"China's Cybersecurity Law: Approaches and Leading Practices for Compliance and Enterprise Security"

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, "China's Cybersecurity Law: Approaches and Leading Practices for Compliance and Enterprise Security," on April 8, 2021.

During this roundtable we explored how enterprises are approaching compliance with China's Cybersecurity Law (CSL) and enterprise risk management. We wanted to explore: What are the compliance imperatives? What are the enterprise risk management priorities? What are the leading practices?

Our speakers included Accenture Security subject-matter experts, enterprise CISOs and board members. The session was hosted by Kris Burkhardt, Accenture CISO and ACF chair.

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

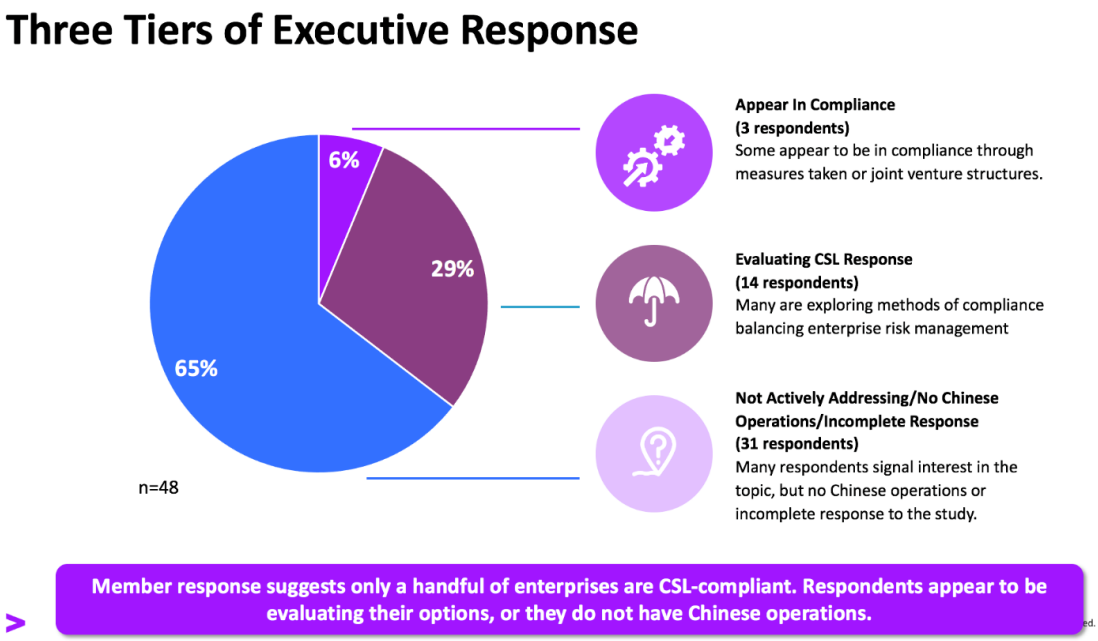
Compliance imperatives

CSL compliance requires knowing the enterprise's tier within the Multi-Level Protection Scheme (MLPS), adhering to core systems requirements, meeting data localization requirements and following encryption and encryption key storage requirements—as well as complying with government requests.

In response to member interest, the ACF conducted a brief survey regarding these challenges and in conjunction with global enterprise risk management. The purpose of the research was to determine how ACF members are responding to the requirements of CSL and the ways they are mitigating enterprise risk.

The data suggests there are some early movers who have operations in China and are addressing the requirements of CSL directly. Of those respondents who are evaluating their options (29%), nearly all report they are actively considering how to comply and take steps to reduce enterprise

risk. Clearly, CSL is on the radar of top executives with operations in China as they await more information and guidance regarding enforcement. Complete survey findings are available here.



CSL compliance is challenging for several reasons, Forum members report, most notably due to ambiguity and uncertainty.

For example, the Chinese government is expected to assert more control and compliance enforcement over time. A subject-matter expert said: "Enterprises would be well-served to exceed their current compliance requirements. Regulations are written ambiguously for a reason and can change in a heartbeat." Another subject-matter expert added: "Assume a broad interpretation of regulatory requirements and assess what it will take to get one level above that."

MLPS tiering also creates challenges. Self-assessment requirements are effective June 2021. Factors that might drive greater scrutiny from Chinese regulators include designation as critical information infrastructure (that is, transportation, telecommunications; the number of Chinese citizens and other Chinese companies engaged with the enterprise; and the volume or value of business transactions).

"Today you may have six months to comply with CSL regulations," said a CISO. "But tomorrow your enterprise may be reclassified as a company of interest." A subject-matter expert told CISOs they will likely encounter situations where they have to tell the CEO: "We'll do everything we can to comply with Chinese regulations, but don't blame me if China changes the rules."

Technology can be a key driver of compliance. CSL requires certain enterprises based on their MLPS tier to maintain and own specific core systems (for example, Active Directory and CRM). Depending on MLPS tier, CSL requires "personal" data and "important" data collected or

generated in China to be stored in China. In addition, CSL has specific requirements for storing encrypted data keys in China.

Risk management priorities

Privacy and data protection are key concerns of Chinese regulators. Several forum members said that complying with other standards, such as the European Union's General Data Protection Regulation (GDPR) or the Organization for Economic Co-operation and Development (OECD), can position enterprises well for compliance with Chinese requirements. "Following core privacy principles will get you 90% of the way there," said a subject-matter expert.

CISOs are advised to segment China operations from the global network. If and when countries such as Russia, Saudi Arabia and Turkey require local country segmentation, enterprises that succeed in China will know what it takes to maintain global security standards on segmented operating networks.

Enterprises must also make informed decisions about what to disclose in the event of a breach. Many instances do not require disclosure and, in fact, Chinese regulators may even discourage it.

The board of directors has its own priorities. A board member said: "I want to understand how the risk profile is changing. What is the rate of change? Where can we get an objective third-party perspective?"

Leading practices

- Begin the CSL self-assessment process now. Requirements are effective June, 2021 and the process could take longer than most enterprises anticipate.
- Get comfortable with ambiguity. The Chinese government continues to revise and update its CSL, but that is not a rationale for maintaining the status quo or delaying plans to address compliance.
- Consider the benefits in localizing, isolating, or segmenting operations in China. Independent China operations, or potentially joint ventures, could be considered. Assume Chinese officials have access to any data that resides in China.
- Explore required technology architecture revisions. Ensure compliance with China's requirements in network, data, applications and access. Understand the options for hard and cold data copies and when and where to back up data.
- Maintain situational awareness. Changes in the geopolitical climate can suddenly influence security posture. For example, one CISO said that employee social media posts about Tibet could draw the scrutiny of Chinese regulators. A subject-matter expert cautioned about references to Taiwan on a company's website that might run counter to China's position. One CISO said: "It is important to make sure employees in China get awareness training and

understand the sensitivity of certain things, so they don't trigger any unwanted attention on social media."

- Assess the implications of CSL and privacy regulations together, not separately. An integrated perspective can improve risk management decisions. The legal team should monitor changes to CSL and data privacy and collaborate with the CISO on cybersecurity implications.
- Recognize that Chinese suppliers will have their own priorities. Even when paying a local vendor, expect them to have obligations to the Chinese government. It's likely that a mainland consultant will provide a different perspective to a consultant based outside China.

Conclusion

CISOs that make the calculation on CSL compliance and enterprise risk management approaches now should emerge with an actionable road map for remediation and regulatory authority review. Enterprises that delay while waiting for greater clarity from Chinese regulators risk falling behind competitors and undermining their strategy in China. For CISOs, CSL presents another opportunity to take a leadership position, working with Legal, the COO and mainland leaders to mitigate enterprise risks and enable the success of operations in China.

CONTACT

Kris Burkhardt

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

LinkedIn

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 537,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

View the entire suite of ACF roundtable summaries on our webpage – here.