up regulations exempting Shanghai-based branches of foreign banks from restrictions on cross-border data flows as long as explicit consumer consent was obtained to send the information overseas. Banking companies report that this workaround has allowed them to maintain communication between their Shanghai-based branches and global operations, but the PBOC notice remains in effect for all of their other China branches.

In addition to formal policies like the PBOC's, companies also report that they are subject to informal requirements or instructions from Chinese regulators to keep certain data within Chinese borders, or to prohibit certain data from leaving China's shores. Companies operating in the aviation and auto sectors note that GPS or terrain data cannot leave China's borders. While USCBC identified one policy published by the Ministry of Land Resources in late 2015, which mandates that mapping data be stored on servers located within China, it seems clear that companies are subject to other, less publicly available regulations. Several interviewees reported that mapping data restrictions were communicated verbally to them by regulators, without reference to a specific policy or legal basis. How China will reconcile its goals of harnessing the power of big data while encouraging or allowing sections of its economy to be isolated from the global information ecosystem, is a matter of ongoing concern for multinational companies looking to apply their global data solutions to the China market.

Company case study: Unwritten data residency requirements

Company A, a consumer-facing company, used international servers based outside of China to host its company website. Company A partnered with one of China's telecommunications giants to use acceleration services—services used to increase the access speed for China-based consumers accessing websites hosted offshore—because accessing the website from the Chinese mainland without these services is often slow or unstable.

Company A says that several years ago, MIIT released an internal directive to the major telecommunications firms prohibiting them from providing these acceleration services for offshore websites or websites without an ICP filing. Because Company A could no longer rely on acceleration services to offset the negative experience faced by Chinese consumers navigating its website domestically, the company was forced to register its website in China and use domestic servers to qualify for the ICP filing, effectively localizing its data. While the costs were minimal and the licensing process relatively straightforward, Company A noted that the government never officially communicated this ruling to its team, either verbally or through a direct policy; instead, their telecommunications provider informed them that acceleration services would be halted. If Company A wished to ensure the quality and speed of service for accessing its website, it would have to move its servers onshore.

Disparate Regulatory Enforcement Challenges

Restrictive data policies have a range of effects on company operations. Current data localization requirements force companies to use infrastructure located within the borders of mainland China for data hosting and storage. This requires companies to source local vendors that can provide a similar quality of service as their contractors used in other markets, although companies note that such strategic decisions should be left to their own discretion— such as whether suitable local partners or technology exists in the market for them to host their data securely. In addition, because localization requirements may often be used to ensure jurisdictional authority, companies are hesitant to move sensitive data into China out of concern that this might jeopardize consumer or company privacy.

Companies in industries burdened with data flow restrictions report that, in addition to increasing infrastructure and local vendor costs, these restrictions can disrupt global communication structures. This impacts the application of analytical and processing services on data collected in China. It also limits global research and development (R&D) teams from sharing crucial information for product development, and undermines processes that require constant communication with devices in other markets— such as security systems that can notify an American user of credit card or identity theft in China. In order to comply with Chinese regulations, companies may be forced to maintain separate China-based data-hosting systems connected to global monitoring networks. In practice, this frequently means that companies have to create two networks—one for China and one for the rest of the world.

Foreign companies also hesitate to bring their innovative data—or information-based solutions—to the China market because of legal concerns. Several companies spoke of reticence in pioneering data-based solutions—such as in finance, healthcare, or other sectors with existing restrictive policies—due to uncertainty as to whether these projects could be legally carried out in China. One particularly important question centers around "state secrets," a vaguely-defined concept that companies note may cover a variety of economic data, such as details on China's grain reserves (important for agriculture companies) or geologic formations (important for companies engaged in resource extraction). Sending information that could be deemed a "state secret" overseas puts companies at risk of serious criminal liability. This

lack of clarity prevents companies from developing reliable compliance mechanisms, a serious deterrent for enterprises that want to bring innovative technology to China.

Company case study: Product support challenges with data restrictions

Company B uses data collected from its industrial machinery in order to provide preventative maintenance services to its clients. The data collected in China is sent to a global analysis center, where it is used to identify trends useful for preventing, responding to, and proactively resolving risks, such as unplanned power outages or equipment failures.

The company highlighted a National Development and Reform Commission (NDRC) policy on cyber and network security in the power industry, which creates different "zones" dedicated to information management. This policy includes provisions which mandate that independent network devices—devices that are not connected to the company's global network—be used in some of these zones, while also prohibiting the flow of data from one zone to another.

Company B notes that this policy has created challenges for their global maintenance structure, because they rely on their global processing centers to identify trends to support their equipment. Due to these restrictions, the company is unable to employ its best monitoring and support practices for its China-based fleet.

Companies must handle issues of performance by taking additional steps to ensure connectivity and IT security between China-based and global networks. Company CIOs noted challenges in finding local IT solutions or support networks that are compatible with global communication and security architecture, which are often designed by company headquarters and based in their home markets. IT support staff in headquarters may not be familiar with China-based IT vendors or IT equipment, which may limit their ability to incorporate China operations into their global network. These challenges are often exacerbated by language barriers, different IT support practices, or even inability to identify the correct local partners to engage on IT issues. This dissonance between China-specific and global regimes may create IT security vulnerabilities specifically for data that has been collected in China, and is a constant concern for companies looking to mitigate security breaches or other risks.

The development of a data-regulatory regime

While Chinese regulators are constantly deliberating new policies to manage data, USCBC identified three draft regulations that are particularly relevant to foreign companies in China.

- **Draft Cybersecurity Law** Released for comment July 6, 2015, Article 31 of this draft mandates that "personal information and other kinds of important information" must remain within Chinese borders, with this data permitted to leave China's shores only after a security assessment. However, the draft law does not define what a security assessment would entail. China released this law for a second round of public comment in July 2016, and discussions with policymakers, industry associations, think tanks, and companies indicate that this law may be finalized sometime before the end of 2016.
- **Draft Insurance Information Management Regulations** Released for comment October 9, 2015, CIRC's draft Insurance Information Management Regulations contain language mandating that data centers be located within the Chinese mainland, a localization policy that has existed in this industry for several years. However, Article 58 introduces restrictions on cross-border data flows, saying that any flow of data overseas must be done in accordance with relevant Chinese regulations, without specifying the content or identity of such

regulations. Without clarification, companies face compliance burdens that may discourage cross-border transfers of data. China has recently filed notification of these draft regulations to the World Trade Organization Technical Barriers to Trade for review, suggesting that implementation may soon follow.

- **Draft E-Commerce Law** While not yet public, industry and government stakeholders have noted to USCBC that the draft Ecommerce law may contain provisions mandating the local storage of Chinese consumer data onshore. Companies have previously reported de-facto challenges or requirements in this area, but the pending ecommerce law could codify such requirements for the first time.

Conversations with industry and Chinese government think tanks indicate China benchmarks against international data regulatory developments to inform its own approach to information security and compliance. One think tank specifically noted the importance of regulatory developments in the EU, which pushed for strong data privacy controls following the replacement of the "Safe Harbor pact" by the EU-US Privacy Shield agreement. While these discussions center on data privacy, they have data localization and cross-border flow components, based on the idea that non-European countries may not have as robust data privacy regulations, and thus information on European citizens should not flow to those jurisdictions.

How these developments play out may be a crucial sign to Chinese policymakers in constructing a domestic data management regime.

How can companies cope?

Companies adopt the following strategies to mitigate policy uncertainty:

- **Track data regulatory policy** Companies note the importance of monitoring draft laws that include data requirements to ensure compliance and proactively identify future regulatory trends. For example, one company noted that its China IT and legal compliance teams have established a data compliance task force that specifically tracks and analyzes the potential impact of regulations with consumer privacy requirements. These teams are becoming increasingly important for non-ICT companies, particularly as more and more companies incorporate internet or data-based technology into their businesses.

- **Proactively engage with data and cyber-regulatory bodies** Companies note the importance of proactively engaging with government agencies. While MIIT and the Cyberspace Administration of China may remain important interlocutors, information, data, and tech security are a major focus for a variety of Chinese government stakeholders. Identifying the regulatory agencies in charge of governing digital operations in a particular sector is important for ensuring compliance.

- **Consider moving *copies* of data overseas** Several companies spoke of moving copies of data overseas while keeping original data within the borders of mainland China, or vice versa. An important component of data localization and prohibitions on cross-border flows is legal jurisdiction: government agencies want to maintain legal authority over information collected in the China market. By retaining original data within China's borders and exporting copies for processing, one company noted that it is able to fulfill these jurisdictional requirements while maintaining their international processing and analytic operations. USCBC encourages companies to consult with legal counsel to ensure compliance should they wish to explore this avenue.

- **Filter out sensitive data** One company noted how restrictive data policies interact with the Multi-Level Protection Scheme (MLPS), an issue that first came to industry attention in 2007.

MLPS emerged as hot topic of debate due to China's broad Regulations on Classified Protection of Information Security (RCPIS), which classify data and data security according to broad and unclear definitions. These regulations prohibit foreign companies from handling certain sensitive data, which can be a problem for companies that provide international monitoring and data processing services to local entities— such as Chinese hospitals or state-owned enterprises (SOEs)—that handle this type of data. To remain compliant with this regulatory regime, which requires that this sensitive data remain within Chinese borders, they have constructed a mechanism that will filter out any sensitive data. For instance, they may receive notification that a server in a local hospital has overheated, but will filter out any patient information hosted on that server so that they can handle the problem from a purely mechanical perspective. By doing so they ensure compliance with the law, while simultaneously carrying out their maintenance operations.

- **Structure contracts to avoid risk** One foreign company operating in a sector involving "state secrets" highlighted the lack of clarity in governing this type of information. Because the sector in question caps foreign investment at a certain percentage, this company is required to operate via a joint-venture (JV) with a Chinese SOE. In drawing up contracts with their partner, the foreign company included provisions requiring the SOE—due to its close relationship with the government and ability to intimately interact with policymakers—to identify any data that could be construed as a "state secret" and take appropriate steps to ensure that this information not be provided to the foreign company or the JV. By placing the onus of responsibility on their Chinese partner, the company felt that it mitigated risk resulting from vague regulations on state secrets, although the company noted that they still must take measures to not fall afoul of these regulations by accident.

Company case study: Where are companies storing data?

China's current data regulatory environment requires companies to adopt a variety of strategies for determining where they store data, often depending on their overall business structure. Companies that operate primarily in a business-to-business (B2B) space tend to access overseas servers, and indicate a preference for storing data offshore. Companies that operate primarily in a business-to-customer (B2C) space, or sell consumer-facing products, indicate that they store data locally.

It's important to note that while companies believe regulations mandating the storage of consumer data within China's borders may not currently exist, many companies store their consumer data within China's borders *anyway* to hedge against an unclear legal environment. Some companies note that in order to comply with these restrictions, they have had to forfeit the application of certain customer relationship management (CRM) software, which may require the input of local Chinese customer data into global solutions—moving it across borders—in order to function.

Companies in the B2C space, or a combination of B2B and B2C businesses, tend to have a closer understanding of existing draft data policies given the legal liabilities of working with PII. In one example, a company in the automotive industry noted it conducts all China market analysis "in China, for China," and scrubs PII before more macro sales data is transmitted to HQ for analysis of global business performance.

Companies in the B2B space, while less likely to have core data stored in China, can still be impacted by data restriction policies. For example, multiple B2B companies noted issues transmitting data directly over their company cellular networks due to restrictions that require all cellular transmissions to go through a third party. Other companies have noted restrictions on transmission of GPS-related information for monitoring product performance, which can limit the scope of services they are able to offer in the China market.

Market Access for Cloud Solutions

Another challenge facing foreign companies in China is the inability to access globally used solutions in the China market. Much of this is because China's approach to regulating the market subjects a broad swathe of foreign company products and services to licensing and market access restrictions, preventing full deployment of these services in China.

One of the most commonly discussed issues in accessing global solutions is the ability to access, apply, or deploy global cloud solutions in the market. China's complicated regulatory regime on cloud computing is enshrined in the MIIT Telecommunications Services Catalogue, which was originally released in 2003 and most recently updated at the end of 2015.

The catalogue segments telecommunication services into two different categories: basic telecom services (BTS) and value-added telecom services (VATS). Both classifications are subject to corresponding licenses from MIIT. China's Catalogue Guiding Foreign Investment (CGFI), most recently updated in 2015, imposes additional foreign ownership restrictions based on these classifications, limiting foreign ownership in BTS and VATS to 49 percent and 50 percent, respectively. These limitations thus require foreign providers of IT solutions to find and partner with local players to deploy their solutions in the market.

Foreign companies are interested in investing in sectors requiring VATS licenses. Unlike other international markets, China's broad definition of telecom services defines Internet-based services—such as cloud computing, e-commerce, online data processing, email and video messaging, conference call platforms—as VATS. While foreign ownership restrictions differ by service and geography—some of China's VATS can be fully owned by foreign companies in free trade zones, and the VATS on ecommerce was liberalized to 100 percent ownership nationwide in early 2015—the majority of China's VATS sectors remain capped at 50 percent foreign ownership.

China's regulators have been slow to adopt changes to the telecom regulatory regime, despite rapid advancements in Internet and mobile-based technology since 2003. Historically, the regulatory environment has been vague and a number of multinational company (MNC) cloud providers have been able to provide cloud solutions in China without major issue. In early summer 2013, MIIT released a draft for public comment on changes to the catalogue before going silent on the issue for two years.

Provider perspectives on cloud computing restrictions in China

In 2015, the update to the catalogue expanded the language on licensing requirements for foreign companies, particularly in cloud computing, although companies remain unsure if they can expand or continue offering these services in China. These uncertainties continue to exist due to continuing vagueness in language: neither the 2003 catalogue nor the 2015 revision directly use the term "cloud computing," or describe any of the major cloud computing platforms — Infrastructure as a Service (IaaS) Platform as a Service (PaaS), or Software as a Service (SaaS)—by name.

Despite this, the catalogue expands the definition of internet data centers (IDCs), a VATS license identified as necessary for the operation of cloud computing infrastructure. Foreign companies state that this license is notoriously difficult to obtain, even via partnerships with local firms. The 2015 catalogue now formally requires licenses for items defined as "internet resources collaboration services," which refers to equipment and resources constructed on data centers and via the internet to provide customers with data storage and management services. Companies report that this language seems to describe IaaS and PaaS models, although other companies note continuing uncertainty on whether SaaS models are subject to this definition.

While the catalogue stated that MIIT would follow up with implementation measures to clarify and guide areas that remain unclear, as of July 2016 no such measures have been published. In the interim, major providers of cloud solutions report uncertainty on whether, and to what degree, they will be able to continue offering these solutions in the market.

Customer perspectives on accessing cloud computing solutions in China

A majority of interviewed companies noted that while most major global cloud applications are still accessible, some are completely inaccessible. For those that are accessible, performance and experience varies. Almost all interviewees indicated a global trend of migration toward cloud-based solutions, but cloud restrictions in China have required companies to alter their global strategies to fit the market in ways that impact efficiency and security.

While some MNCs indicated interest in exploring local options like AliCloud, the majority emphasized the importance of global uniformity, and using global solutions contracted via headquarters and deployed in home and international markets to ensure network stability. However, due to the investment restriction capping foreign investment at 50 percent in VATS services, customers must still engage with local vendors when looking for cloud solutions in China. Companies report difficulties in finding vendors that can ensure safe and effective integration of "China-specific" cloud solutions with their global company networks. These separate requirements can increase the cost, time, and information security risks for international companies operating in China. Inhibiting the use of global technology solutions in China may also force companies to develop China-specific information security solutions that could isolate China operations from an otherwise global network.

Overall, companies have varying policies on the use of cloud services in China, and are hesitant to commit to this new technology—even if they have already done so in other markets. For example, one B2B company imposed a China-specific restriction on using cloud services due to the inability to secure data or integrate data protection measures with local operations. Other companies engaging in consumer products may host their own private cloud servers to serve local needs, such as payroll or human resources information, but may hesitate in exploring public cloud or cloud-based enterprise solutions that would otherwise allow them to expand their business scope.

Company case study: Ensuring good service with local contracted service providers

Restrictions on overseas cloud service providers requiring local partners to service their product have created challenges and extra obstacles to troubleshooting issues with the provider. Companies report that the technical support offered by local third-party Chinese partners may not match the quality provided by global vendors. This is because global providers innately have a better understanding of their own global products, have know-how in handling issues with global connectivity, and have experience troubleshooting issues with clients.

One company noted that one solution to ensure better service from contracted providers was to work with providers to arrange local payment to the service provider. While not all providers allow this arrangement, paying the local contracted party directly can yield better service than making payment to their headquarters.

Internet Access

The explosive growth of China's internet industry presents companies with seemingly limitless opportunities for innovation and creativity. But to realize this, a reliable internet connection is a fundamental requirement.

Many of the challenges raised by companies are rooted in China's internet infrastructure. While companies report that access to domestically hosted websites is relatively smooth, all companies agree that access to the internet "beyond China's borders"—including sites that are hosted overseas, as well as sites that are completely or partially blocked by China's "Great Firewall," which filters or restricts access to certain websites or data hosted outside of China— is a challenge for their business operations. With only three major landing places for trans-oceanic optic fiber cabling systems in Qingdao, Shantou, and Shanghai, international internet traffic often encounters heavy service bottlenecks, which limit the flow of information. Service constraints are further impacted by the state monopoly in the telecommunications sector, providing companies with limited choices in terms of service and performance. Filtering content via the Great Firewall, which can increase latency, or slow internet speed, and lead to packet losses—the failure of information to arrive at the destination—during information transfer, creates additional obstacles to communication.

The overwhelming majority of companies interviewed for this report indicated that poor internet accessibility ranks among their top operational concerns, and is perhaps the top IT challenge in China. Internet problems hinder operations such as sharing R&D information between China-based and global teams; sharing files between internal offices or with China-based external clients; promoting products on global social media platforms; or communicating internally, such as via cross-border video conferences. Certain client relationship management (CRM) products or cloud-based file sharing solutions have been rendered completely unusable in the market due to issues with latency and deployment.

This challenge is compounded for companies operating critical applications that require instant transfer of information or immediate processing. These companies suffer high rates of packet loss between China and other markets, making it difficult to ensure stable operations. This can put international companies at a competitive disadvantage, as rival domestic companies may be able to provide these services onshore without similar obstacles. Other companies noted poor user

experience for consumers and internal teams due to latency in accessing corporate websites or company applications hosted offshore.

The majority of interviewed companies highlighted the additional cost of setting up China-specific infrastructure compliant with China's internet regulatory regime. Recurring challenges include constructing local data centers, creating local applications, or finding local vendors that can tailor, support, and maintain company global networks operating under the Great Firewall. Companies that are able to deploy global solutions often need to work with their global providers to customize their IT architecture specifically for China, in effect creating two different IT systems that country, regional, and global CIOs must manage.

A recurring challenge is the difficulty communicating the intricacies of the China-specific internet to the global headquarters, particularly in liaising with global IT support. Numerous CIOs emphasized the "China-specific" nature of internet problems they encounter, which can be difficult to communicate if similar issues are not experienced in other markets. Companies need to internally justify the cost and time of realignments to their global cyber strategy if the majority of the rationale is only emerging from a single (yet essential) market.

Finally, the internet has emerged as a modern tool of business, with companies leveraging online power to connect with new people, develop new ideas, and create new services. The growth of these business models in China is tempered by policymakers' strict approach to internet governance, which has barred many global user-generated content services in the Chinese mainland. Such policy prescriptions bring uncertainty to the future development of the "shared economy," a concept discussed in China's 13th Five-Year Plan and by Premier Li Keqiang.

Ensuring Connectivity

Every company interviewed for this study emphasized that the internet environment in China adds cost burdens to their operations that do not exist in other markets. CIOs noted the importance, and ubiquity, of establishing global internal networks to ensure that business performance is not impacted by China's internet regulatory regime. These solutions can range from using internal virtual private networks (VPNs) to setting up internal company networks that connect China operations directly to headquarters in other markets, although this option may be expensive and time consuming to construct.

Companies report varying performance for VPN set-ups in terms of speed and reliability via lease lines that connect through gateways in Hong Kong, Singapore, or other regional ports. Some companies improve connections by hosting servers in China, installing network accelerators to handle latency issues, or setting up local (China) and external (Hong Kong- or Singapore-based) internet gateways with real-time switching capabilities. Other solutions include setting up international mobile connections (such as through Hong Kong or Singapore) or reverse proxies. Companies also noted the importance of regularly monitoring and upgrading bandwidth capacity to account for increased traffic flows to ensure stability and speed, although the lack of telecommunication players in the market limits service options.

Company case study: Increasing connectivity speeds

One company that was working to increase the connection speed for their mobile business development teams noted that moving their corporate VPN connection to China from overseas improved access speeds. In one example, a company that was having difficulty accessing a CRM system hosted overseas moved to a local VPN, which made the connection considerably faster.

Network accelerators provided by third-party services also are a solution to boost connection speeds for CRMs and other cloud-based services hosted overseas.

Compliance

Companies report that they prioritize compliance with Chinese laws and regulations as they form their internet policies, although the regulatory framework remains grey on VPN use. Most of the interviewed companies said local authorities and telecommunications companies have generally allowed MNC IT teams to set up corporate VPN structures to ensure uninterrupted communication with their international businesses, recognizing VPNs as a necessity for their operations.

To emphasize compliance, some companies proactively engaged with regulators to demonstrate that their internal VPN or connection networks are used solely for business purposes. Through this active engagement, companies were able to demonstrate willingness to comply, which sent an important message to local regulators. Other companies emphasized the importance of allowing "non-China web" access to employees who require VPN access for their core business functions, such as research teams that need access to information outside of Chinese borders.

Despite this, no company has found a magic bullet to solve their internet problems. Even if companies are able to set up internal networks that can provide a manageable connection between China and international teams, CIOs report having to be constantly aware of a changing environment that may impact the long-term use of a product.

Technology Policies and Transparency

China's rapidly developing tech policy framework has left CIOs uncertain about the types of technologies they can deploy in China. Changing or uncertain regulations have the potential to affect the functionality of products one day and then render them inaccessible the next. Key products of concern include file sharing solutions, CRM software, or other applications that are internet-based or use cloud-based servers.

China's opaque regulatory environment poses challenges to global IT teams that might be unfamiliar with China-specific regulations, particularly governing encryption functionality, which has been historically vague and sensitive. This makes it challenging for CIOs to determine how or whether to deploy global solutions in the market, and may lead companies to hesitate before venturing into business areas that could be explored using new types of technology.

Domestic Security Policies

Political tensions and recent high-level attention from the Chinese and US governments about technology security continue to affect the ICT industry. News reports have focused on hacking incidents and requests for government backdoors for espionage purposes, creating a sense of urgency for regulators. Companies in all sectors are concerned about policies that favor domestic technology in the name of national security, rather than technological performance.

Throughout 2015, discussion on this topic has focused on the promotion of "secure and controllable" technology in China's IT industry. This term has not been publically defined by regulators, but is understood by many companies to mean not using foreign products and technologies. This language first received international attention following the publication of draft documents by the China Banking Regulatory Commission (CBRC) calling for "secure and controllable" technologies in the banking industry. Foreign companies then began reporting the loss of major contracts with Chinese state-owned banks based on the perception that foreign ICT products were not acceptable. Although these regulations were ultimately suspended, this language became clear in China's National Security Law, which calls for achieving "secure and controllable" technology for "critical infrastructure" and in "critical information sectors," terms that have not yet been defined by policymakers.

Following pushback by USCBC and other industry associations, these discussions were elevated to the highest levels of the US-China relationship, culminating in pledges by Chinese regulators at the end of 2015 that China's ICT security measures would not unnecessarily limit or restrict the purchase, sale, or use of ICT products based on nationality. Despite this, foreign ICT companies report that challenges remain with "secure and controllable," particularly because these policies are "suspended" rather than "cancelled," and because many policies continue to use this undefined terminology. While there have been reports that a technical committee under the Cyberspace Administration of China (TC-260) has been developing 10 standards for "secure and controllable" that will cover CPUs, office productivity suites, operating systems, and other enterprise functions, it is unclear how much foreign companies will be able to influence these processes.

Company case study: Secure and controllable

USCBC members in the ICT industry have identified the following effects of "secure and controllable" regulations:

- **No definition of 'secure and controllable'** USCBC members noted that because "secure and controllable" lacks a concrete definition, Chinese clients and business partners interpret this language as code for "local." Because of this, foreign products face unwritten restrictions in procurement tenders that prioritize local products. Members report that SOEs continue their preference of domestic products despite high-level commitments to nondiscriminatory ICT procurement.
- **Regulation suspension leads to uncertainty** USCBC members noted that the CBRC regulations were simply "suspended" rather than eliminated, which influences how SOEs and Chinese banks perceive the situation. Because "secure and controllable" could mean "local," many SOEs and banks believe that the ultimate goal of the Chinese government is to push for domestic procurement of ICT security products. The draft CBRC policies called for 75 percent of all ICT products to be "secure and controllable" by 2019. Therefore, many SOEs and banks are choosing to comply now, rather than continue contracts with foreign vendors and run the risk of an expensive switch in the future.

- **Internal procurement practices discriminate against foreign products** The procurement system among many SOEs and banks places foreign products at a disadvantage against local products, based on measurements that automatically classify foreign products as less secure than domestic products. One USCBC member company noted that some SOEs assess IT products with a point-based system based on cost, quality, and security. There are cases where foreign products were assigned a score of "0" in the security category based solely on their non-Chinese origin, which puts them at an inherent disadvantage to domestic competitors. Many of these measurements come from internal SOE product bidding processes, rather than overt policies, but are reflective of how Chinese SOEs are hedging their long-term procurement decisions against the uncertainty of whether "secure and controllable" policies will be implemented.

USCBC conducted extensive analysis of company challenges with "secure and controllable" policies and policies with similar language, and compiled and maintains a regularly updated chart of draft and existing policies invoking "secure and controllable" terminology (see Appendix II).

Encryption

An important component of the security discussion is China's developing regulatory approach to encryption. The regulatory environment began in 1999, when the Office of the State Commercial Cryptography Administration (OSCCA)—the commercial encryption arm of the State Encryption Management Bureau (SEMB), which is the lead organization for cryptography and encryption issues in China—released provisions outlining the scope of devices subject to China's encryption management regulations. These provisions stipulate that any product whose "core functionality" is to provide encryption services must receive relevant certification from OSCCA, otherwise it may be confiscated; blocked for sale, import, or export; or used as grounds for criminal prosecution.

Over the past 16 years, several subsequent rules governing encryption products have been issued, although many companies believe the crucial question remains: which encryption functions are "core functions?" Although the 2015 US-China Joint Commission on Commerce and Trade talks discussed the issue, companies report continued confusion on the types of products subject to regulation.

This confusion has effectively required companies in all industries to acquire certification for devices including mobile phones, laptops, servers, and other common equipment that contain chips that facilitate data encryption. Before procuring certain types of IT hardware or software, it is critically important to determine whether these devices require OSCCA certification. These certificates—which vary depending on purpose, ranging from manufacturing, product sales, and until recently, R&D—are reportedly difficult to obtain. The process may require the disclosure of product source code, as well as documents such as business licenses, descriptions of the project, and import licenses for overseas products.

Some companies noted that products must also employ Chinese encryption algorithms—known as "SMX," whereby "X" represents a number corresponding to a specific encryption standard, such as SM2 or SM3—even though these algorithms have not been tested by international experts. Companies cited examples of IT products purchased by global IT teams that could not be imported into China because they lacked OSCCA certification. Several companies lamented wasted resources when globally-produced IT equipment was completely blocked due to a lack of relevant certification.

Some OSCCA certification requirements can be relatively easily met by locally purchasing global devices. One company reported successfully bypassing the certification problem by approaching global vendors' local teams and purchasing identical devices that met OSCCA requirements. The company reported that the devices performed on a global standard, but that it enhanced monitoring for the networks to which the devices were connected due to uncertainties about the strength of local encryption algorithms.

Several other companies noted they were able to successfully navigate the encryption certification process themselves. One company obtained the required encryption certification for the installation of BitLocker by applying for a license at local OSCCA bureaus in each of the cities where the company had operations. The two-month process was relatively smooth, possibly because regulatory authorities had already cleared BitLocker for use in China.

Recent references to encryption in draft laws have mandated the storage of encryption keys with local security bureaus or the complete adoption of local Chinese encryption algorithms by a specific date. China is also drafting an encryption law, which will govern all aspects of encryption, including commercial application. This law is expected to be released sometime in 2016.

Best practices in navigating the encryption environment

USCBC and CCA members identified the following strategies for navigating China's encryption policy environment:

- **Ensure communication between local IT and global compliance teams** Companies noted the importance of conferring with local IT policy teams to determine what type of global hardware products can be used in-country under China's licensing regime, and whether similar products offered by global vendors are available for purchase in China.
- **Communicate with local vendors** Companies with global contractors need to know if their partners have local vendors in China. Most major international IT solutions providers have a China presence with staff familiar with China's encryption regulations. Proactively engaging with these companies before IT procurement decisions are made, either at the China-level or at global HQ, is critical in ensuring the legality of IT products that may require encryption certification in the market.
- **Monitor the local policy environment** Companies in all industries should recognize that China is adopting an increasingly active stance on encryption policy, particularly by mandating the complete adoption of Chinese encryption algorithms over cryptographic solutions that have been tested for use in other markets. Understanding how the encryption environment may develop, and if or how these developments may impact your operations, will be important to companies going forward.

Internal Company Policies

China presents a unique set of challenges to companies and their IT outfits in deploying solutions and maintaining the security of their operations. Ensuring the safety of data, intellectual property, and other sensitive information is of vital importance for any MNC with global operations. Most companies adopt global security policies crafted by their headquarters, but some companies note security policies specific to the China market, which include:

- **Hardware** Companies set restrictions preventing visiting executives from bringing laptops and other devices to China. This can be challenging when executives are visiting additional countries in conjunction with their China travel. In order to ensure executives have access to files needed to maintain their daily operations, some companies have set up work stations in their China offices where executives can access their files through a secure corporate network connection.

- **IP concerns** Companies with intellectual property prioritize information security. While most companies adopt the same security policies in China that they employ in their global operations for the protection of IP, some companies report that they use advanced monitoring of files in China to proactively sense unwanted or excessive file movement. For example, one company with B2B operations stated that it uses sophisticated file monitoring systems in China. Companies also note the importance of classifying IP based on sensitivity—more sensitive IP would be under closer monitoring with additional permissions.

Adopting Local Solutions

Many companies adopt local software solutions to help them meet business goals in the China market. For example, the mobile communication application WeChat has been adopted by business development teams to stay competitive with Chinese firms who leverage WeChat as a marketing and customer engagement tool. However, security is often a concern when adopting local solutions, and many companies note ongoing discussions with their global IT teams related to software and data security. Some companies prohibit WeChat due to security reasons, while others report challenges in communicating with HQ to get approvals to deploy local solutions outside of external marketing functions, such as for business development, customer correspondence, and internal communications.

While social media and platforms such as WeChat are common marketing platforms, it is less common for companies to use local hardware and data storage. One company reported that it uses local branded routers for non-sensitive connections. Other companies say they have considered the viability of domestic cloud solutions, with one company using the local cloud solution AliCloud to host non-sensitive information shared with external partners. Adopting local products depends on the company, and while companies noted that marketing tools are essential to being competitive in the China market, they remain hesitant to adopt local solutions for internal functions or data storage because of security concerns.

Working with JVs

While most companies do not report strong pressure to adopt domestic IT solutions, it is experienced by some companies in joint ventures (JV) with domestic partners. One company reported being pressured by its JV partner to integrate its networking solutions with domestic networking equipment—a move that ran counter to the company's global IT policy.

Companies with JVs commonly structure their internal networks so that the JV may only have partial access to their corporate network, while other companies indicate that they keep networks completely separate. This choice can depend on the requirements of the JV partner, and companies should work with their JV partners to ensure they are connected where needed, while also maintaining security for both parties. Companies operating in more sensitive, IP-intensive fields tend to be JV-adverse, and keep networks separate where JV partnerships are required. Companies in less sensitive areas may share certain networks or integrate storage for their external clients' information where sharing is required to advance the business cooperatively.

Conclusion

China is at the cusp of the digital frontier. Companies in all industries are leveraging "analytics" to tailor services to consumer needs, integrate payment methods for convenience, optimize industrial supply chains, and predict or prevent accidents. Companies note that the speed of innovation is unlike any other market; before, online products could take 10-15 years to come to market, whereas now it may only take one year. The coming of age of China's "internet generation" —young people who grew up with the internet as a tool—has primed the development of an information-based sharing economy and created just as many disruptions to traditional commercial models as opportunities for new growth and creativity.

Companies are seeing changes in their internal structures to respond to these trends, particularly with the role of their CIO increasingly demanding competence in hard skills as well as the policy environment. Having an understanding of both is vital in communicating to headquarters what companies can and cannot do in China in terms of technology solutions and access. While CIOs must continue to ensure their IT infrastructure is functional and secure, they are working more closely with their local legal, government affairs, R&D, and other support teams to develop a comprehensive understanding of the new growth channels in China's economy.

Despite these trends, companies remain concerned with a policy regime that may be out-of-step with a rapidly changing environment. China is not alone in its efforts to find order in the complex web of possibilities and threats that arise at the intersection of data, information technology, and security. However, China's opaque and sometimes contradictory framework creates a scenario where companies often cannot assist in these efforts.

Companies support efforts to create a cyber and IT environment that optimizes commercial performance *and* ensures the safety of user experience, whether those users are individuals, companies, or governments. To do this, policymakers must be willing to engage with industry stakeholders to identify how the policy environment can be developed to achieve their ultimate objectives in security and economic development. Building consensus on this issue is critical in developing a regulatory framework that encourages innovation and development, while maintaining an IT environment that is safe and accessible.

Appendix 1: Policy Announcements Related to Data Management

USCBC compiled a database of China's policies mandating data localization and restricting cross-border data flows, based on public sources and conversations with industry members. This list is not exhaustive and will be regularly updated.

Policy	Releasing Agency	Release Date	Specific Clauses
Regulations on Telecommunications, Regulations on Internet Information Services, and Regulations on Electronic Bulletin Services	MIIT	September 20, 2000; September 25, 2000; October 08, 2000	These regulations set the framework for obtaining internet content provider (ICP) licenses and permits, for nonprofit and profit-making websites, respectively. While the clauses do not contain explicit references to data localization, conversations with companies indicate that to obtain an ICP permit or license, servers hosting relevant websites must be located within mainland China.
Law of the People's Republic of China on Guarding State Secrets	NPC	Originally released September 5, 1988; Updated April 29, 2010	Mentioned several times throughout the document; Article 48, Clause 4 specifically forbids mailing or consigning state secrets to leave the country, or physically carrying or transmitting state secrets without permission from relevant departments.
Notice of the People's Bank of China on Urging Banking Financial Institutions to Protect Personal Financial Information	PBOC	January 21, 2011	Article 3.6 states that banks in China that conduct analytical or data processing for personal financial data collected in China must do so within the country.
Guidelines on the Information System Security Management of Insurance Companies (for Trial Implementation)	CIRC	November 16, 2011	Article 23 states that IT facilities must be within China (not including Hong Kong, Macau, or Taiwan).
Guidelines on the Business Startup Check of Insurance Companies	CIRC	Released November 22, 2004; Updated April 26, 2011	Article 6.4 states that business data, financial data, and other kinds of important data must be stored within the Chinese mainland, on independent data storage facilities.

Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services (GB/Z 28828-2012)	SAC, AQSIQ; voluntary guidelines that are legally non-binding	November 5, 2012	Article 5.4.5 states that administrators of personal data may not deliver that data outside of China, including to any individual located overseas, or any organization or institution registered overseas, without the explicit consent of the owner of that personal data, explicit provisions of laws and regulations, or permission from relevant authorities.
Regulation on the Administration of the Credit Investigation Industry	The State Council	January 21, 2013	Article 24 states that credit information collected in China must be analyzed, stored, and processed within China's borders.
Measures for the Administration of Population Health Information (for Trial Implementation)	NHFPC	May 5, 2014	Article 10 states that population health information may not be stored abroad.
Information Security Technology—Security Guide of Cloud Computing Services (GB/T 31167-2014)	SAC; recommended standard, although companies note Chinese officials have treated it like a mandatory one. Forms part of the cloud computing cybersecurity review.	September 3, 2014, implemented April 1, 2015	Articles 6.7.9, 7.1.10, 7.3.2(c) have provisions that cloud computing servers and related equipment must be stored within the Chinese mainland.
Information Security Technology—Security Capability Requirements of Cloud Computing Services (GB/T 31168-2014)	SAC; recommended standard, although companies note Chinese officials have treated it like a mandatory one. Forms part of the cloud computing cybersecurity review.	September 3, 2014, implemented April 1, 2015	Articles 14.2.1(d) and (e) state that cloud computing servers and related equipment must be stored within the Chinese mainland.
Specifications for Information Security of Credit Information Service Agencies (JR/T 0117-2014)	PBOC	November 17, 2014	Article 9.9 states that credit information service agencies operating in China must store all data collected in China within the country; sorting, storage, and processing must be done within China.

Provisions on Security Protection of Power Monitoring Systems	NDRC	Originally released December 20, 2004; Updated August 1, 2014	Article 7 states that power dispatching data networks must employ independent network devices isolated from other data networks within the power company. This is interpreted by companies to mandate the construction of separate, China-based network devices.
Opinions of the Office of the Central Leading Group for Cyberspace Affairs on Strengthening Cybersecurity Administration of Cloud Computing Services for Communist Party and Government Agencies	CAC; forms part of the cloud computing cybersecurity review.	December 30, 2014	Article 2 states that data processing centers must be stored within the country for cloud computing platforms providing services to the Chinese Communist Party and to government agencies.
System Safety Program for Cloud Computing Services	CAC	August 8, 2015	Specifically referencing the requirements under GB/T 21168-2014, article 4.10.2 states that cloud computing providers must ensure that their machine rooms, cloud computing servers, and physical devices that run critical business applications and data are all located within China.
Regulations on Map Management	The State Council	November 26, 2015	Article 34 states that internet mapping entities should store their servers within China.
Regulations on Online Publication Services	SAPPRFT, MIIT	February 14, 2016	Article 20.7 states that publishing websites and related servers must be kept on the Chinese mainland.

Cross-Border Data Flows

Policy Title	Releasing Agency	Release Date	Specific Clauses
Notice of the People's Bank of China on Urging Banking Financial Institutions to Protect Personal Financial Information	PBOC	January 21, 2011	Article 3.6 states that banks in China that conduct analytical or data processing for personal financial data collected in China must do so within the country. Banking institutions are forbidden from sending this data overseas, unless otherwise permitted by relevant provisions from the PBOC.
Guidelines on Personal Information Protection in Public and Commercial Service Information Systems of Information Security Technology	SAC, AQSIQ; voluntary guidelines that are legally non-binding	January 21, 2013	Article 5.4.5 states that administrators of personal data may not deliver that data outside of China, including to any individual located overseas, or organization or institution registered overseas, without the explicit consent of the owner of that personal data, explicit provisions of laws and regulations, or permission from relevant authorities.
Measures for the Administration of Population Health Information (for Trial Implementation)	NHFPC	May 5, 2014	Article 10 states that population health information may not be stored abroad. Article 13 states that personal healthcare information that touches on "confidential information" may not be sent overseas.
Specifications for Information Security of Credit Information Service Agencies (JR/T 0117-2014)	PBOC	November 17, 2014	Article 9.9 states that credit information service agencies operating in China must store all data collected in China within the country; sorting, storage, and processing must be done within China, and this information cannot be passed overseas via the internet or other channels or intermediaries. In the case of providing overseas institutions with personal financial data, these agencies must respect relevant laws and regulations within China.

Information Security Technology—Security Guide of Cloud Computing Services (GB/T 31167-2014)	SAC; recommended standard, although companies note Chinese officials have treated it like a mandatory one. Forms part of the cloud computing cybersecurity review.	September 3, 2014, implemented April 1, 2015	Articles 6.7.9, 7.1.10, 7.3.2(c) have provisions that cloud computing servers and related equipment must be stored within the Chinese mainland. These provisions also state that due to relevant Chinese laws and regulations, data hosted on these servers is not to leave China's borders.
Information Security Technology—Security Capability Requirements of Cloud Computing Services (GB/T 31168-2014)	SAC; recommended standard, but often treated as mandatory. Forms part of the cloud computing cybersecurity review.	September 3, 2014, implemented April 1, 2015	Articles 14.2.1(d) and (e) state that cloud computing servers and related equipment must be stored within the Chinese mainland. Article 7.10.2 states that it is forbidden to send data hosted on these servers outside of China.
Provisions on Security Protection of Power Monitoring Systems	NDRC	Originally released December 20, 2004; Updated August 1, 2014	Article 7 states that power dispatching data networks must employ independent network devices isolated from other data networks within the power company. This is interpreted by companies to mandate the construction of separate, China-based network devices. Article 11 also states that it is prohibited for any universal network server to cross the borders between production control and information management zones, which companies note imposes a mandate on "one-way data," effectively blocking data from communicating with international operations.
Opinions of the Office of the Central Leading Group for Cyberspace Affairs on Strengthening Cybersecurity Administration of Cloud Computing Services for Communist Party and Government Agencies	CAC; forms part of the cloud computing cybersecurity review.	December 30, 2014	Article 2 states that data processing centers must be stored within the country for cloud computing platforms providing services to the Chinese Communist Party and government agencies. Sensitive information cannot be sent, processed, or stored overseas without approval.

System Safety Program for Cloud Computing Services	CAC	August 8, 2015	Specifically referencing the requirements under GB/T 21168-2014, article 4.10.2 states that cloud computing providers must ensure that their machine rooms, cloud computing servers, and physical devices that run critical business applications and data are all located within China. Article 4.3.10.2 states that cloud computing platforms are restricted from sending client data and other kinds of "important data" overseas.
Regulations on Map Management	The State Council	November 26, 2015	Article 24 states that no entities and individuals may publish, exhibit, sell, import, or export maps that do not conform to relevant Chinese standards and regulations, and it is forbidden to carry or transmit non-conforming maps outside of China. Article 34 states that internet mapping entities should store their servers within China.

Appendix II: Existing Regulations Containing References to "Secure and Controllable" or Similarly Worded Language

Policy Title	Releasing Agency	Release Date	Specific Clauses
Guidelines on the Information System Security Management of Insurance Companies (for Trial Implementation)	CIRC	November 16, 2011	These guidelines call for "secure and controllable" data exchange processes with external agencies, and "secure and reliable" transaction processes when handling personal information and client-sensitive business information.
Guiding Opinions from the Ministry of Industry and Information Technology (MIIT) on Strengthening Cybersecurity in the Telecommunication and Internet Industry	MIIT	August 29, 2014	These opinions call for the application of "secure and controllable" software and hardware for telecommunication firms, which should be taken into consideration in government tenders.

Opinions on Vigorously Developing Ecommerce and Accelerating the Fostering the New Economy Engine	The State Council	May 7, 2015	These opinions call for the adoption of "secure and controllable" information equipment and cybersecurity products, as well as the establishment of "secure and dependable" public service and mobile platforms.
Guiding Opinions of the State Council on Actively Rolling out the Internet Plus Initiative	The State Council	July 4, 2015	These opinions highlight the importance of building a "secure and dependable" financial transaction network.
National Security Law	NPC	July 1, 2015	The law states that China must ensure that core technologies in information technology, critical infrastructure, and the development of internet structures are all "secure and controllable."
Interim Measures for the Supervision of the Internet Insurance Business	CIRC	July 22, 2015	The measures state that third-party internet platforms involved in online insurance businesses must have "secure and reliable" internet operating systems and information security management systems.
Notice of the MIIT on Performing Cybersecurity Pilot Demonstration Work in the Telecommunications Industry	MIIT	August 5, 2015	This pilot program calls on telecommunication firms to adopt "secure and reliable" technology, which may have an impact on procurement of foreign-produced equipment.
Opinions of the State Council on Reforming the Pharmaceutical and Medical Equipment Review and Approval System	The State Council	August 18, 2015	These opinions state that "secure and controllable" medical devices can be eligible for expedited reviews at the provincial level. USCBC has learned that only domestic medical devices are considered "secure and controllable."
Guidelines of MIIT and the Standardization Administration of China on National Standards for Intelligent Manufacturing	MIIT, Standardization Administration	December 30, 2015	These guidelines state that China's intelligent manufacturing is held to the standards of "indigenous, secure, and controllable."
Action Plan of MIIT for Effectively Implementing *Guiding Opinions of the State Council on Actively Rolling out the Internet Plus Initiative* (2015-2018)	MIIT	November 25, 2015	The action plan calls for the construction of a "secure and reliable" environment for the production of ICT products, beginning with high-end general chips and software. The plan also calls for "secure and reliable" servers, memory storage systems, desktop computers, external devices, network systems, basic software, and other ICT products.

Guiding Opinions of the State Council General Office on Promoting and Regulating the Development of Big Data Application in Health and Medical Sectors	The State Council	June 24, 2016	The policy calls for the adoption of "secure and controllable" and "indigenous and controllable" standards and technology, particularly in areas using "critical infrastructure."

Appendix III: Guide to Names of Chinese Agencies

This list includes the full names for the Chinese official ministries, agencies, and organizations listed in Appendices I and II.

CBRC	China Banking Regulatory Commission
CIRC	China Insurance Regulatory Commission
MIIT	Ministry of Industry and Information Technology
NDRC	National Development and Reform Commission
NHFPC	National Health and Family Planning Commission
NPC	National People's Congress
PBOC	People's Bank of China
SAC	Standardization Administration of China
SAIC	State Administration of Industry and Commerce
SAPPRFT	State Administration of Press, Publication, Radio, Film and Television