A Global Perspective: The New U.S. White House Cybersecurity Strategy

Accenture Cybersecurity Forum
Global Executive Leadership Network

8 June 2023
Session Summary

From the Accenture Leadership

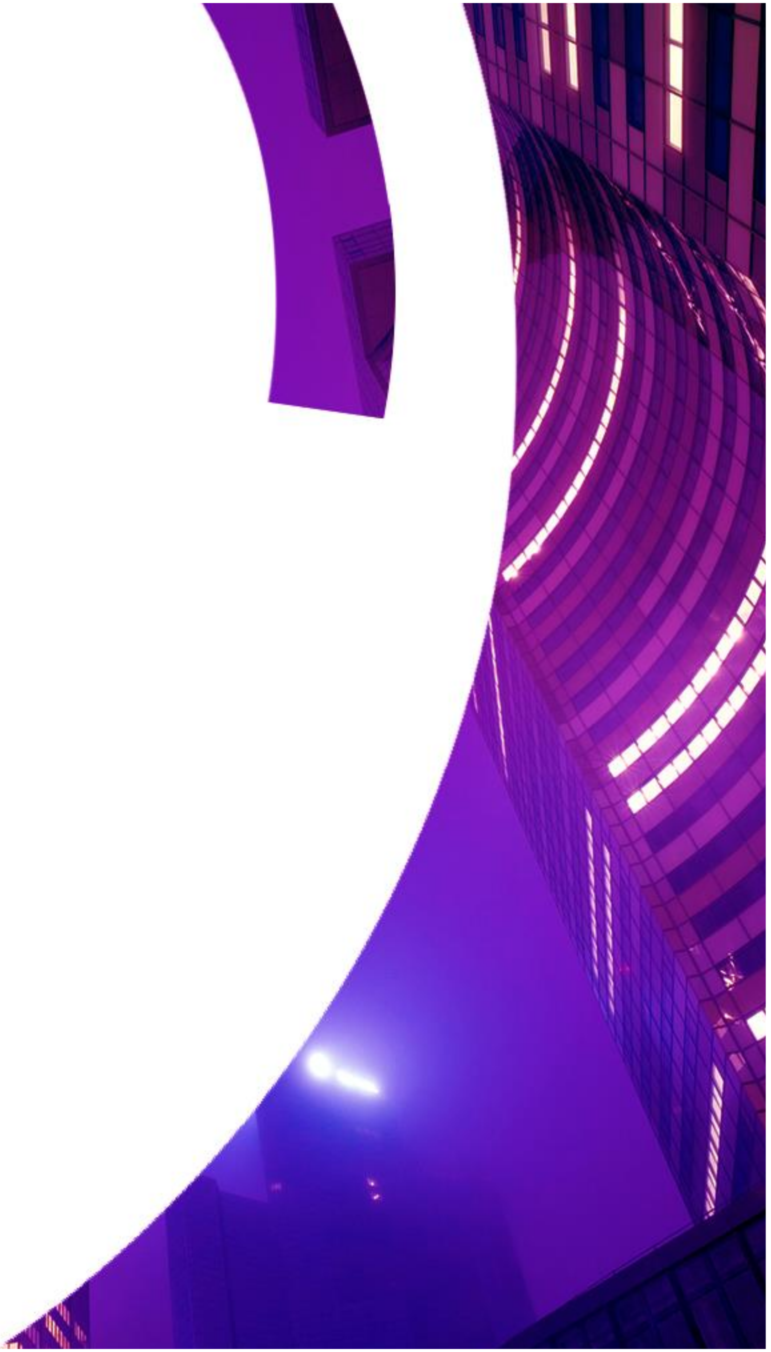
The U.S. federal government and other nations are proactively promoting cybersecurity best practices at the national, regional and industry sector levels. Our guest subject matter expert from the White House Office of the National Cyber Director joined ACF members from around the world to share perspectives on progress and challenges in driving public/private partnership cyber strategy.

Thank you also to all those who participated in the roundtable discussion. We hope you find the perspectives that emerged from the conversation useful as you refine your own cybersecurity strategy.

Cheers,

Paolo Dal Cin
Global Head of Accenture Security
ACF Executive Sponsor
LinkedIn

Kris Burkhardt
Accenture CISO
ACF Chair
LinkedIn



A Global Perspective: The New U. S. White House Cybersecurity Strategy

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “A Global Perspective: The New U.S. White House Cybersecurity Strategy,” on June 8, 2023.

The event featured a senior White House Office of the National Cyber Director (ONCD) subject matter expert.

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:

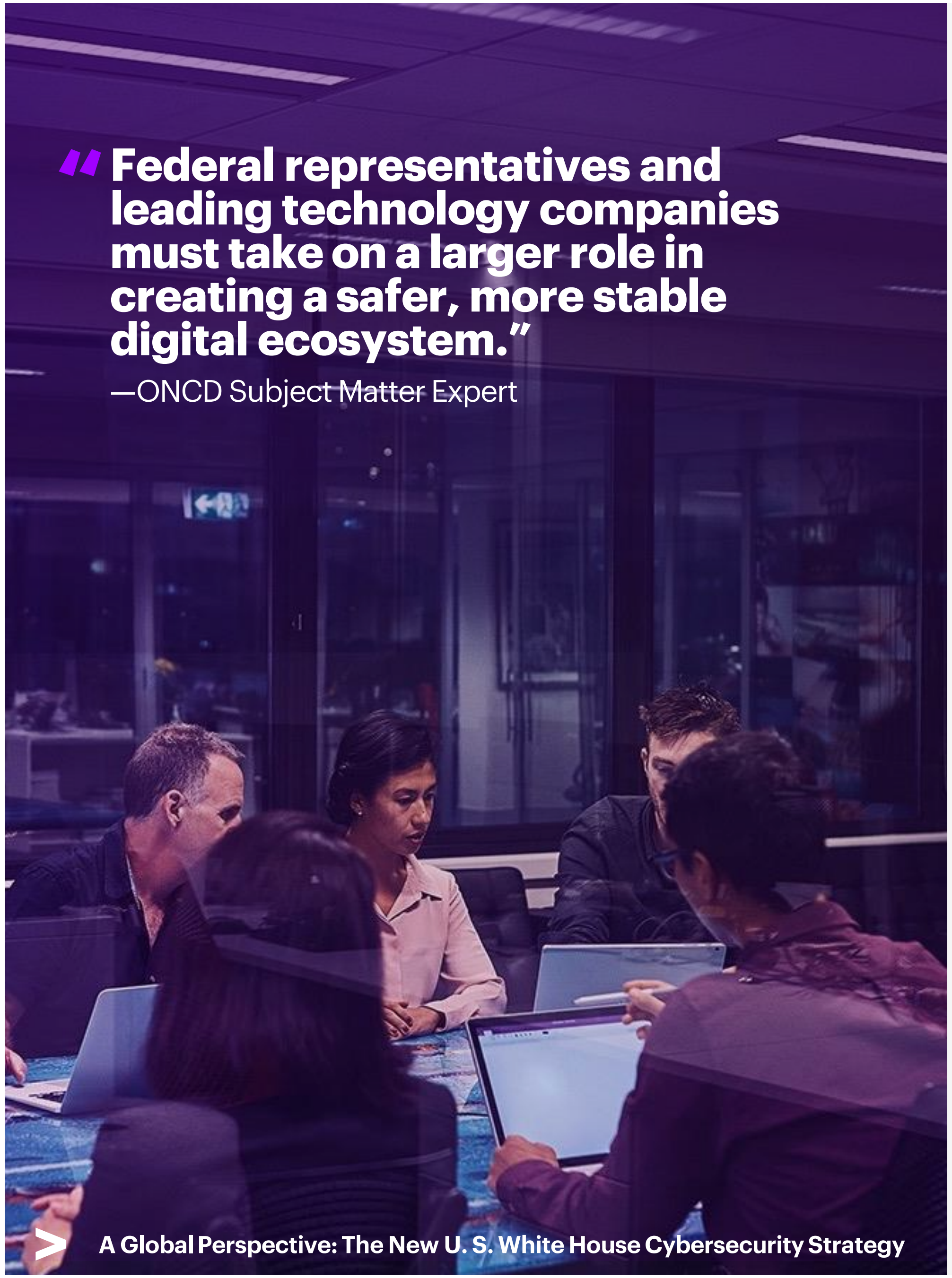
> “ONCD’s mission is to advance national security, economic prosperity, and technological innovation through cybersecurity policy leadership.”
>
> —ONCD Subject Matter Expert

Evolving federal cybersecurity priorities

Established in January, 2021, ONCD’s mission is “to advance national security, economic prosperity, and technological innovation through cybersecurity policy leadership. In carrying out its directive, ONCD works closely with White House and interagency partners, as well as with all levels of government, America’s international allies and partners, non-profits, academia, and the private sector, to shape and coordinate federal cybersecurity policy.”

The ONCD subject matter expert said that the office is focused on four priorities:

1. Federal cohesion—Driving a positive, forward-looking strategy across U.S. federal agencies.
2. Public/private collaboration—Particularly implementing a national information-sharing strategy across the public and private sectors.
3. Current and future resiliency—Pushing forward initiatives across all available avenues in order to increase present and future resilience, ensuring our workforce, technologies, and organizations are fit for purpose today and future-proofed for tomorrow
4. Statutory funding authority alignment—Aligning resources to aspirations by ensuring U.S. departments and agencies are resourcing and accounting for the execution of cyber initiatives, assets, and talent entrusted to their care, and considering all possible future such requirements.



"Federal representatives and leading technology companies must take on a larger role in creating a safer, more stable digital ecosystem."

—ONCD Subject Matter Expert

Pillars to increase cyber resilience

In broader terms. the subject matter expert (SME) said a shift was required to establish a defensible, resilient digital ecosystem across sectors and borders.

Today, individual cyber hygiene is important and personally laudable, but systemically inadequate. Critical services for millions can be imperiled because of a single person's failure to recognize a phishing attempt. The SME said Federal representatives and leading technology companies must take on a larger role in creating a safer, more stable digital ecosystem.

The SME also identified five "pillars" where the Federal government can use its authority to increase cyber resilience:

1. Making critical Infrastructure more resilient.
2. Leveraging agency authority to disrupt criminal operations.
3. Offering incentives for market forces to promote R&D and adoption of best practices such as security by design and zero trust architecture.
4. Promoting investment in technology and people.
5. Fostering international cooperation.

> “Cross-border collaboration among the private sector, national and regional policymakers is essential in countering threat actors.”
>
> — Paolo Dal Cin, Global Head of Accenture Security

Member Q&A – Pt. 1

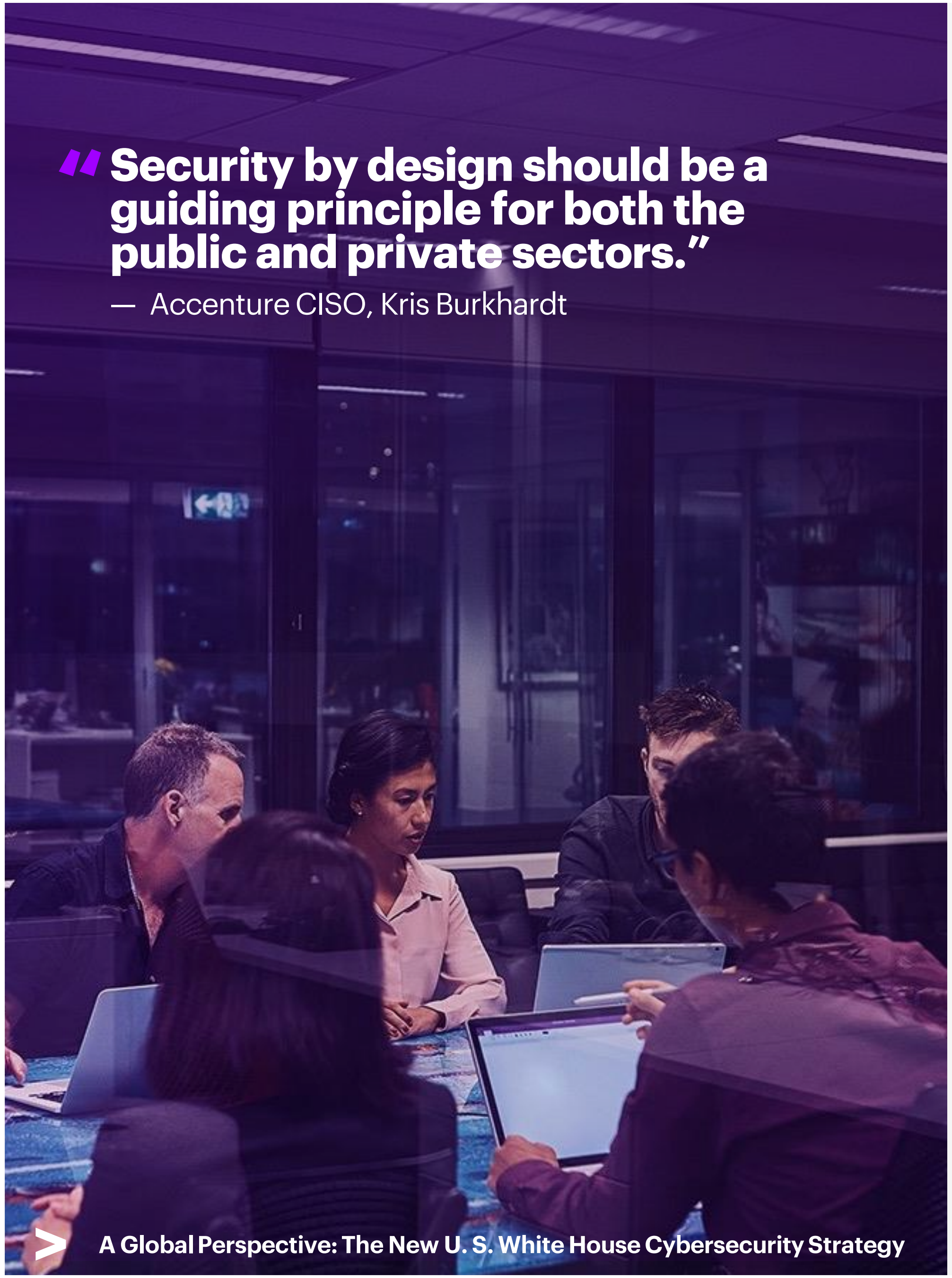
A variety of issues were raised by Forum members, including:

- **“Sand in the gears” of threat actor operations** — The SME said that tactics for disrupting threat actors will include cross-border collaboration to shut down safe havens of operation; interfering with payments, particularly crypto-currencies; and working with cloud service providers on Know Your Customer efforts to interfere with the environments threat actors are using to launch attacks.

  A Forum member with a law enforcement background added that it is important to implement cross-border operational plans to pursue criminals and make attacks less profitable.

- **Balancing security and innovation** — A CISO discussed the importance of promoting Federal policies that did not hinder software firms from delivering innovative new products.

  The SME suggested that companies consider using security and privacy as points of market differentiation. Some automakers, for example, used federal safety regulations as an opportunity emphasize the safety of their vehicles.



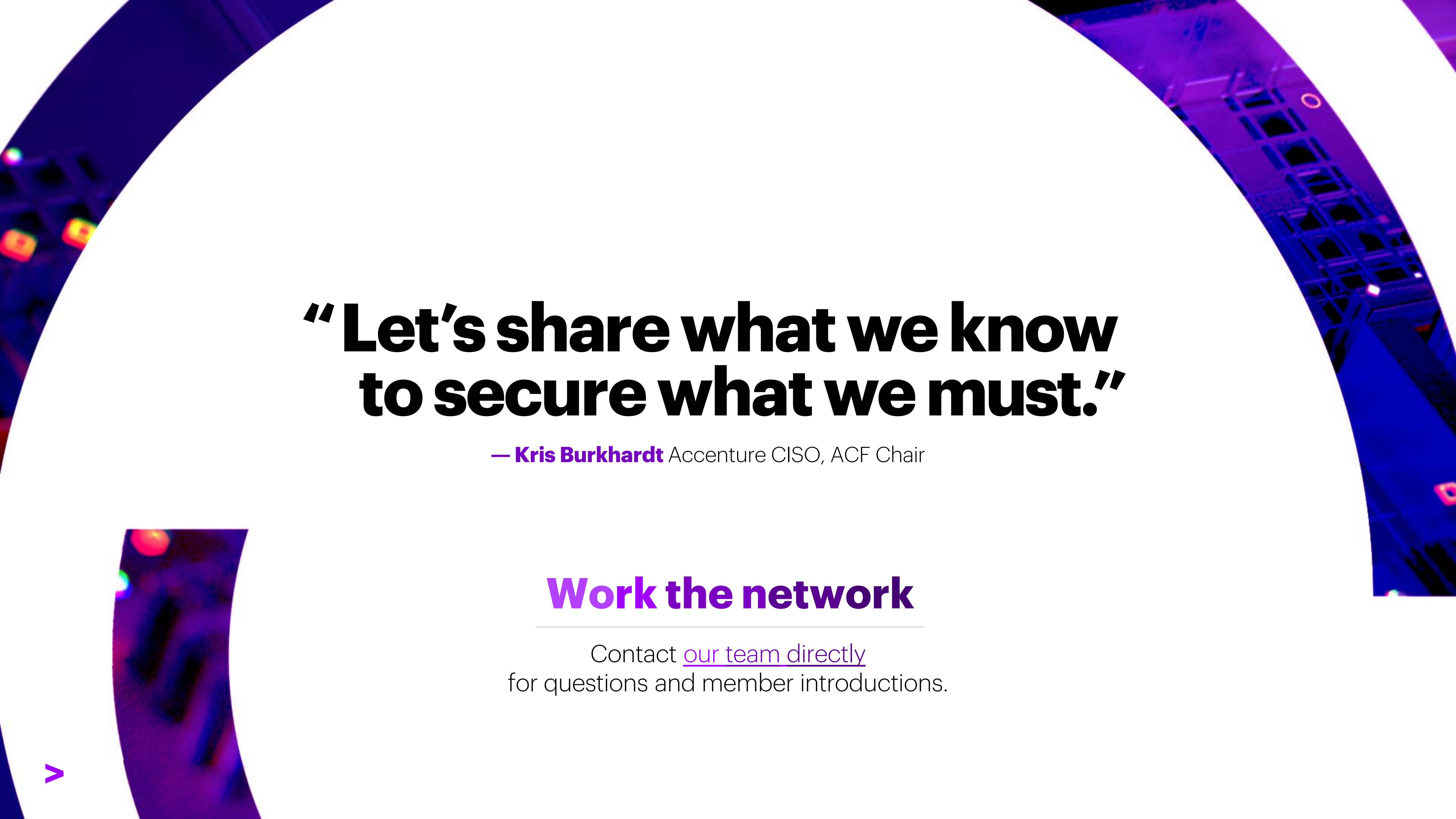
> **"Security by design should be a guiding principle for both the public and private sectors."**
> — Accenture CISO, Kris Burkhardt

Member Q&A – Pt. 2

A variety of issues were raised by Forum members, including:

- **Open source risks** — The SME said that a multi-year initiative is being developed to promote software security by design (SBD) that would leverage the NIST framework and encourage SBD curriculums in software engineer education.
- **How the private sector can contribute to ecosystem security** — The SME called for "operational intimacy" between the public and private sectors. Specific opportunities include sharing threat intelligence and mitigation experience by engaging with the National Security Agency's Cybersecurity Collaboration Center, and working with sector-specific agencies. The SME also noted the value of CISA vulnerability bulletins.
- **Acknowledging business risk** — The SME stressed the importance of a CEO mindset that cybersecurity is a capital, not an operational, expense. The SME said that CEOs they speak with have a "lightbulb moment" when they understand that threat intelligence and vulnerability assessments present a business risk. "CISOs may have seen this information, but it's news to the CEO and the board," the SME said.

  For example, sharing threat intelligence on the eve of Russia's aggression in Ukraine with senior executives worked. This conversational model for sharing bespoke threat and vulnerability intelligence may be applied again to provide a picture of risk for business and agency leadership.



“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.