

Maximizing Security Investments: Doing More with Less

Accenture Cybersecurity Forum
Global Executive Leadership Network

January 30, 2024
Session Summary



From the Accenture Leadership

Accenture Cybersecurity Forum members tell us that budgeting is always a top priority, but the challenges continue to evolve. The mix of CapEx and OpEx investment is shifting as enterprises move to the cloud. New regulations are forcing some CISOs to make difficult investment choices. The tech stack is getting more complex. And as an ACF member said: “If we’re doing well in protecting the company, management wants to cut budget. It’s almost detrimental to the budgeting process if you’re not getting breached.”

In that challenging environment ACF members and subject matters shared their perspectives and best practices on maximizing security investments. Thanks to everyone who participated in the call. We trust you will find the experiences our subject matter experts and ACF colleagues shared useful as you invest wisely to keep your enterprises secure and resilient.

Cheers,



Paolo Dal Cin

Global Head of Accenture Security
ACF Executive Sponsor

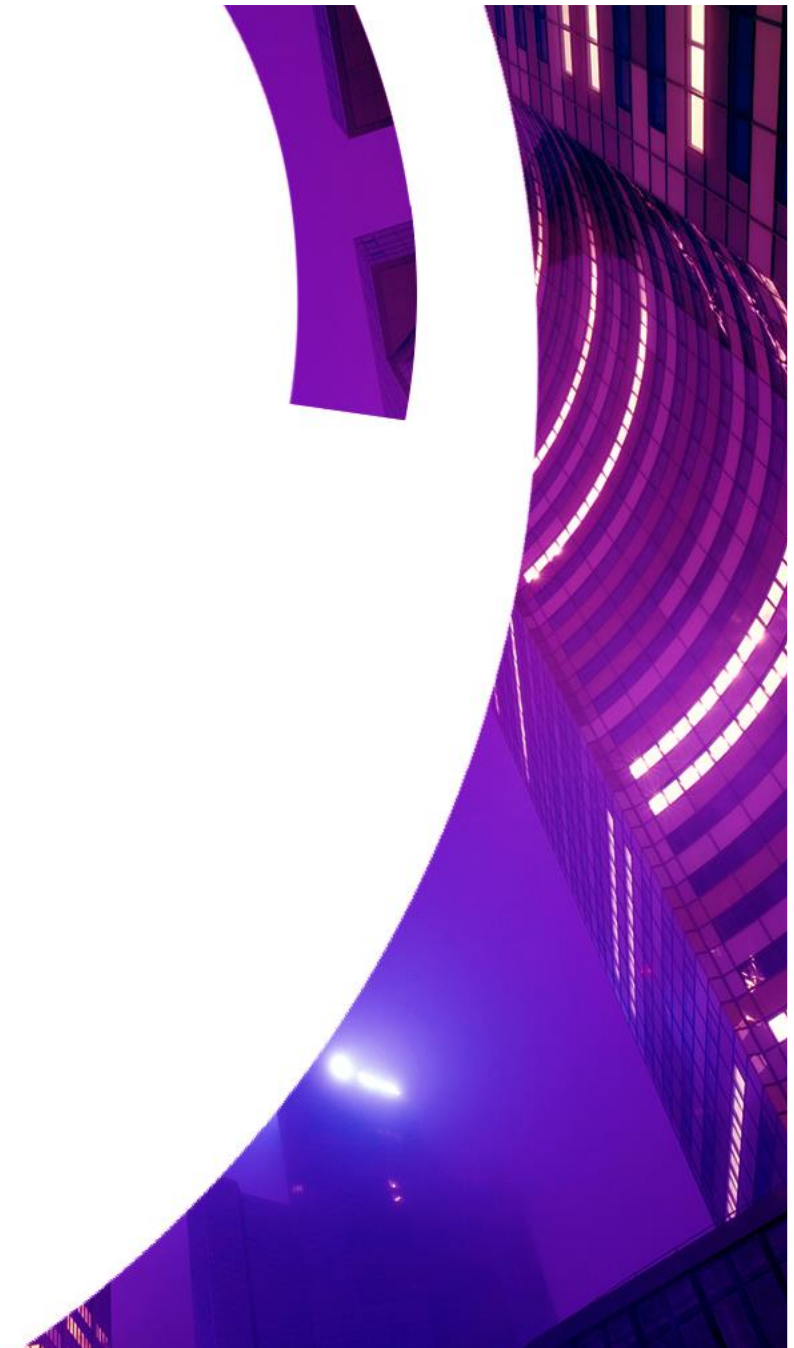
[LinkedIn](#)



Kris Burkhardt

Accenture CISO
ACF Chair

[LinkedIn](#)





Maximizing Security Investments: Doing More with Less

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled “Maximizing Security Investments: Doing More with Less” on January 30, 2024.

Today’s security budgets are under significant review, yet threats to the enterprise are unrelenting. ACF members explored how CISOs are approaching their budget analysis responsibilities in this challenging environment. In addition, they shared best practices that CISOs are utilizing to support the enterprise’s requirements to reduce cost while defending the enterprise from near-term and long-term risks.

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.

.

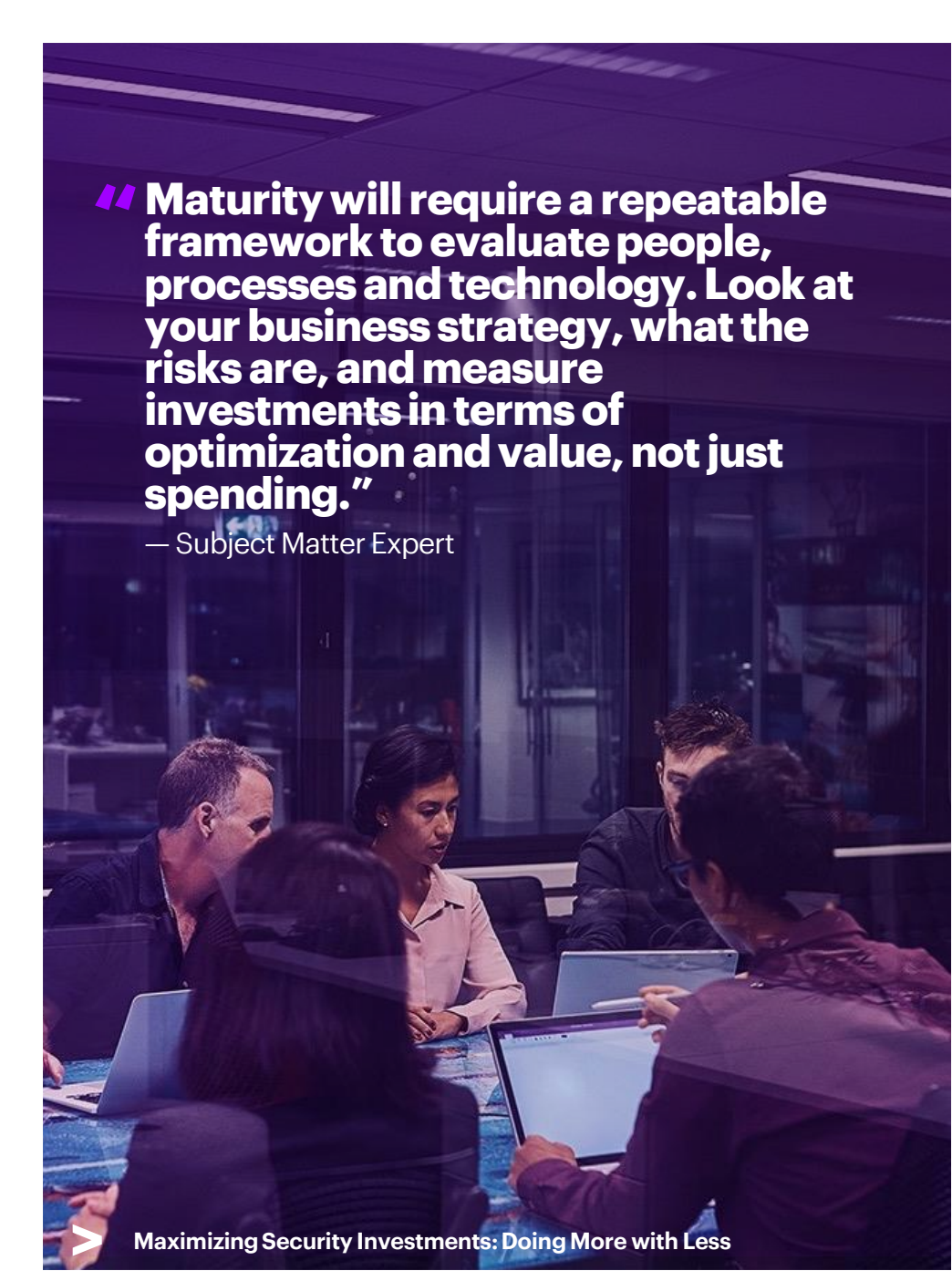
In this summary:

[The value of a budget framework crisis >](#)

[Doing more with what we have >](#)

[The Cyber-resilient CEO >](#)

[Best practices >](#)



“Maturity will require a repeatable framework to evaluate people, processes and technology. Look at your business strategy, what the risks are, and measure investments in terms of optimization and value, not just spending.”

— Subject Matter Expert

The value of a budget framework (part 1)

ACF members shared their experiences in using a framework for maximizing security investments.

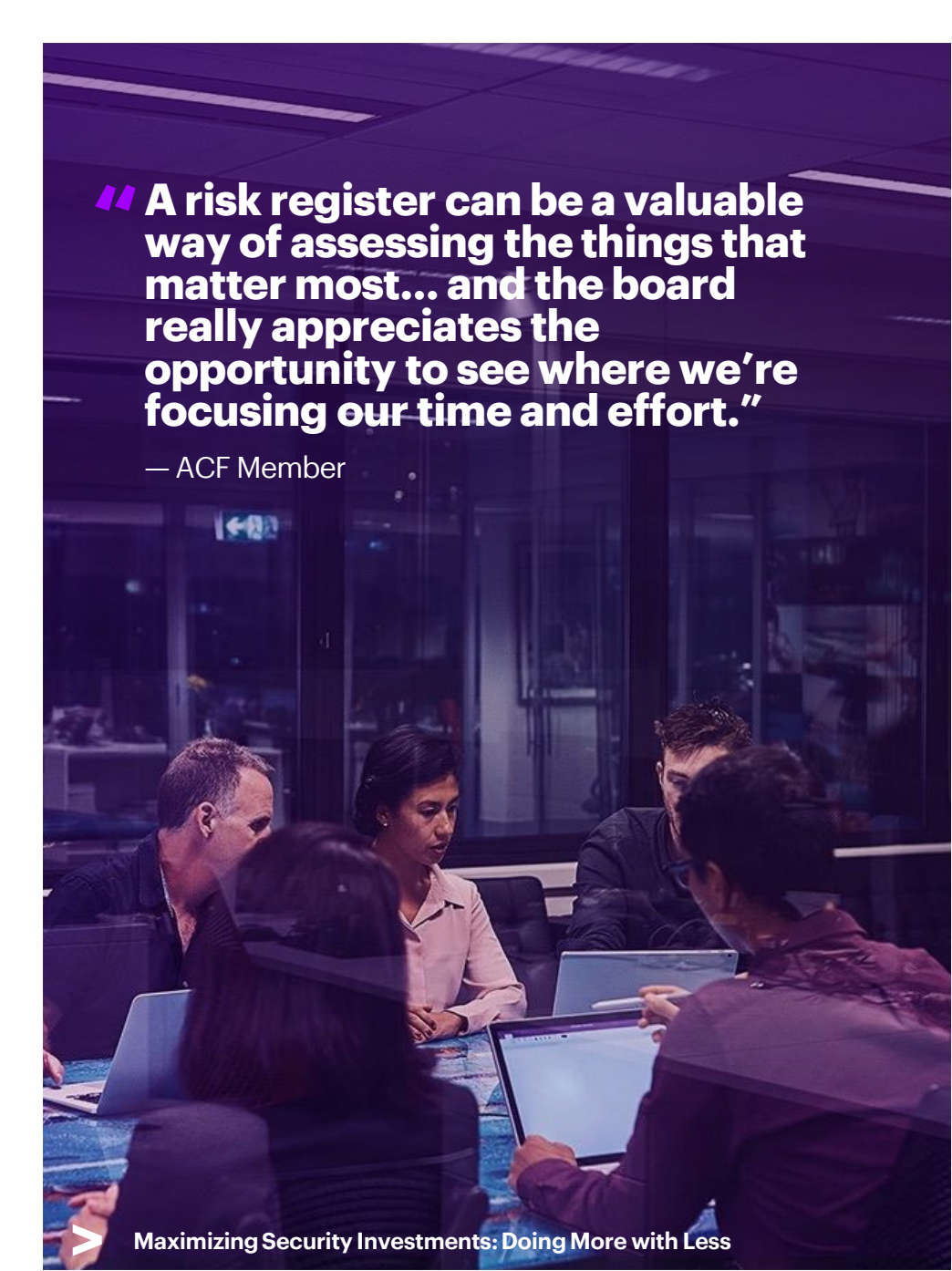
A subject matter expert said: “Maturity will require a repeatable framework to evaluate people, processes and technology. Look at your business strategy, what the risks are, and measure investments in terms of optimization and value, not just spending.”

For example, an ACF member divided investment into two categories.

“Operational tasks” include what the cyber team is doing and will continue to do to protect the enterprise in terms of tooling, people and associated costs.

“Initiative tasks” focus on current year investments to protect against new and different threats, and to support new business initiatives such as acquisitions or new business models.

Another member said that they participate in a top-down, enterprise-wide approach mandated by senior management to help them view investments through a common lens. Elements of that framework include scope of work, outcomes, business need, business value and business risk assessment.



“ A risk register can be a valuable way of assessing the things that matter most... and the board really appreciates the opportunity to see where we’re focusing our time and effort.”

— ACF Member

The value of a budget framework (part 2)

One member pointed to the FAIR (Factor Analysis of Information Risk) model for understanding, analyzing and quantifying cyber risk and operational risk in financial terms. Another said that a robust risk register documenting the likelihood and impact of various threat events helps to prioritize cybersecurity investment. “A risk register can be a valuable way of assessing the things that matter most,” an ACF member said. “And the board really appreciates the opportunity to see where we’re focusing our time and effort.”

A subject matter expert cautioned that “The NIST framework is good but it’s not enough. You need to be able to identify risks but measure them against the company’s risk appetite and be able to articulate the material impact of risk management investments.”

The idea of internal “pressure testing” can help ensure that cyber investments are aligned with business priorities. “We look at what everyone on the cyber team is doing, and whether or not activities are aligned with our budget and business priorities.”



“ CISOs should look for opportunities to consolidate, retire and automate. Commodity functions, in particular, present opportunities to automate processes that can reduce costs.”

— ACF Member

Doing more with what we have

CISOs should look for opportunities to consolidate, retire and automate, said an ACF member. Commodity functions, in particular, present opportunities to automate processes that can reduce costs. A subject matter expert said that software vendors are investing in tools, meaning “We expect to see a lot of innovation that will drive automation.”

Prioritizing risks helps with planning where to devote scarce, highly experienced resources on “the things that are going to matter most and give us the biggest bang for our buck and focusing on the more complex business issues.

A Forum member in a regulated industry said that changing regulatory requirements are affecting their budgeting. “Compliance sucks budget; we are being forced to make investment choices and trade-offs to meet the demands of regulators.



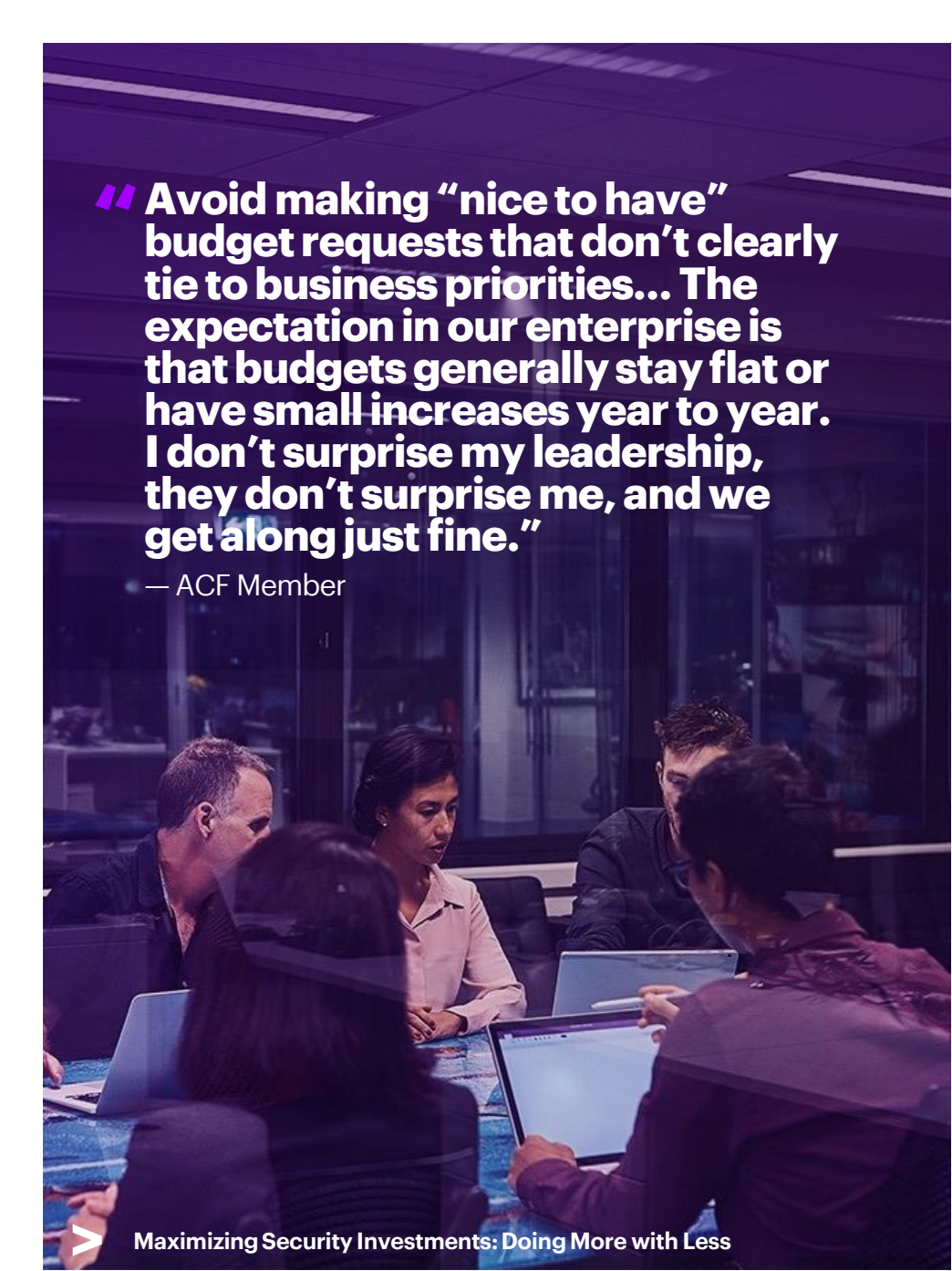
“ Only 15% of CEOs said they have dedicated board meetings for discussing cybersecurity issues.”

— Cyber-Resilient CEO research report

The Cyber-resilient CEO

Accenture’s [Cyber-Resilient CEO research report](#) reveals just how challenging budgeting can be. The report states: “More than one-half (54 percent) of CEOs said the cost of implementing cybersecurity is much higher than the cost of suffering a cyberattack, yet this is the reverse of reality. Unsurprisingly, the lack of understanding results in limited strategic focus; only 15% of CEOs said they have dedicated board meetings for discussing cybersecurity issues.”

Furthermore, 95 percent of the CEOs said that compliance with standards and regulatory requirements drives their cybersecurity strategy. And only 33 percent of the CEOs strongly agree that they have deep knowledge of the evolving cyber threat landscape.



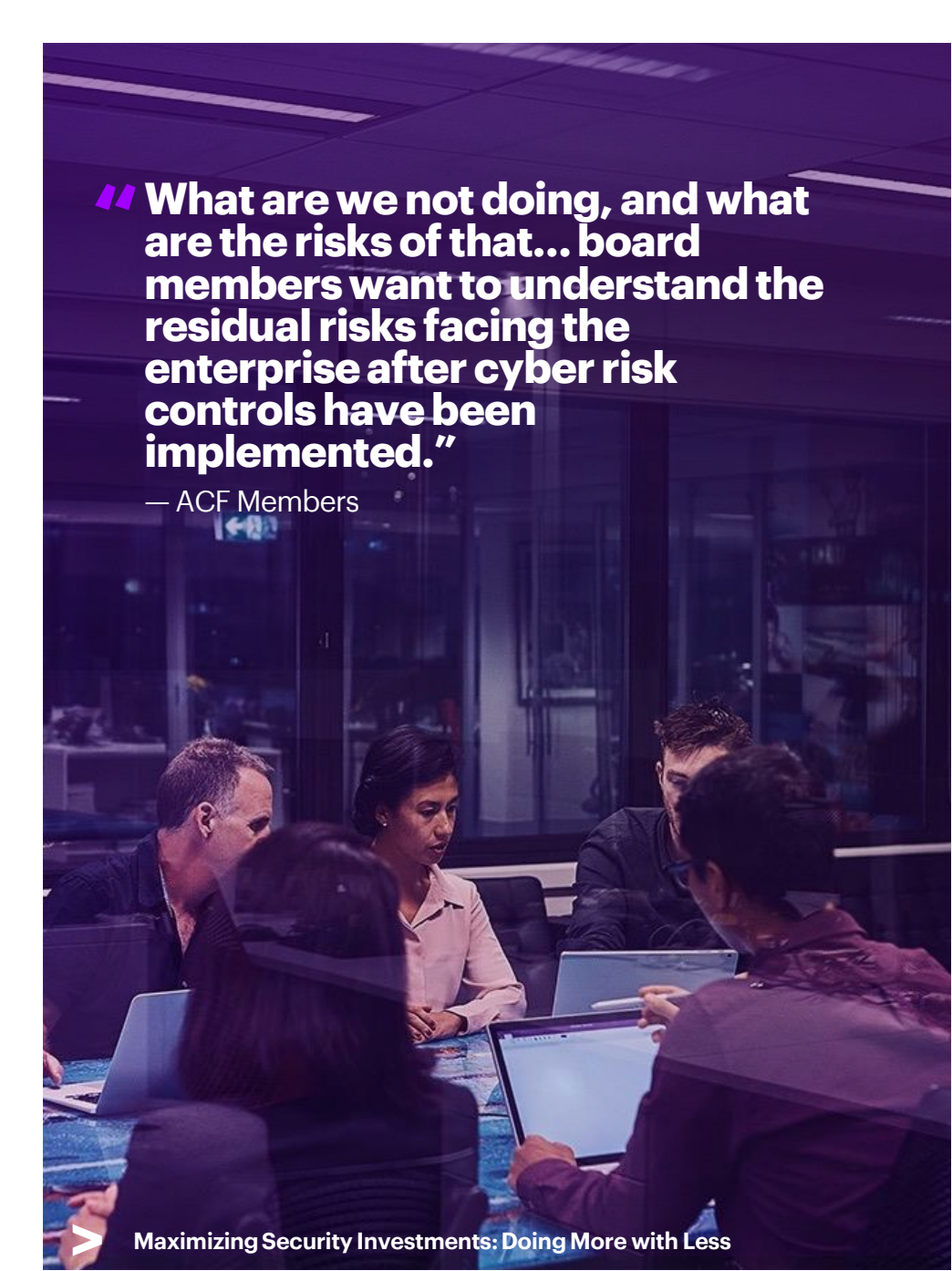
“ Avoid making “nice to have” budget requests that don’t clearly tie to business priorities... The expectation in our enterprise is that budgets generally stay flat or have small increases year to year. I don’t surprise my leadership, they don’t surprise me, and we get along just fine.”

— ACF Member

Best practices (part 1)

Forum members identified the following best practices:

- **Make clear what management is getting for their money.** Use “weekend language” to help management connect the dots between cyber investments and business value.
- **Avoid surprises. Communicate regularly. Deliver on commitments.** Avoid making “nice to have” budget requests that don’t clearly tie to business priorities. An ACF member said: “The expectation in our enterprise is that budgets generally stay flat or have small increases year to year. I don’t surprise my leadership, they don’t surprise me, and we get along just fine.”
- **Understand and align with the enterprise’s strategic risk philosophy.** Several members stressed the importance of helping other executives understand cyber risks in terms of management’s risk appetite.
- **Benchmarking may be one piece of the puzzle.** An ACF member said they engage a third-party to compare their spending vs. peers across several dimensions (i.e., security spending as a percentage of total IT spend and of total revenue.)



“What are we not doing, and what are the risks of that... board members want to understand the residual risks facing the enterprise after cyber risk controls have been implemented.”

— ACF Members

Best practices (part 2)

Forum members identified the following best practices:

- **Establish a cybersecurity oversight council.** Engage finance and other business functions in a regular cadence of meetings to discuss spending, priorities and risks. Engaging with other functions builds collective buy-in. For example, a member said: “The VP of finance is a member of our cross-functional committee, and we make sure we have frequent touch points.”
- **Be prepared to answer the question:** “What are we not doing, and what are the risks of that.” Several ACF members said that board members want to understand the residual risks facing the enterprise after cyber risk controls have been implemented.



**“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.

Copyright © 2024 Accenture All rights reserved.
Accenture, and its logo are trademarks of Accenture.