Operating Securely in China

What CISOs Need to Know about Security Challenges in the Region

Accenture Cybersecurity Forum
Global Executive Leadership Network

12 April 2023
Session Summary

From the Accenture Leadership

Cybersecurity challenges in China, including nation-state threat actors, ambiguous regulations, alignment with business strategy and resource constraints, are significant concerns among Accenture Cybersecurity Forum members.

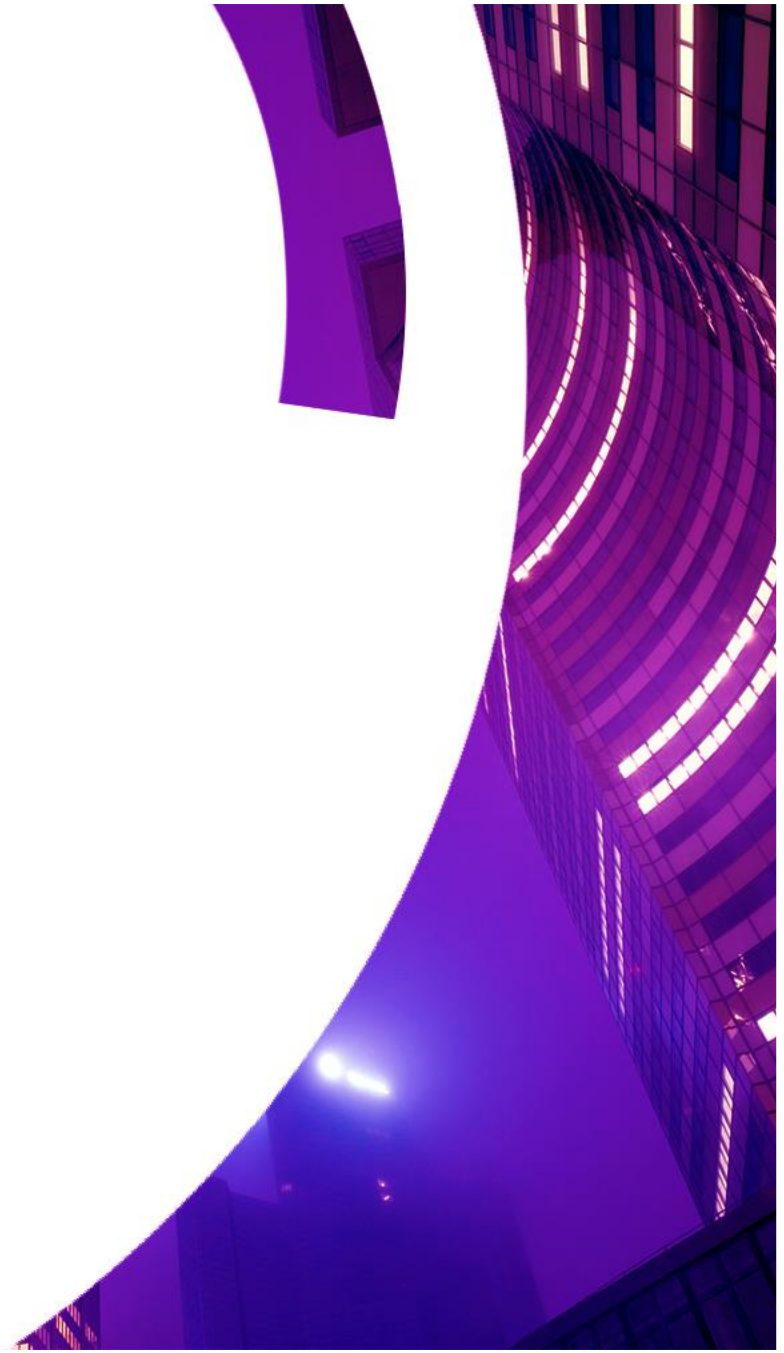
We are grateful that members shared their experience and questions about operating securely in China. Regulatory compliance and data protection are clearly top of mind. A major takeaway was about the importance of optionality, flexibility and resiliency in implementing China cybersecurity strategy. The current tensions between China and other nations must be considered in scenario planning. And initiatives such as the 'China Standards 2035' strategy which aims to create a blueprint for the Chinese government and leading tech companies to set global standards for emerging technologies, such as 5G, Internet of Things (IoT), and artificial intelligence (AI), need to be on the CISO's radar.

Thank you to all those who participated in the roundtable discussion. We hope you find the ideas and best practices that emerged from the conversation useful as you lead your enterprise in operating securely in China.

Cheers,

Paolo Dal Cin
Accenture Security Global Lead
ACF Executive Sponsor
LinkedIn

Kris Burkhardt
Accenture CISO
ACF Chair
LinkedIn



Operating Securely in China: What CISOs Need to Know about Security Challenges in the Region

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “Operating Securely in China: What CISOs Need to Know about Security Challenges in the Region,” on April 12, 2023.

Forum members have told us that they have questions about cybersecurity best practices when operating in China. In this session Forum members and subject matter experts discussed how global security executives can successfully address operations, resilience and compliance concerns within the suite of Chinese Cybersecurity Laws, including the China Cybersecurity Law (CSL), Data Security Law (DSL) and Personal Information Protection Law (PIPL). What are the top compliance issues facing CISOs related to these laws? What steps should CISOs take to assure their enterprise data and assets remain secure? What leading practices should CISOs consider?

This 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, nor participants, is revealed.

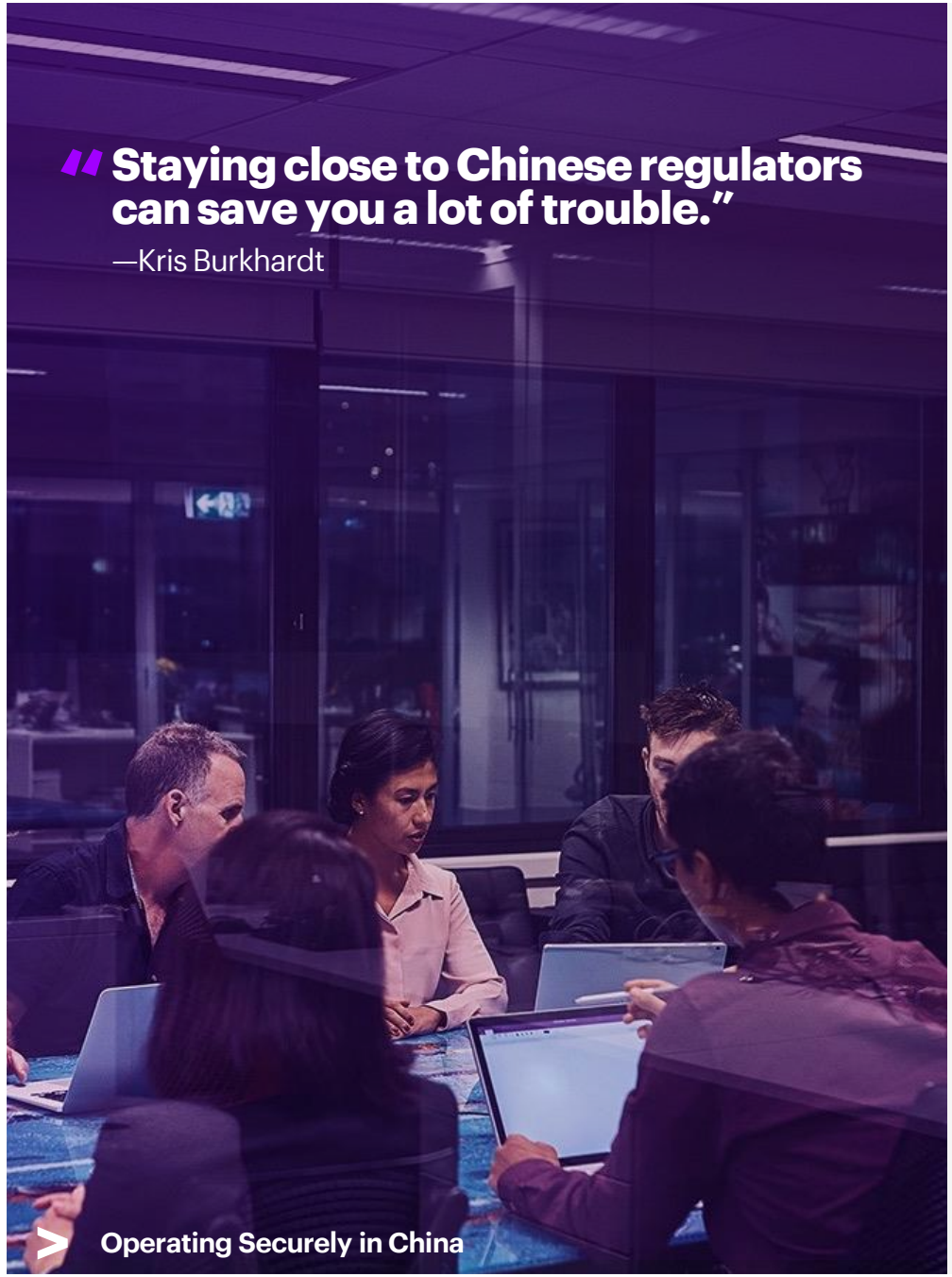
In this summary:

Optionality, flexibility and resiliency

The fluid nature of China’s approach to cybersecurity regulation enforcement was a major topic of conversation. “We can’t really know what’s going to happen,” said a subject matter expert. “The interpretation and application of regulations will vary by law and by the attitudes of those responsible for enforcement.” Another Forum member added: “Expect uncertainty and ambiguity.”

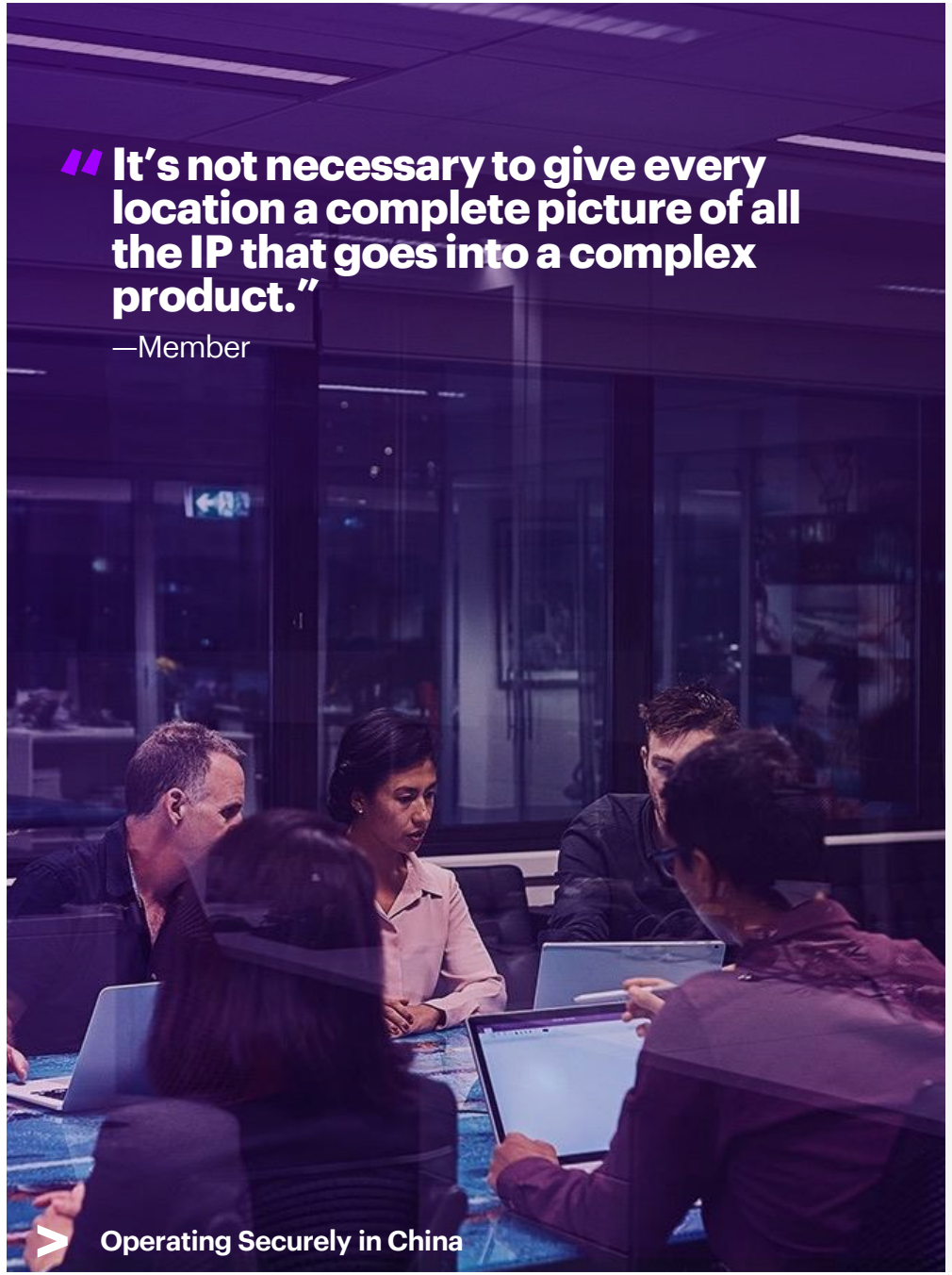
In that environment, the best approach is to focus on the basics and keep options open. CISOs need to understand the enterprise’s China business strategy. They should work with the rest of the business to find the right balance between flexibility and efficiency and identify where the most critical data and processes fit on that spectrum.

A subject matter expert added that CISOs need to add to their list of responsibilities monitoring geopolitical tensions and shifting national alignments (i.e. Brazil and China)



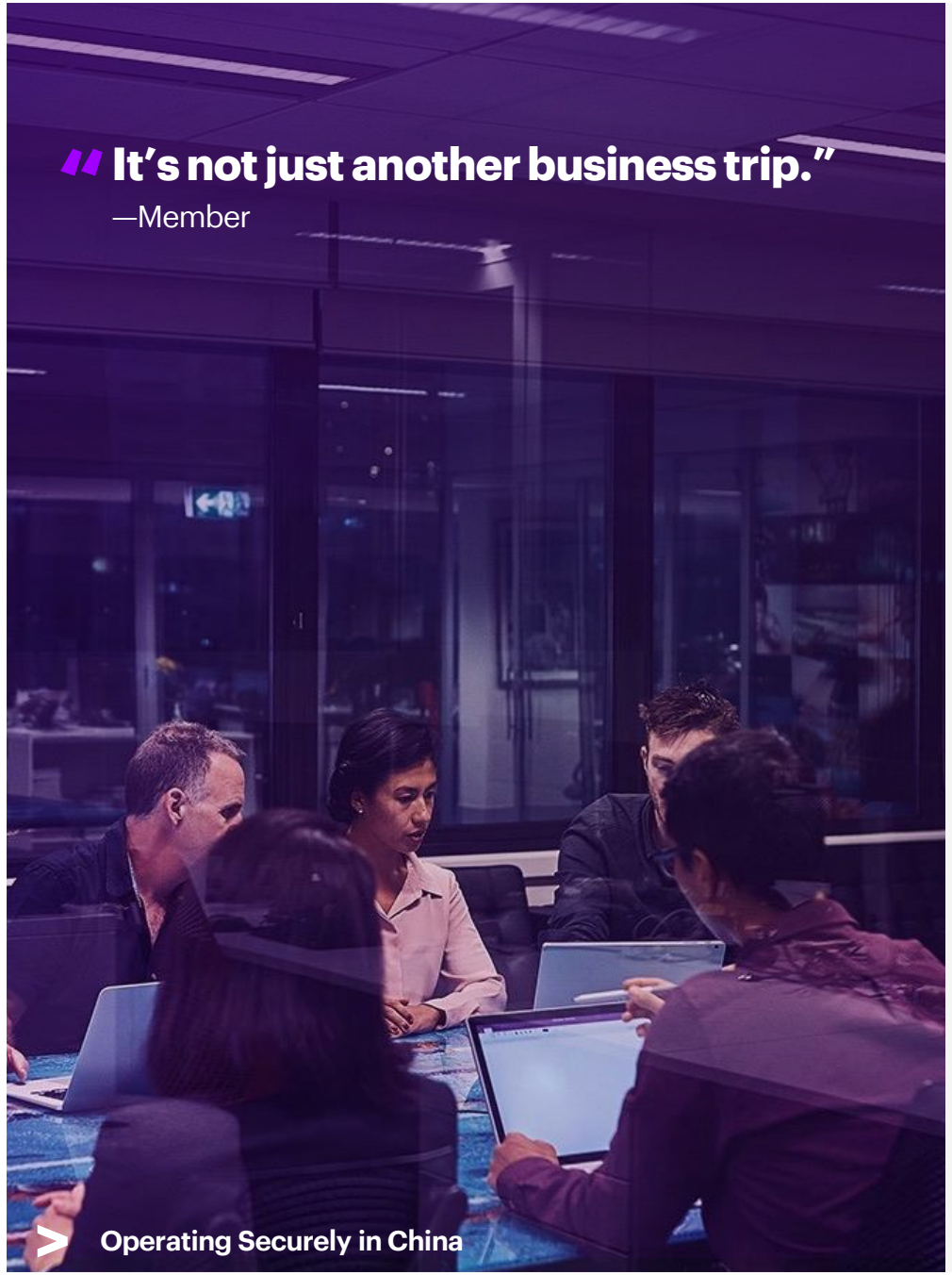
Regulatory compliance best practices

- Be best friends with local legal counsel. Corporate legal support is likely insufficient for working on the ground in China.
- Get to know the regulators. A global CISO said: “Staying close to your local Chinese regulators can save you a lot of trouble.”
- A “wait and see” approach may be best. A SME said that because of regulations are evolving and different regulators have different ideas about compliance, many enterprises are monitoring trends carefully before making significant investments in data security and personal information protection.
- Conduct “Dawn Raid” scenario planning. Prepare for regulatory inspections. Know how to react, who should be involved and what questions or actions (like seizing assets) to anticipate. Protect employees from regulatory pressures. “It can be very hard for a local Chinese IT professional to say ‘no’ if the regulators start asking questions,” said a CISO.



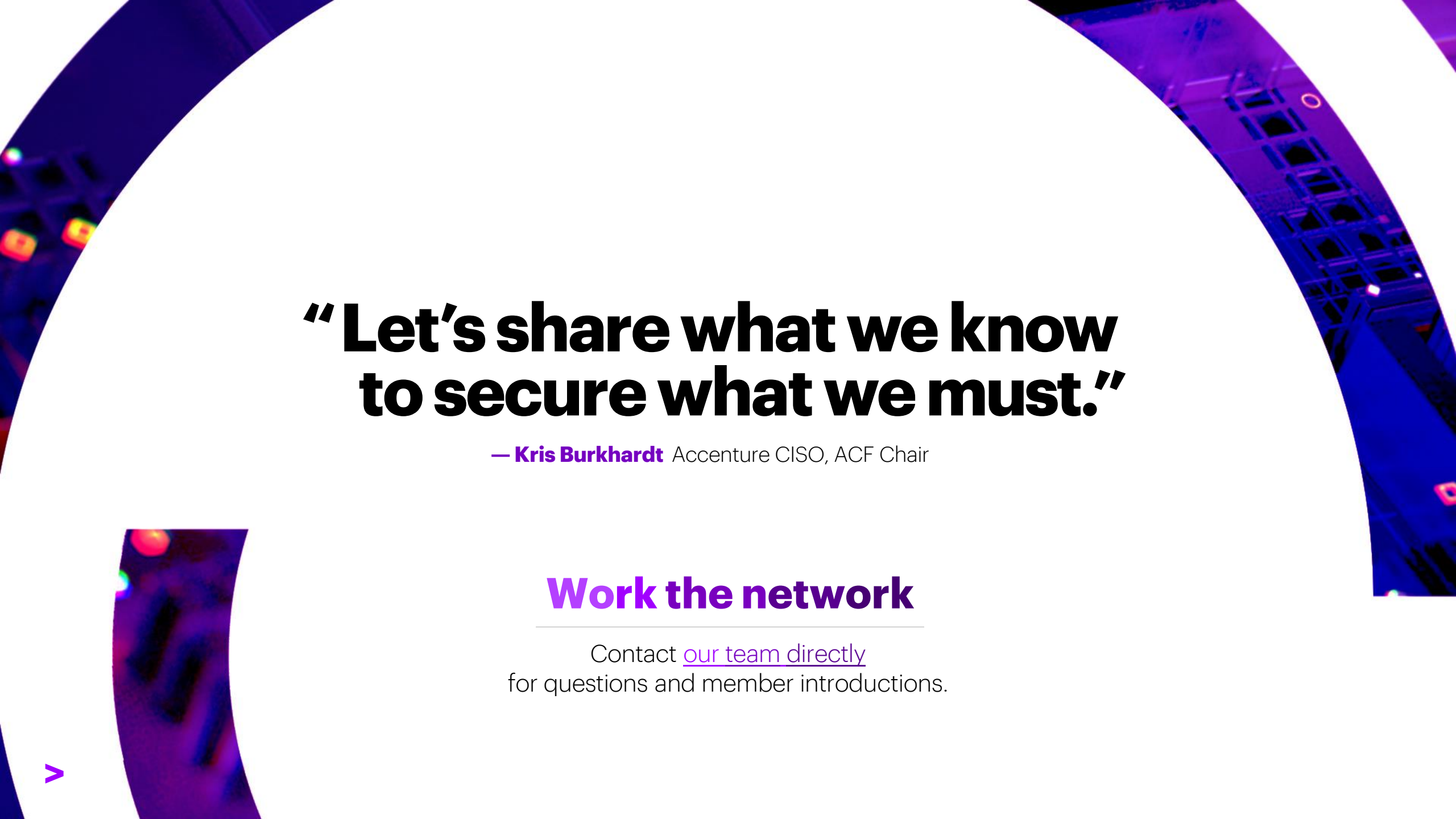
Data security best practices

- Managing insider risk should be a high priority. For example, employment contracts should include language specific to cybersecurity practices.
- “Lighten your footprint.” Minimize access to intellectual property. Consider segmenting the tech stack by creating “China for China” systems that are firewalled from other enterprise assets. Carefully control who has systems access and deploy a zero-trust model.
- Segment intellectual property within China. “We engage in what we call compartmentalization. We have operations in several Chinese cities but those locations are only given access to IP specific to their operations,” said a CISO. “It’s not necessary to give every location a complete picture of all the IP that goes into a complex product.”
- Be skeptical about relying on global data policies and systems to thwart Chinese threat actor behavior.
- Find a balance of flexibility and efficiency that’s right for your data and your enterprise. People, processes, policies and technology all contribute to maintaining that balance.



Data security best practices (cont.)

- Create partitions. Know your data, where it comes from and who has access to it. A CISO said that separate “air pockets” to store data about Chinese citizens. Another said: “We have deliberately partitioned our networks. If we had to cut off a Chinese operations network, we can do that.”
- Conduct scenario planning that accounts for geopolitical uncertainty. For example, a SME asked: “What impact would an escalating conflict between mainland China and Taiwan have on your operations, or your supply chain?”
- Tap into the pool local cybersecurity talent. A CISO suggested that Shanghai was a rich source of talent but she added that English speaking was a mandatory requirement at her Chinese cyber operations.
- Create a technology travel kit for employees working China. “It’s not just another business trip,” said a CISO. While that CISO reported receiving some pushback from executives who wanted to use their traditional tools, high-risk and medium-risk “travel kits” relying on VPN connections and secure third-party access to a virtual work station and resources are now mandatory.



“Let’s share what we know to secure what we must.”

— **Kris Burkhardt** Accenture CISO, ACF Chair

Work the network

Contact our team directly
for questions and member introductions.

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 738,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities. 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. Visit us at accenture.com/security.