Geopolitical Impacts on the Global Attack Surface

Accenture Cybersecurity Forum
Global Executive Leadership Network

13 April 2023
Session Summary

From the Accenture Leadership

Russia's invasion of Ukraine a year ago may have heightened awareness in some quarters of the impact geopolitical disruption can have on cyber defenses. However, ACF members have long been aware of nation-state threat actors and the risks they pose to the enterprise. The challenge now is guiding management to make fact-based decisions that strengthen defense posture and enable the flexibility required to face new threats.

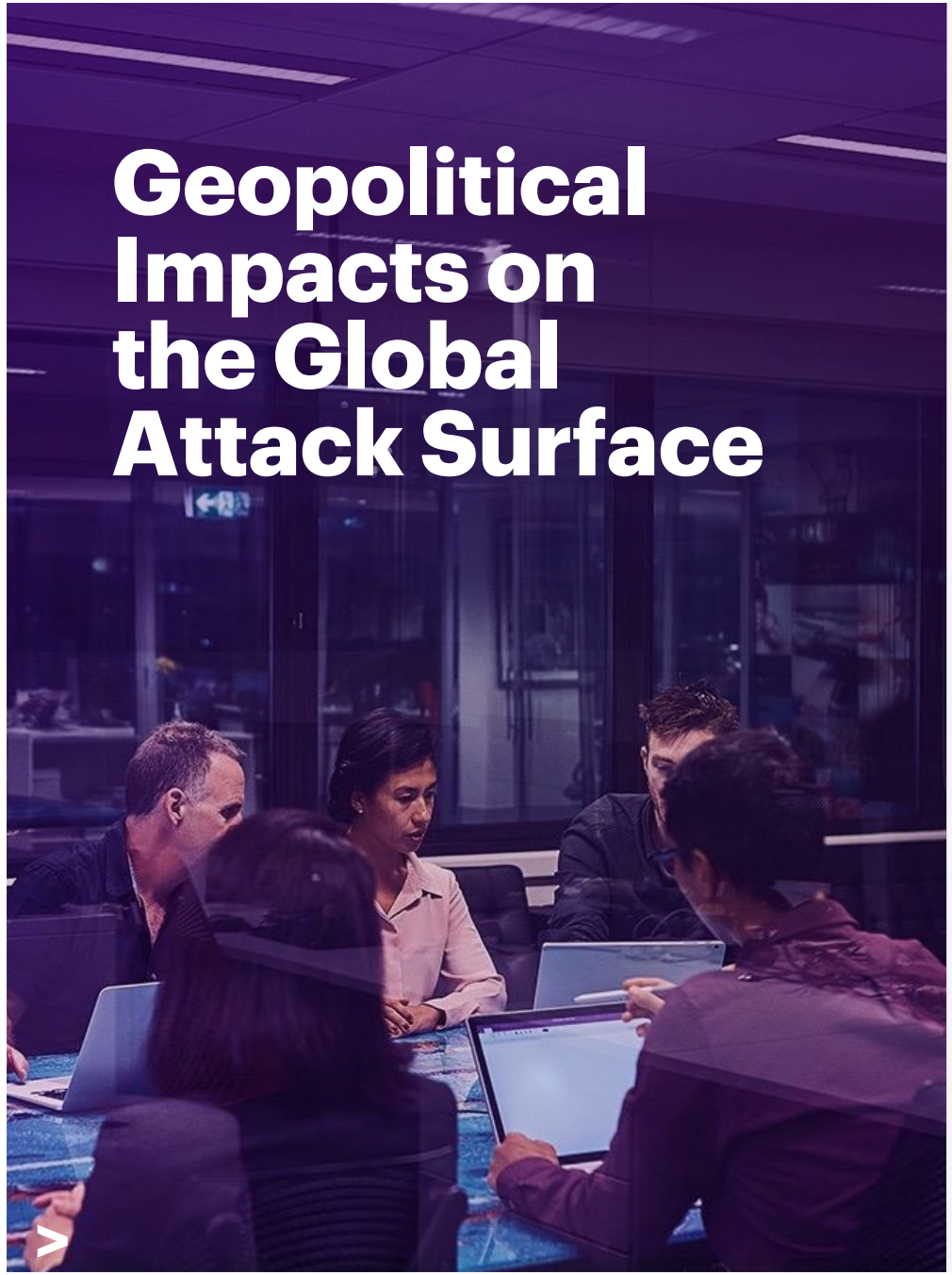
Our guest subject matter expert, a former government official, offered practical insight and prompted important questions from the Forum membership. We thank them for their participation..

Thank you also to all those who participated in the roundtable discussion. We hope you find the perspectives and best practices that emerged from the conversation help you and your enterprises thrive despite an increasingly hostile geopolitical threat environment.

Cheers,

Paolo Dal Cin
Accenture Security Global Lead
ACF Executive Sponsor
LinkedIn

Kris Burkhardt
Accenture CISO
ACF Chair
LinkedIn



Geopolitical Impacts on the Global Attack Surface

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “Geopolitical Impacts on the Global Attack Surface,” on April 13, 2023. The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “Geopolitical Impacts on the Global Attack Surface,” on April 13, 2023. The event featured a guest subject-matter expert with deep government cybersecurity experience.

Forum members have told us that they require an awareness of and sensitivity to geopolitical matters ranging from the conflict in Ukraine to tensions in China, Taiwan and Iran. What are the potential impacts of geopolitical tensions on the global attack surface? What practices should CISOs consider in this risky environment?

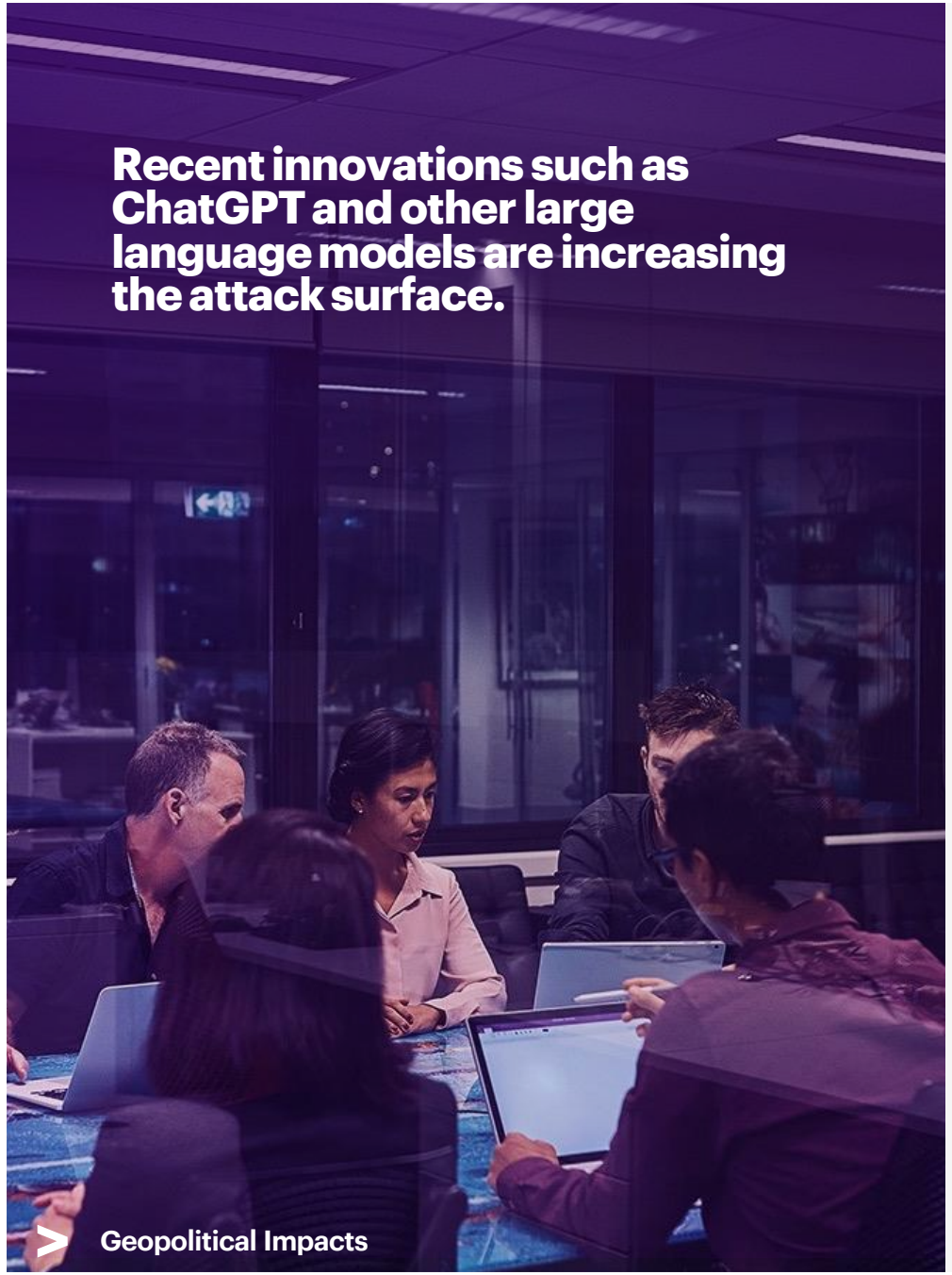
This roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers, nor participants, is revealed.

In this summary:

Balancing efficiency with flexibility, optionality and agility

Forum members noted that while efficiency has traditionally been a top CISO priority, geopolitical shifts are changing the rules of the game. The guest subject-matter expert (SME) said that threats from foreign nations and the risks to technology have never been this active. Agility—the ability to respond to determined threat actors, shifts in international relationships (i.e. Ukraine and Russia, China and Brazil) and the impact on global computing platforms—are driving CISOs to explore new ways of responding to a dynamic, risky environment.

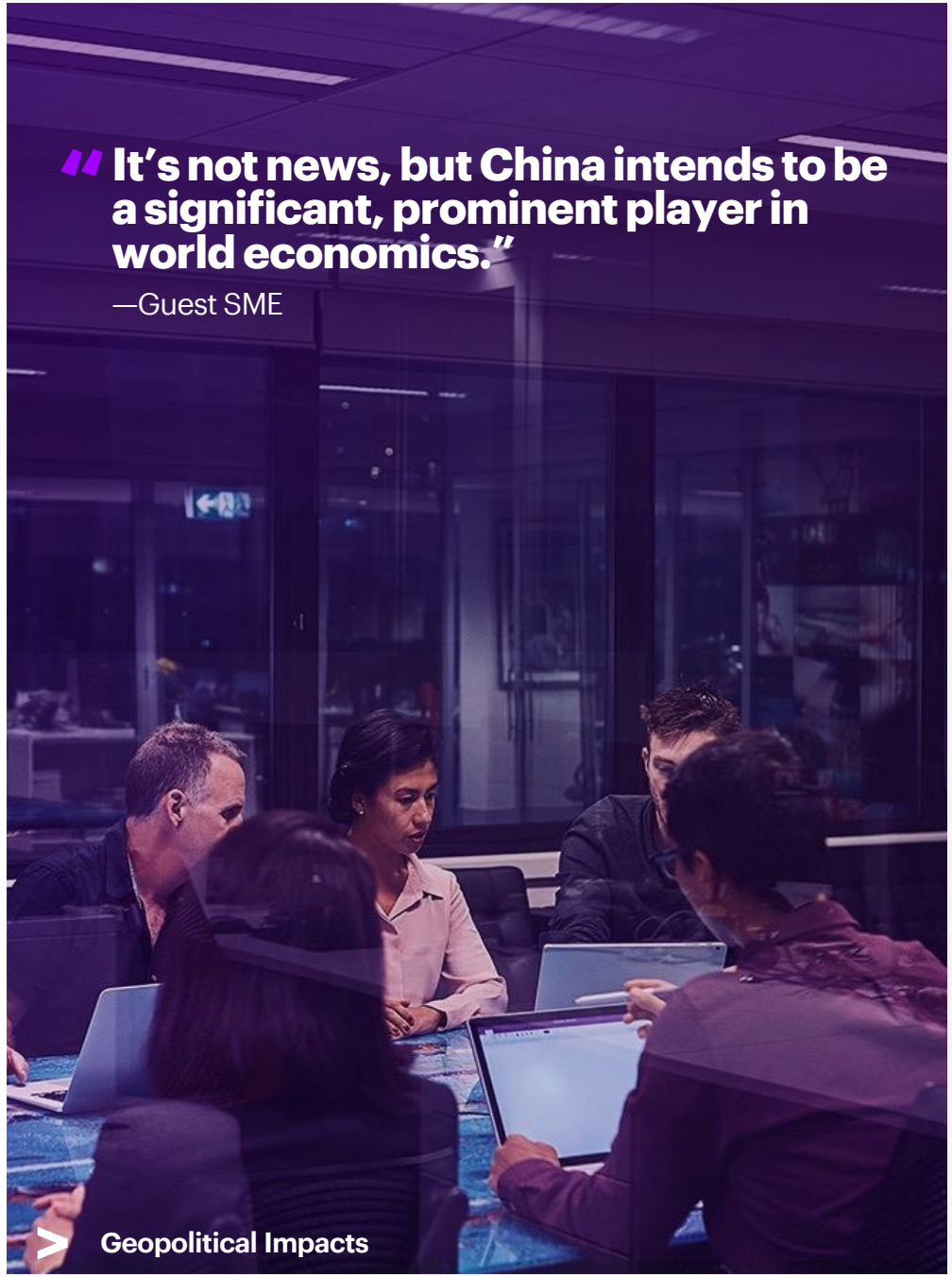
The challenge for CISOs is amplified by news coverage and threat assessment reports seen by senior management and board members. Another subject-matter expert said that a consistent, structured approach to analysis and communication is essential to keeping management focused on the issues that matter most to the business.



Balancing efficiency with flexibility, optionality and agility (cont.)

On the technical front, the guest SME said that recent innovations such as ChatGPT and other large language models are increasing the attack surface. “Threat actors are actively exploring how to exploit these innovations for their own gain, whether it be for IP theft, industrial espionage or most notably, domestic surveillance.”

Several Forum members said that the cloud offers elasticity that is valuable in responding to geopolitical threat requirements such as being forced to exit a country in 48 hours.

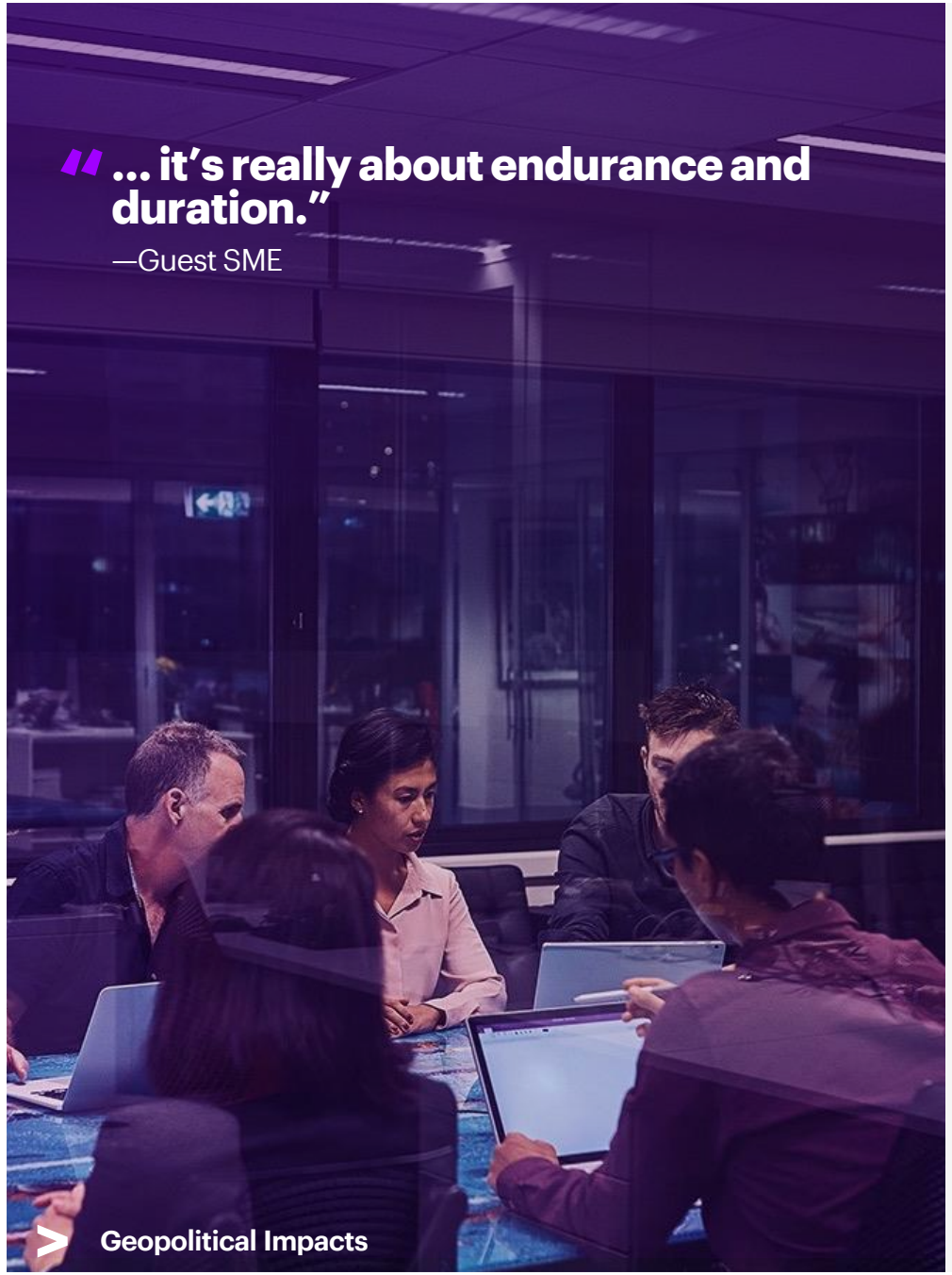


What is China planning?

The guest SME and Forum members acknowledge that China has been playing “the long game” for at least 15 years, which is a challenge for commercial enterprises with shorter planning horizons and more immediate performance expectations. “It’s not news, but China intends to be a significant, prominent player in world economics,” the guest SME said. The Chinese government is particularly strong in wielding “soft power,” such as controlling a major commercial port in Monterrey, Mexico or acquiring farming operations in Australia. This strategy will continue to pose threats.

While a Chinese invasion of Taiwan is not inevitable, there is speculation that the Mainland will take aggressive action in 2027. That gives all of us time to prepare, to create a robust risk registry and conduct creative scenario planning. The guest SME added that CISOs need to be thinking about threats other that an actual attack—a naval blockade, supply chain disruptions and IP theft, and espionage. That gray area is much more important now.

The guest SME said: “You’ve got a target on your back if you’re one of China’s 10 priority sectors” (i.e. information technology; electric vehicles; aerospace/aeronautical; ocean engineering/high tech ships; railway; numerical control tools/robotics; power equipment; new materials; biological medicine/medical devices; agricultural machinery. Source: Made in China 2025 Strategy). “The Chinese will be going after your intellectual capital and looking for opportunities for disruption.”

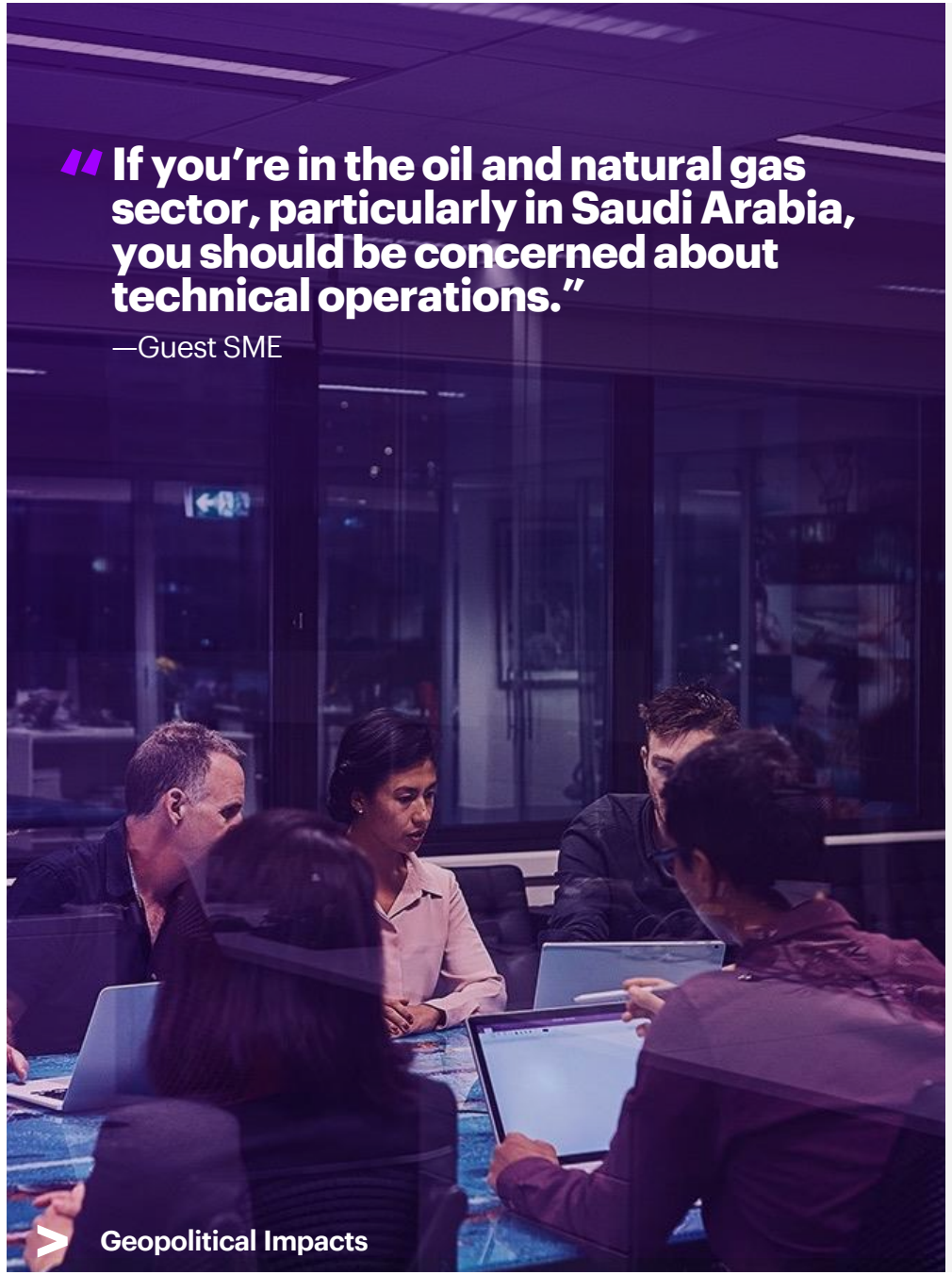


Keeping an eye on Russia

During the first Russian attack on Ukraine in 2014, the response from the West was muted. The SME said: “Now you look forward, and we are still in the early days of this conflict, but one of the lessons learned is that this is going to be a years-long event, so it’s really about endurance and duration.”

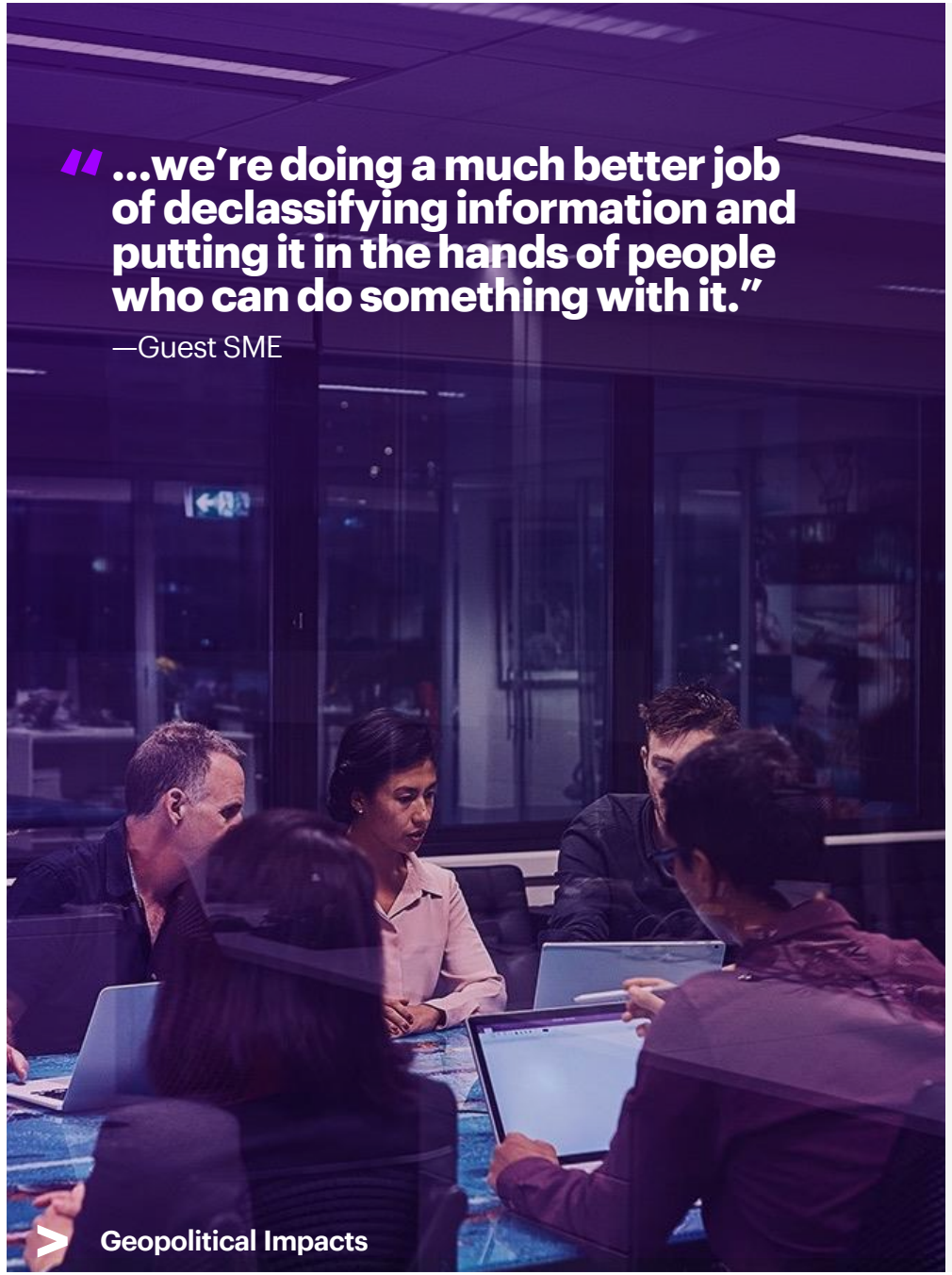
The fact that we haven’t seen a significant cybersecurity incursion from Russia may be a good news story, or it may be attributable to the fact that enterprises are playing better defense. There is speculation that Russia used 10 years of malware in a matter of months. In a recent interview, Andrew Boyd, director of the CIA’s Centre for Cyber Intelligence, said the integration of kinetic and cyber attacks relies on speed, intensity and control and if one of those is missing, effectiveness is minimized. Russia may be struggling in that respect.

The guest SME speculated that China’s relationship with Russia may be a way to divert attention from China’s intentions as that country tries to drive a wedge between allied nations. French Prime Minister Macron’s recent visit to China is an example of that intention.



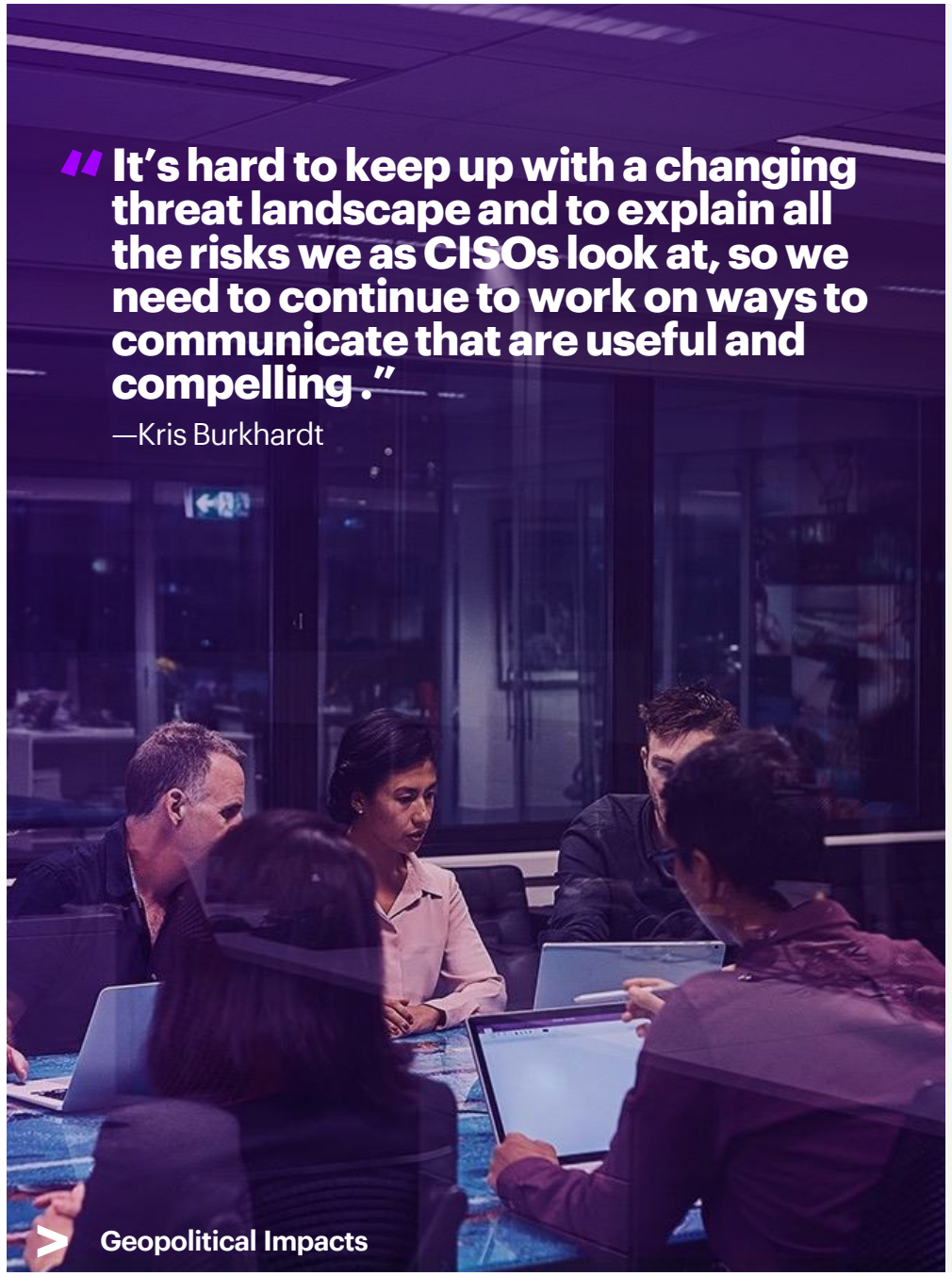
Iranian intentions

Like Russia, the guest SME said, Iran does a pretty good job of mixing information and technical operations and looking for psychological and psychosocial attacks to provoke civil unrest.” They added: “If you’re in the oil and natural gas sector, particularly in Saudi Arabia, you should be concerned about technical operations. A few years ago, they were using drones to attack pipelines, for example.”



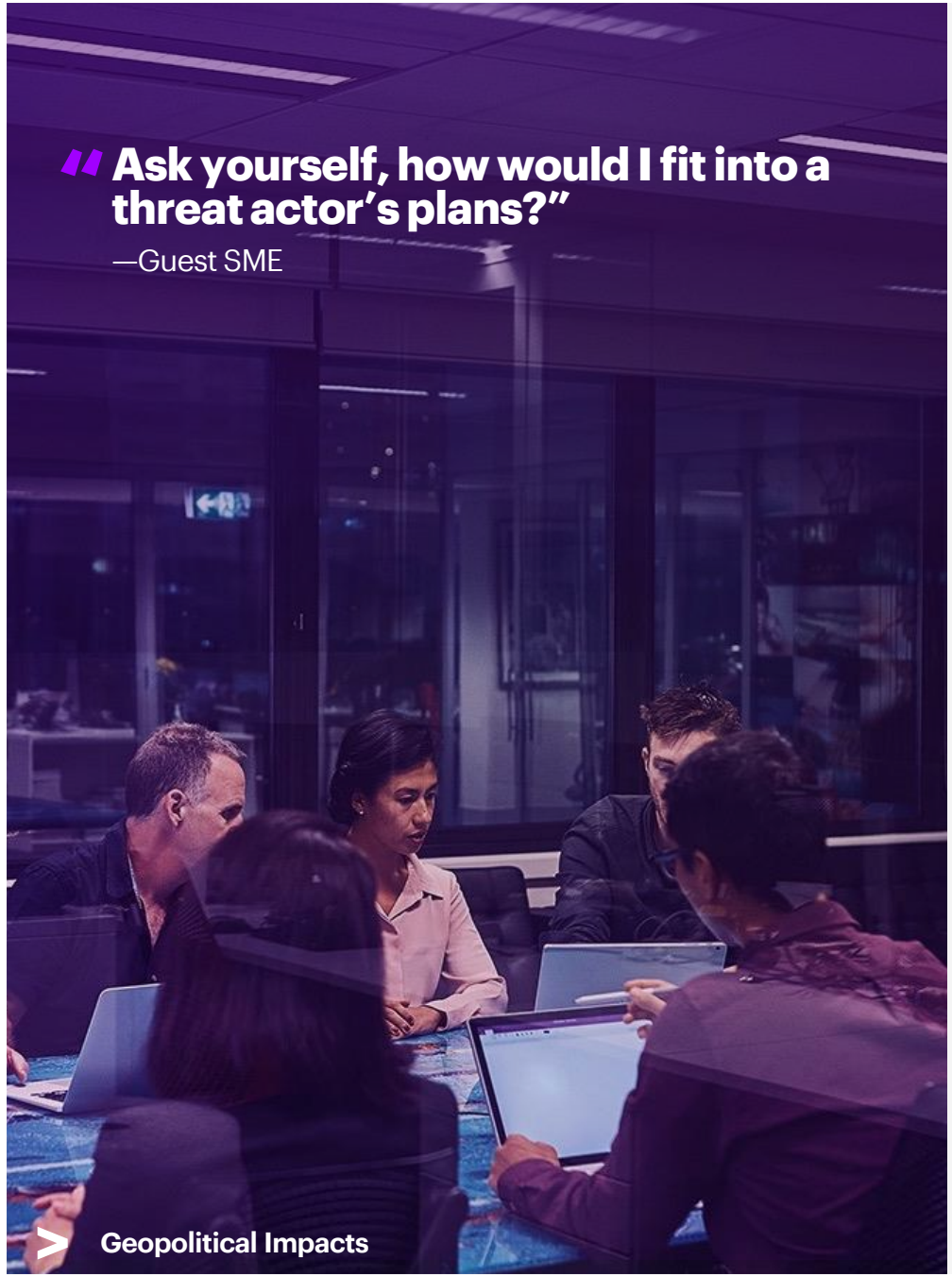
Are the "Five Eyes" up to the task?

Regarding the Five Eyes Alliance (the US, UK, Canada, Australia, New Zealand) the guest SME said: "If you look back the last five years, they are doing a much better job of declassifying information and putting it in the hands of people who can do something with it. Now we need to focus information on an executive level of understanding so that the CISOs on this call can go into the boardroom and the C-suite and say in layman's terms, 'This is what they are trying to tell us.'"



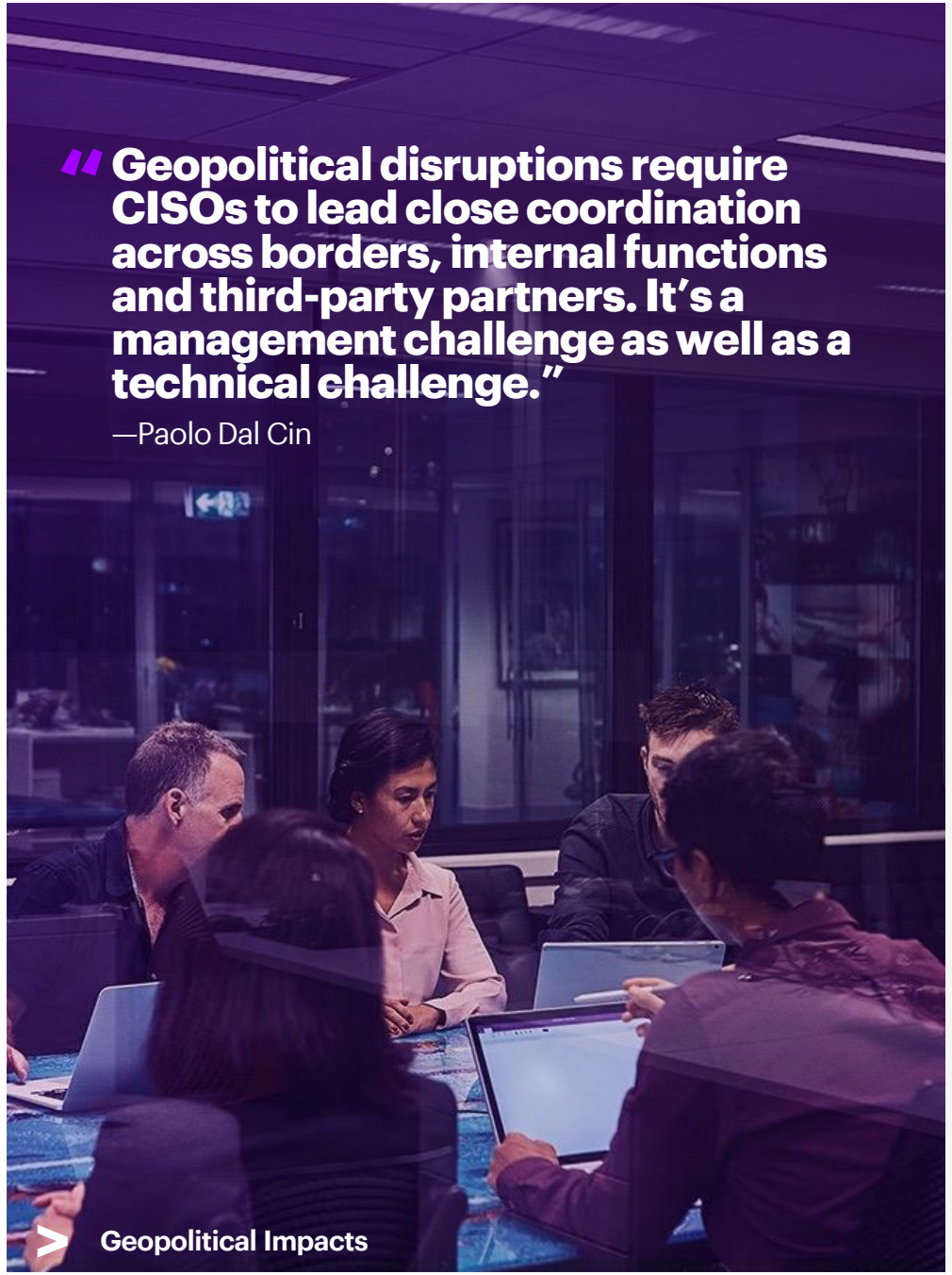
Strategic best practices

- “My biggest concern,” said the guest SME “is the volume of requests coming from the C-suite. Those demands put you in a really reactive role, yet the requirements coming down the road, such as from the SEC, require a much broader set of skills. When a flood of requests come in from the board, the CISO has to be strategic, not reactive, or you’ll be putting out fires forever. The question becomes how do I become a more strategic CISO? You need to work with your InfoSec team and find the time—say two hours on a Friday afternoon—to think about where you want to be in two to three years and how to communicate new requirements.”
- Develop a plan to maintain freedom of operations in high-risk countries, accounting for an indigenous workforce and the need for segmenting assets throughout the tech stack.
- Establish repeatable processes for analyzing risk and responding to attacks, such as ransomware. “If you can consistently defend against ransomware attacks, you’re 80% to 90% there.” said the guest SME.



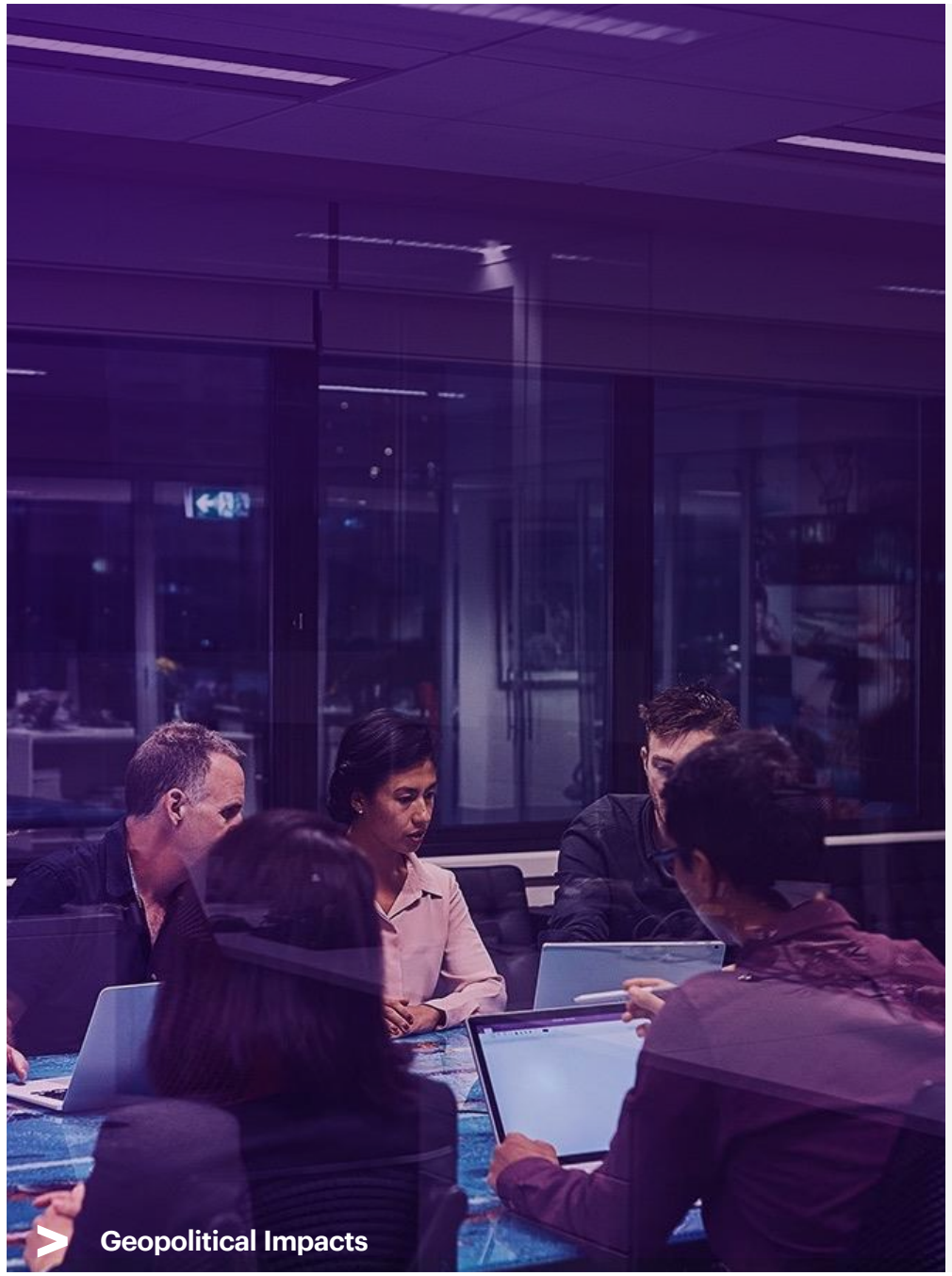
Strategic best practices (cont.)

- Explain cyber risks for the board at the Harvard Business Review level. A layman’s scorecard that quantifies cyber risks that are relevant to the enterprise and the business can be useful but there is no clear consensus on what that scorecard should look like.
- Consider how your enterprise’s strategy or actions could inadvertently be leveraged by an adversary. “Ask yourself, how would I fit into a threat actor’s plans?” said the guest SME. “For example, how could you be a target to disrupt logistics in a shooting war?”
- Strike the right balance in focusing on the elements of cybersecurity. A Forum member proposed “the 1/3rd rule: 33% strategic planning, thinking; 33% "security by design" for company R&D; and 33% improvement in Security operations.



Tactical best practices

- “It all starts with scenario planning and building your risk registry so you know where things can fail,” said the guest SME. “Then you can build the capabilities and resources on top of that—to improve resiliency, get back up and running more quickly.”
- Focusing on the cybersecurity basics and getting tech hygiene right is a key to resiliency from inevitable attacks. “I wouldn’t spend a lot of time on defending AI, because the basics still matter,” said the guest SME. “You can’t defend against a ransomware event or an advanced persistent threat from China or Russia but they are relying on the same trick bots, so don’t forget the basics.”
- Management’s questions about issues in the news should be leveraged as learning opportunities.
- Use tabletop exercises with the board and other business leaders to specifically expose the “gray space” where the enterprise could be exploited.
- The biggest risk in an event may be the diffusion of responsibility. Stress test your playbook. “Never assume that someone else is doing the right thing,” said the guest SME. “Confirm that it is actually happening.”

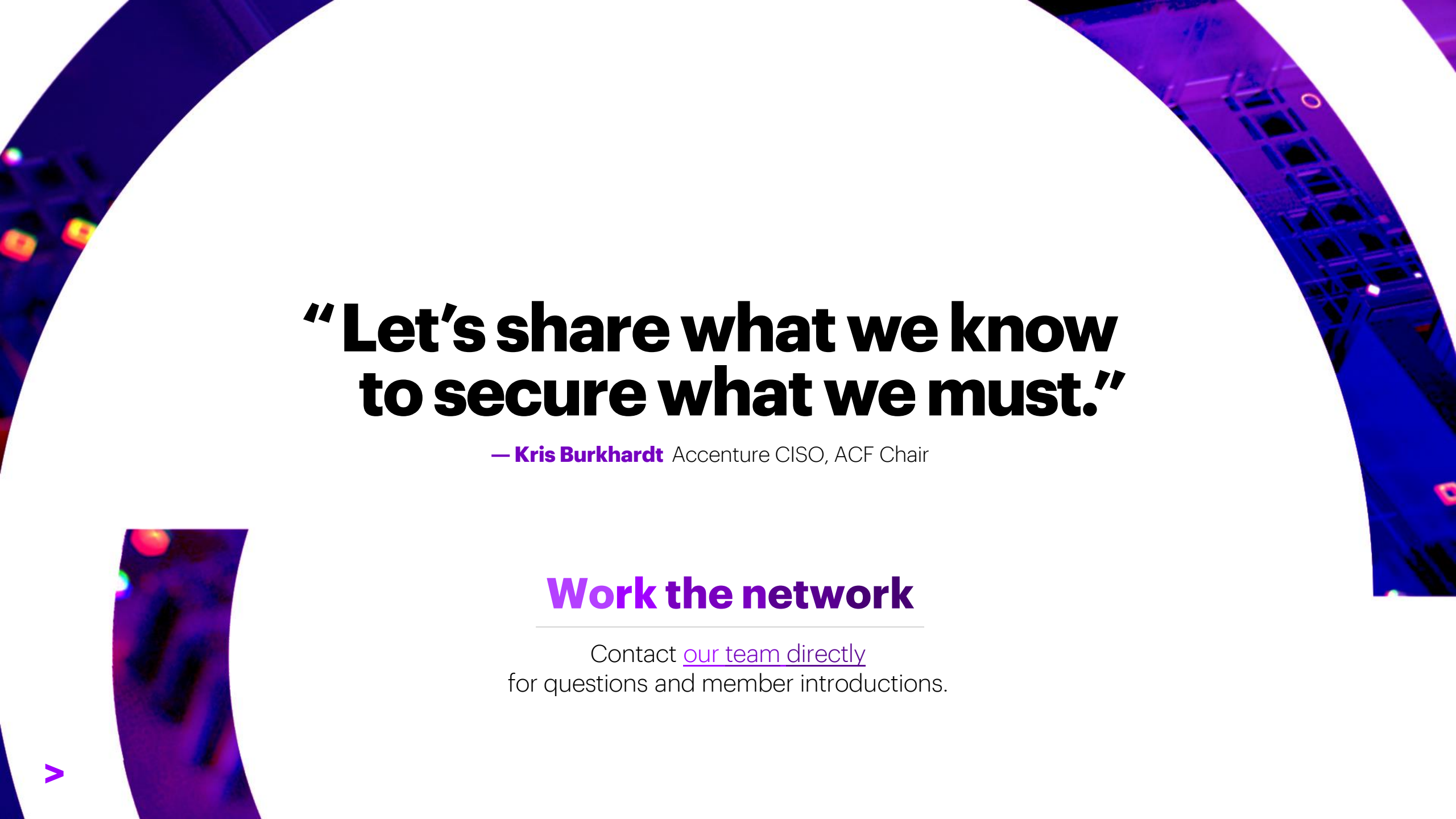


For additional information

The guest SME pointed to two US government sources for more detail about the cyber threats posed by geopolitical upheaval:

- An interview with Andrew Boyd, director of the CIA's Centre for Cyber Intelligence (https://risky.biz/andrewboyd/).
- The Lawfare Podcast: Rob Joyce, NSA Director of Cybersecurity (https://www.lawfareblog.com/lawfare-podcast-rob-joyce-nsa-director-cybersecurity)

In addition, a Forum member recommended the following Washington Post article, "An emboldened China hones its craft and gets more aggressive in cyberspace."



“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.