Demonstrating Cybersecurity Value to the Business and the Board

Accenture Cybersecurity Forum
Global Executive Leadership Network

September 2023
Session Summary

From the Accenture Leadership

"It's hard to prove a negative," said an ACF subject matter expert. And while successfully defending against breaches is a win for the CISO and the enterprise, success can make it difficult to focus the attention of the C-suite and the board of directors on cybersecurity priorities. Investments, innovation, regulatory compliance and emerging threats need to be addressed before an attack occurs.

ACF members shared their personal experiences and practical advice for demonstrating to the business and the board how cybersecurity is delivering value to the business. It is a particularly timely topic given budget pressures, new compliance requirements and generative AI. We are also sharing a new research report, "The Cyber Resilient CEO," that underscores the strategic importance of cybersecurity.

Cheers,

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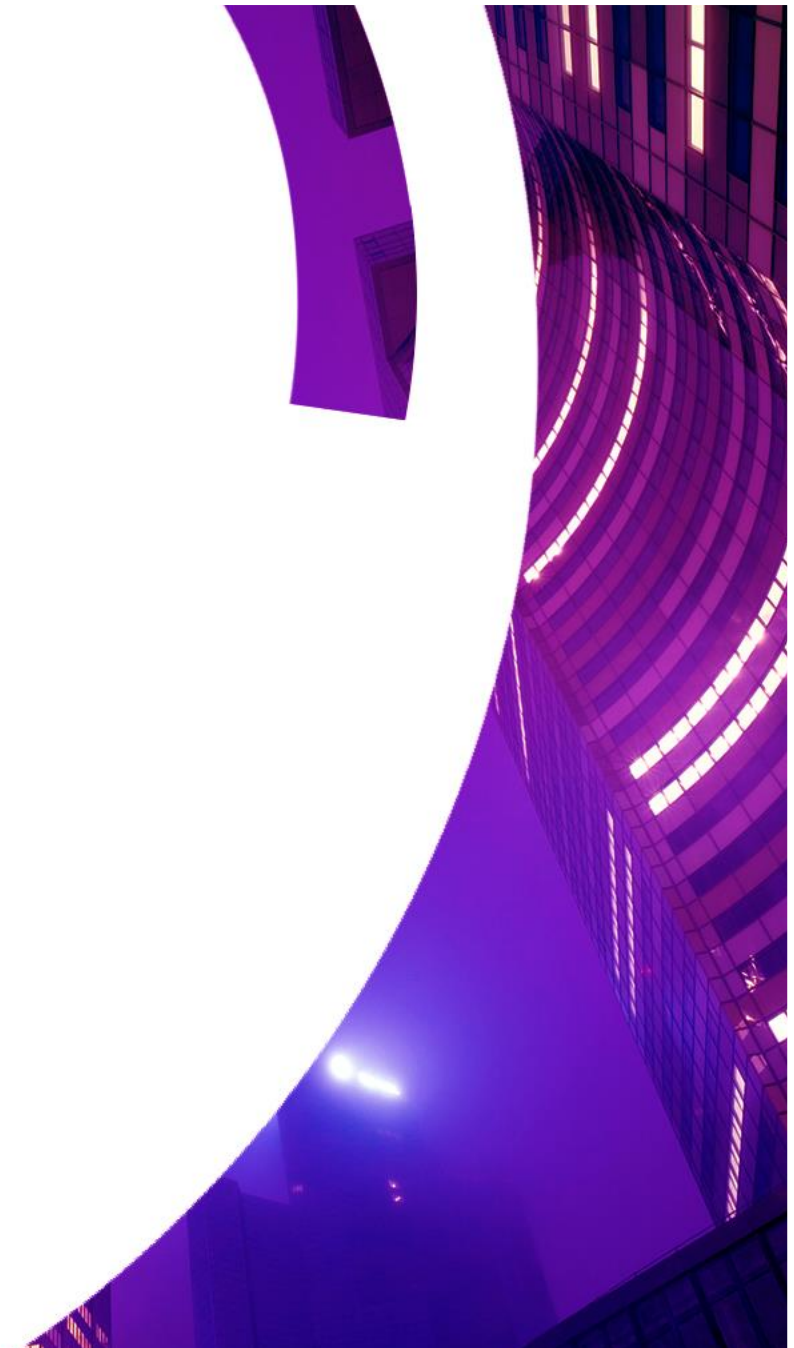Global Head of Accenture Security
ACF Executive Sponsor
LinkedIn

Kris Burkhardt
Accenture CISO
ACF Chair
LinkedIn

>

Demonstrating Cybersecurity Value to the Business and the Board

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled "Demonstrating Cybersecurity Value to the Business and the Board" on September 26, 2023.

How can CISOs best showcase the value of the security organization to the business and Board? Are there best practices? Is there a playbook? Facing rising business risks and management concerns, ACF members shared ideas for communicating most effectively.
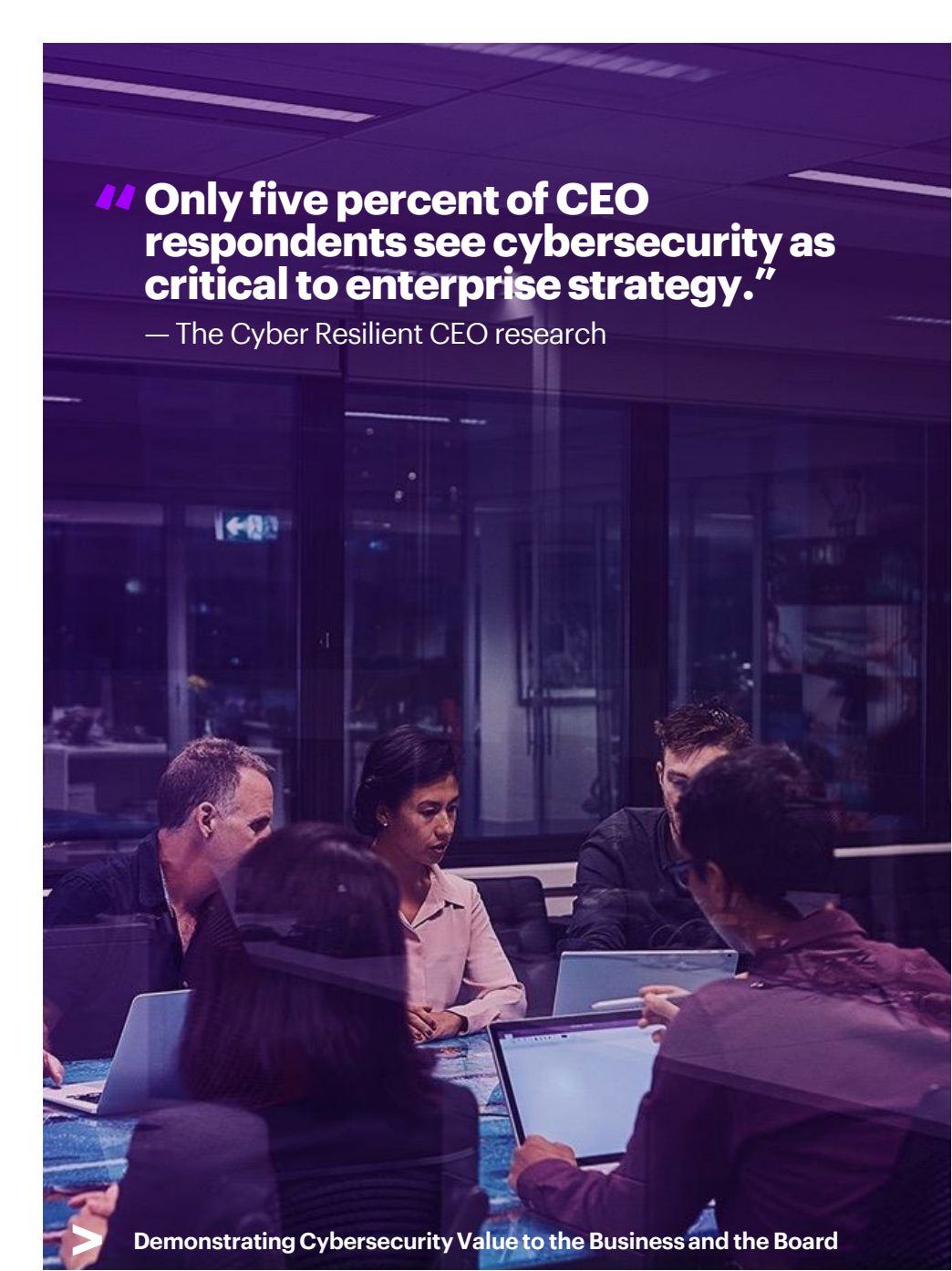
This roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers, nor participants, is revealed.

.

In this summary:

Supporting the cyber resilient CEO >

Focus on "why" in the right context >

Best practices >

Supporting the cyber resilient CEO

The subject matter expert (SME) shared key findings of Accenture's global research with more than 1,000 CEOs. Among the key findings of "The Cyber Resilient CEO" research:

- Only five percent of CEO respondents see cybersecurity as critical to enterprise strategy. These cyber resilient CEOs are taking specific steps to embed cyber support across the organization.

- More than 54 percent only focus on cyber when an episodic event occurs.

Recommendations for CEOs to become cyber leaders supported by the research findings include:

1. Embed cyber resilience from the start of business strategies

2. Establish shared cybersecurity accountability across the C-Suite. "Being CISO is not an 'alone' job," said the SME. "The CMO, the CHRO, everyone in the C-suite has an obligation to make the organization more secure. The CISO needs to be part of broadening the conversation."

3. Secure the digital core at the heart of the organization

4. Extend cyber resilience beyond boundaries and silos

5. Embrace ongoing cyber resilience to stay ahead of the curve

> **You need to align the messaging with the needs of the Board audience.**"
>
> — ACF Member

> **What works for one board of directors, works for one board of directors.**"
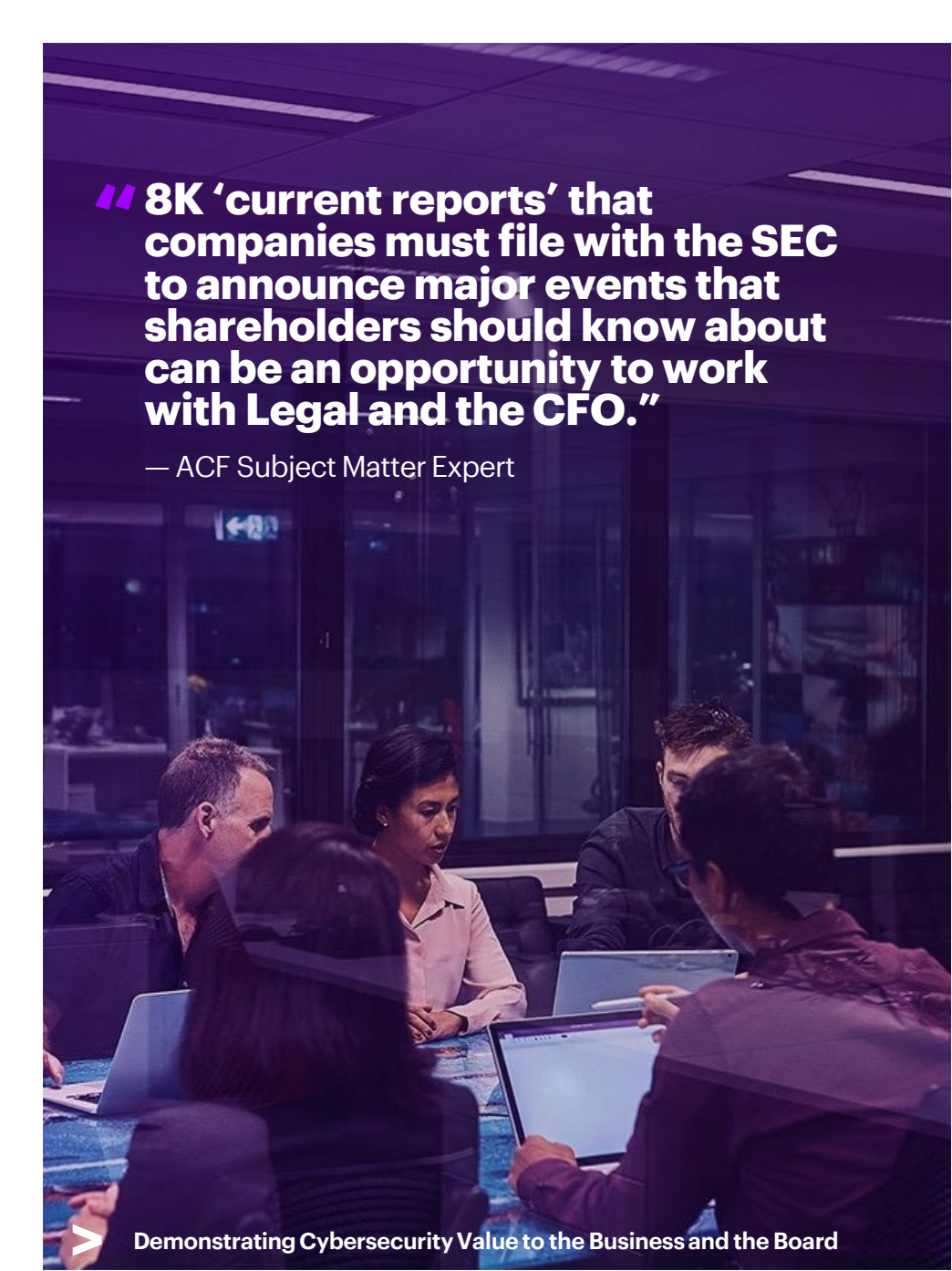>
> — ACF Member

Focus on "why" in the right context (part 1/2)

Rather than coming to the table with KPIs, complicated data analysis and technical jargon to explain "how" the enterprise is being kept secure, CISOs are encouraged to first discuss the "why" of cyber strategy.

ACF members said that in board conversations context matters. An ACF member said: "You need to align the messaging with the needs of the Board audience." Another member added: "As the saying goes, What works for one board of directors, works for one board of directors."

Another member said: "we all need to make sure we understand our audience and ensure we are telling the story that needs to be told for that organization. Over the last couple of years of presenting to the Board, we have evolved our presentation based on our maturity across the organization. Today, we focus on 6 things each quarter, Cyber Strategy, Governance Risk and Compliance, SecOps, Vendor Risk, Cyber Education and External Landscape. We highlight key risks and actions across each area in three slides which become the conversation during the Board meeting."
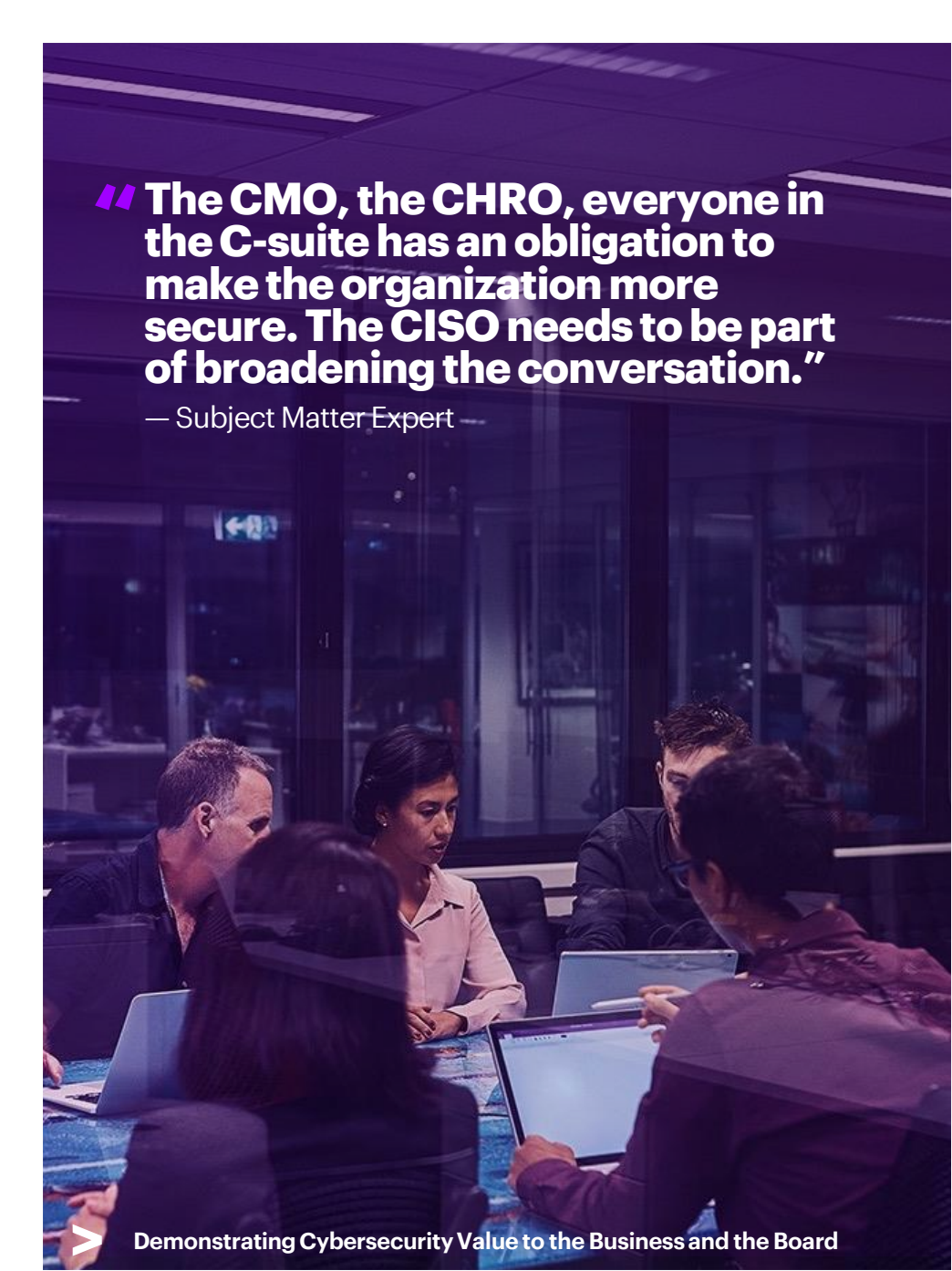
Focus on "why" in the right context (part 2/2)

Another member said: "Our CEO always focuses on three things in board discussions, so I did three things for each of my board agenda topics. Does seem to work!"

The SME said that 8K "current reports" that companies must file with the SEC to announce major events that shareholders should know about can be an opportunity to work with Legal and the CFO. In July, the Securities and Exchange Commission adopted rules requiring registrants to disclose material cybersecurity incidents and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance.

> **"The CMO, the CHRO, everyone in the C-suite has an obligation to make the organization more secure. The CISO needs to be part of broadening the conversation."**
> — Subject Matter Expert

Best practices (part 1/2)

Forum members identified the following best practices:

- Encourage the CEO to create an environment of shared accountability for a strong cybersecurity posture. "Being CISO is not an 'alone' job," said the SME. "The CMO, the CHRO, everyone in the C-suite has an obligation to make the organization more secure. The CISO needs to be part of broadening the conversation."

- Make cyber part of the company's success story. One way to retain funding and management interest, particularly when there haven't been any significant incidents, is to explain in business terms how a secure posture has contributed to the balance sheet, revenue and other business performance.

- Share newsworthy incidents from other companies, explain the attack, and share how your defenses (or proposed defenses) would help prevent or respond to a similar event. Current examples bring issues to life for the audience.

- Add stories, weekend language and metaphors to your messaging. For example, a CISO said they tell management: "Just because a family doesn't have as much money coming in as they did last year doesn't mean they should stop paying home insurance."

> **There is no 100 percent. We have to change people's mental model about cybersecurity."**
> — ACF Forum Member

Best practices (part 2/2)

Forum members identified the following best practices:

- Set expectations about the likelihood of breaches. One ACF member said: "We can't expect to shut down the 'big game hunters' like China and Russia. We may have to change management's perspective from defense to harm reduction." A member said: "We never use the word 'prevent." Another said: "There is no 100 percent. We have to change people's mental model about cybersecurity."

- Including too much detail into the appendix of a presentation or report might inadvertently put the board or CEO in legal jeopardy. For example, board members may face personal liability if it is discovered that they failed to implement a good-faith process for overseeing cybersecurity risks.

- An ACF member said: "No one starts on center stage on Broadway. It is important for leaders to recognize the team effort when you have the spotlight. It's also important to tread the boards off- Broadway. Avoid the metaphor of CISO as DIVA and communicating through tirades."

- Share information about the effectiveness of control programs, not the details of that program.

- Build relationships with other business leaders and the board by engaging in off-cycle conversations. Ask questions about their concerns and objectives.

"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 733,000 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.

\>