Current Imperatives

for the Future of Cybersecurity

Accenture Cybersecurity Forum
Global Executive Leadership Network

25 January 2023
Session Summary

From the ACF Chair

We're in the business of constantly keeping our house in order. And some new approaches are called for.

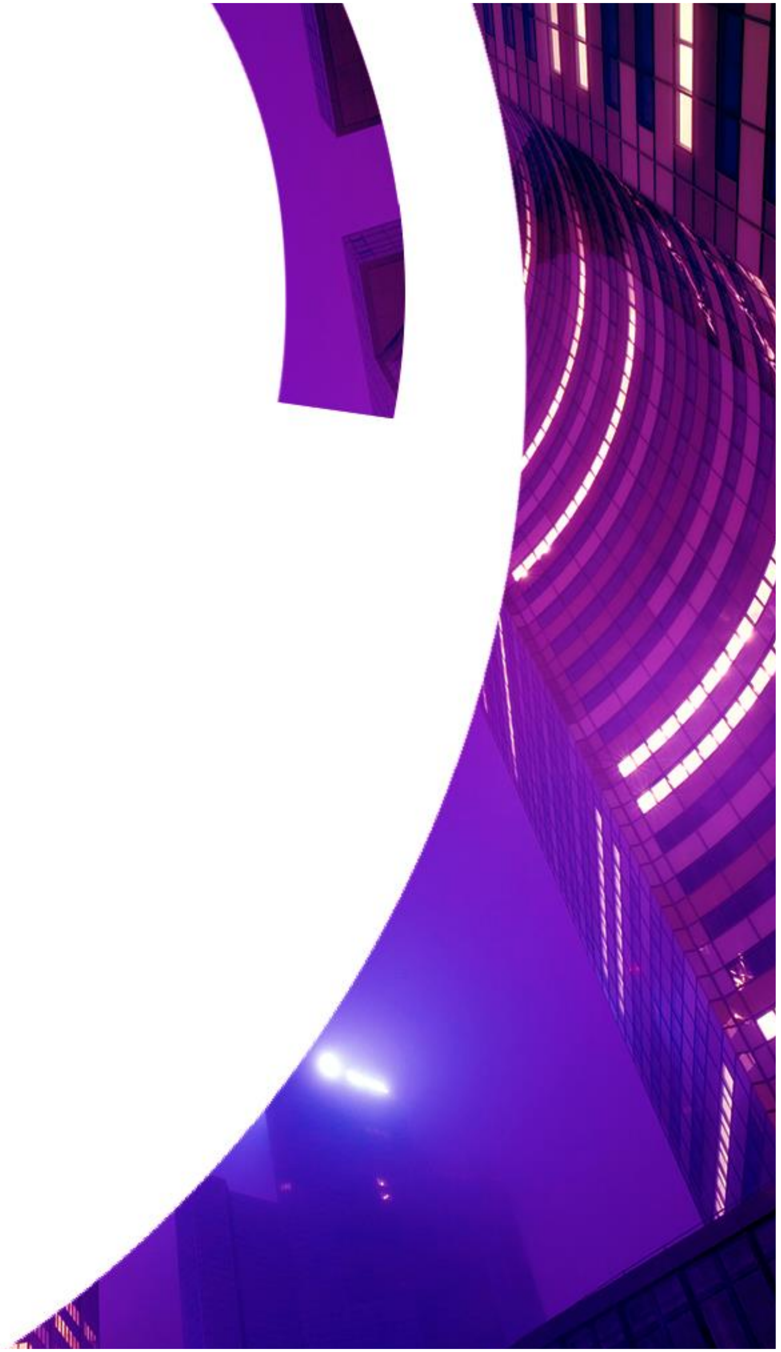
That's just one of the insights I drew from our January 25 Accenture Cybersecurity Forum where members shared fresh ideas for reinforcing foundational enterprise security and bracing for new challenges. For example, one member shared a powerfully simple housing analogy for explaining concepts like identity, network segmentation and data protection to the board. Members also offered practical ideas for strengthening foundational elements of our cybersecurity model.

Looking over the horizon, Forum members discussed the impact of emerging trends such as threat actors weaponizing ChatGPT for phishing campaigns, the know-your-crypto-customer imperative and heightened board of director expectations.

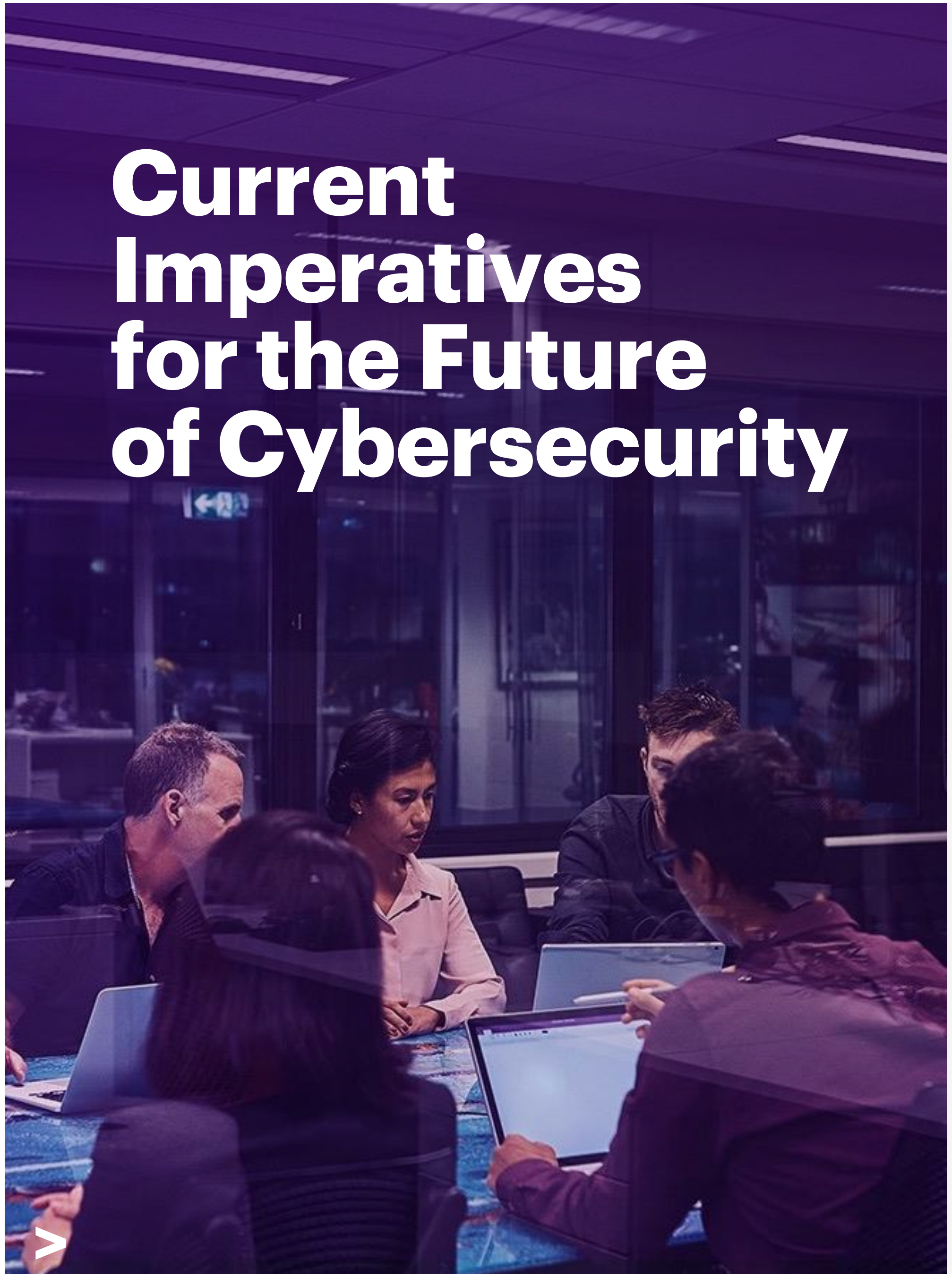
I hope you find these perspectives useful as you keep the security of your enterprise in order. If you want to connect, just drop me an email. Until then, wishing you all the best in keeping your house safe from intruders.

Cheers,
Kris Burkhardt
Accenture CISO, ACF Chair

LinkedIn: Kristian Burkhardt



Current Imperatives for the Future of Cybersecurity



The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “Current Imperatives for the Future of Cybersecurity,” on January 25, 2023. Members say they face a variety of challenges ranging from the threat environment and global instability to budget pressures and organizational misalignment. New technology such as ChatGPT and the potential of automated and tech-enhanced attackers begs the question: What can fundamentally be done to improve enterprise security?

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.

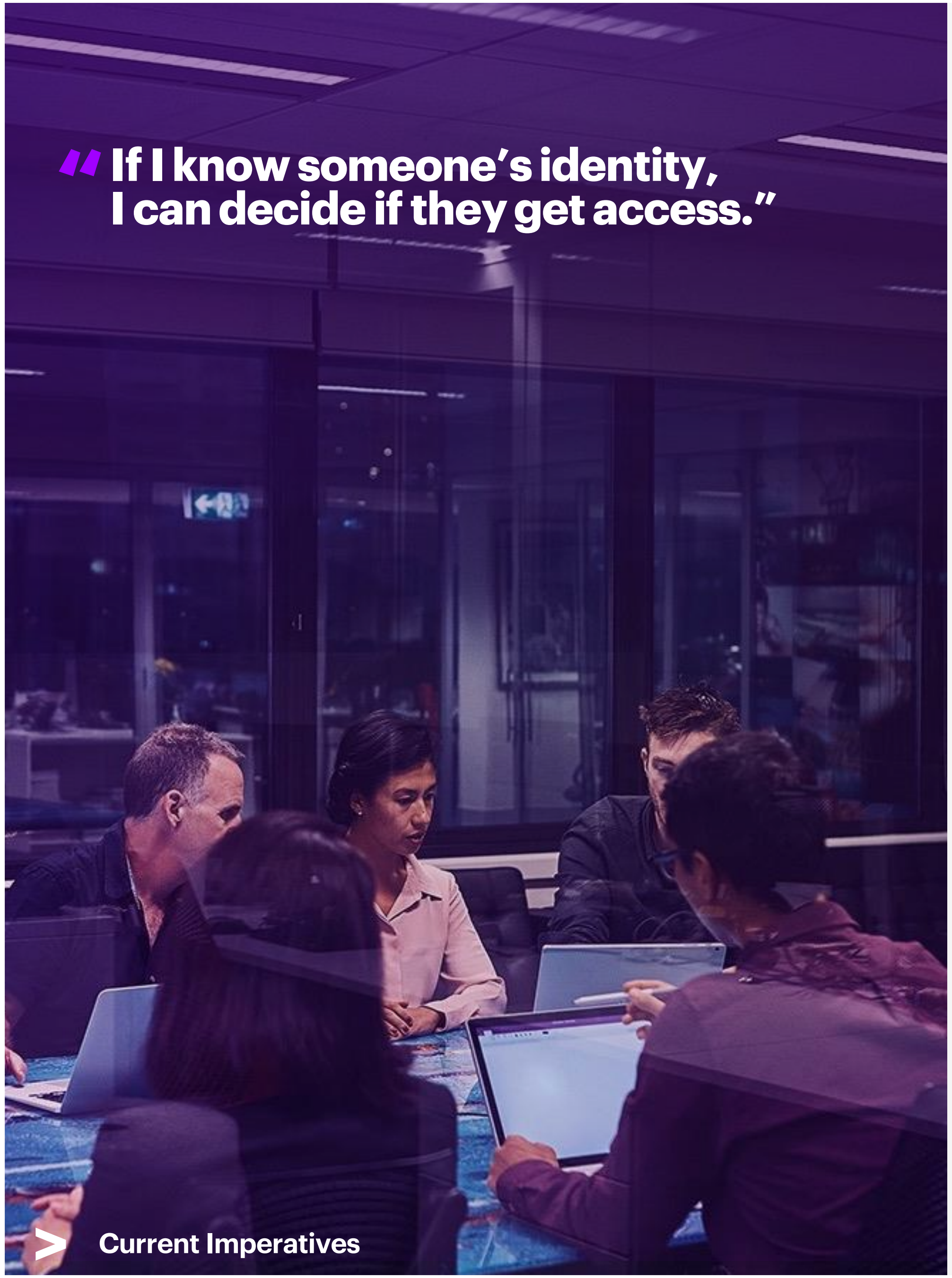
In this summary:

Research shows the gap in perception of cyber risks between business executives and cybersecurity leaders appears to be closing.

The view from Davos

Accenture teamed with the World Economic Forum in January to share the findings of research with CISOs and C-level business executives. The “Global Cybersecurity Outlook 2023” report identified three main areas of cybersecurity concern: a more complex computing environment characterized by legacy and multi-cloud platforms; political instability; and the introduction and secure adoption of new technologies such as the metaverse and quantum computing. On a positive note, the gap in perception of cyber risks between business executives and cybersecurity leaders appears to be closing. However, more of the right kinds of information about potential business impact are still required to drive investment and action at the business level.

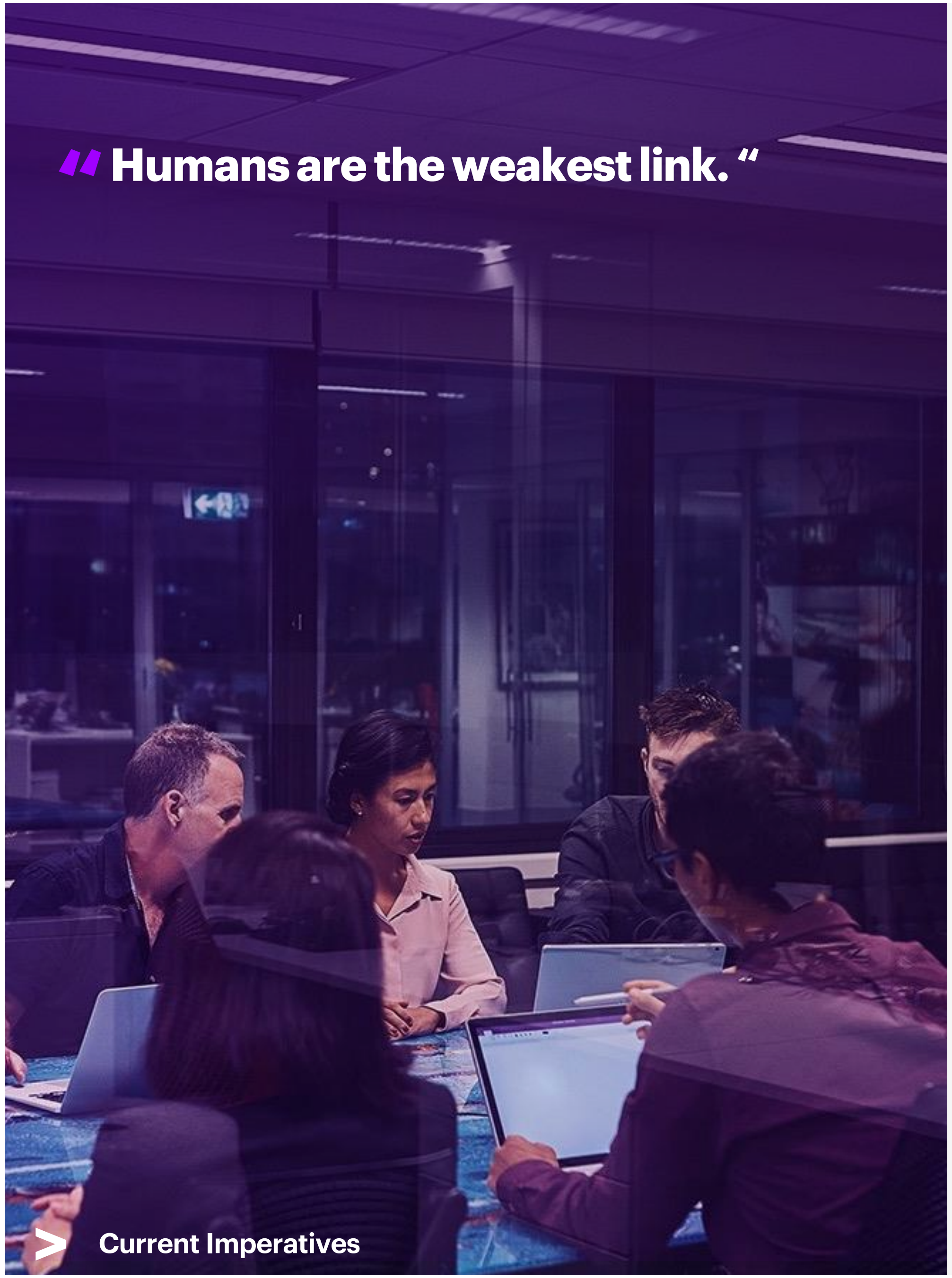
Download the complete report here.



"If I know someone's identity, I can decide if they get access."

An analogy for the CISO's current imperatives

A member offered a way to explain the CISO's priorities to the board and non-technical audiences by using a house as an analogy. "I keep the keys to my house. If I know someone's identity, I can decide if they get access," they said. "Once someone is in my house, I want to control which rooms they can visit. Think of that as network segmentation. And if they get into somewhere where they don't belong, like the master bedroom, where they can steal the jewelry, I want to know what they're after or might have left with. That's like data protection."



“ Humans are the weakest link. “

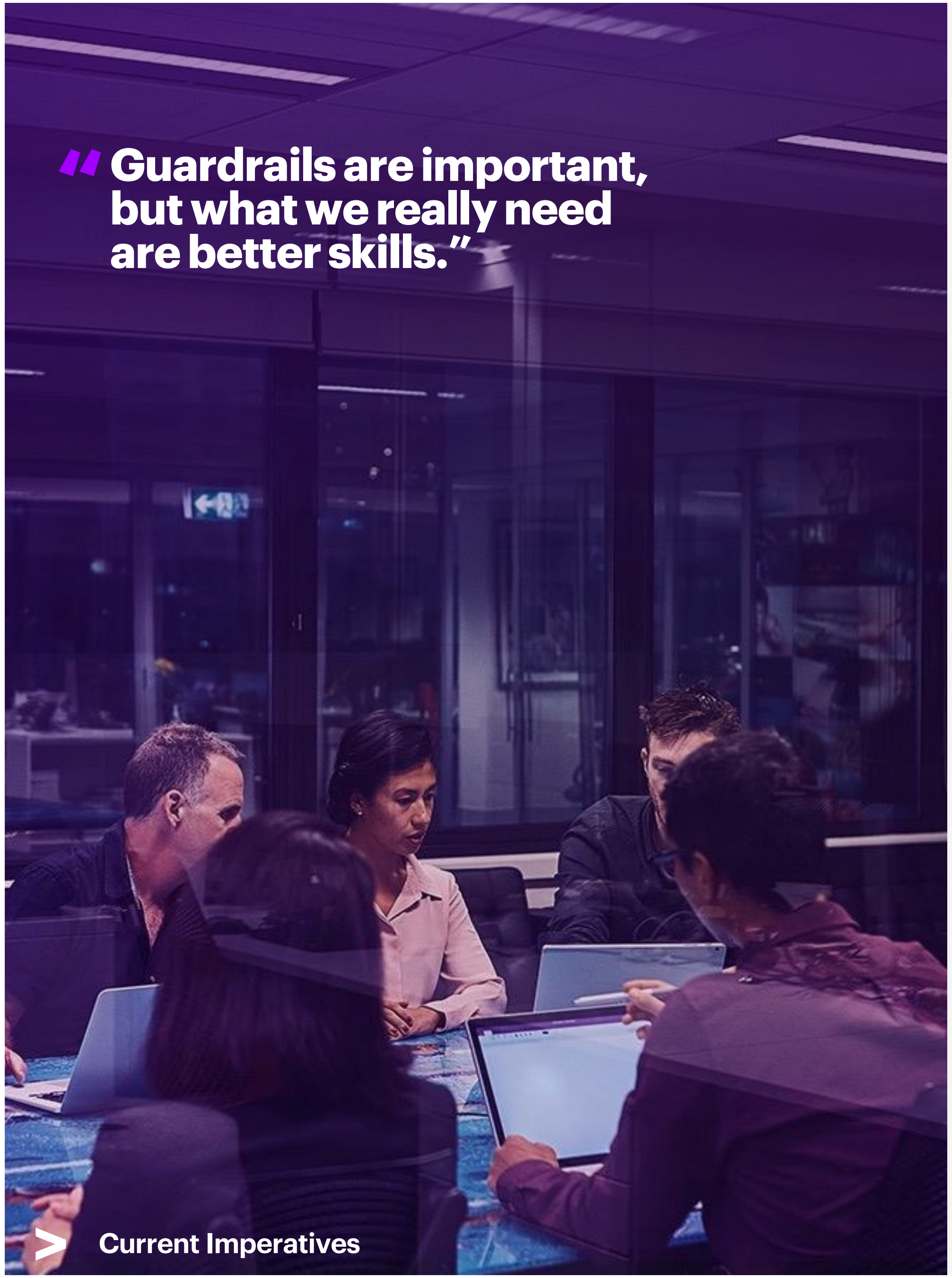
Strengthening the foundation

ACF members shared a variety of insights and leading practices for addressing the ongoing challenges CISOs face every day.

□ Address supply chain insecurity in new ways— Elevate security’s importance with partners and acquisitions. A member said: “Humans are the weakest link. We need to raise the bar on what we require from third parties to deliver real security for our enterprise.” Another added: “Software supply chain and code dependencies must continue to be a focus for Business…and it must be better automated.”

A member explained that only after a detailed investigation did the company become aware that a core industrial control system relied on code from Chinese and Russian developers. “We were assured that we were using software from U.S. developers, but a deeper dive revealed that wasn’t the case,” the member said.

□ Address security early on in cloud migration—Several ACF members spoke about the need for greater interoperability between security tools used across the technology stack. Another member discussed the challenge of finding the right security talent to support the enterprise cloud journey.



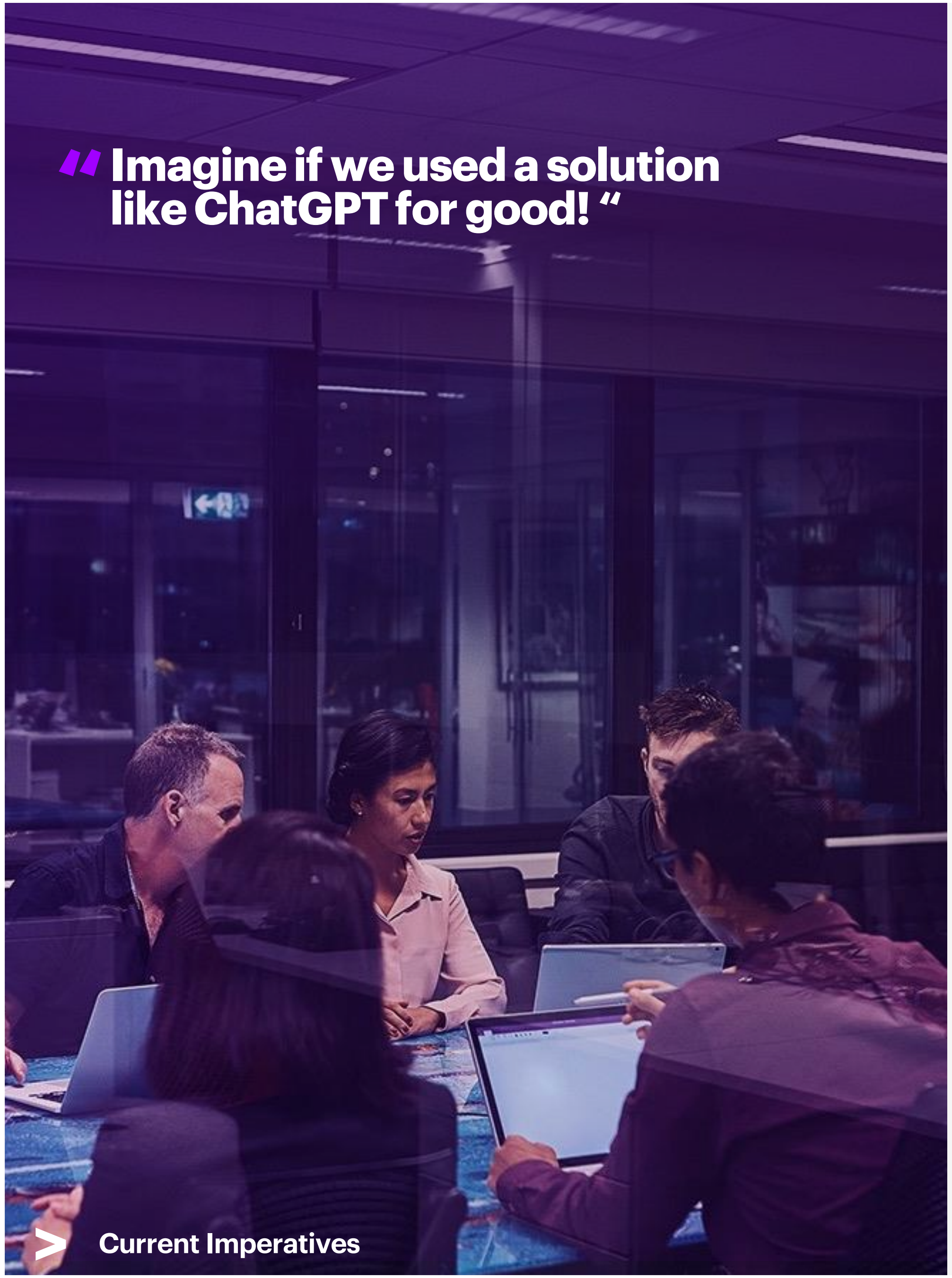
"Guardrails are important, but what we really need are better skills."

Strengthening the foundation (con't)

- ❑ Deploy security resources in new ways—One member found success in the DevSecOps approach of embedding members of the security team into the CRM, website and other apps development teams. Another member noted: "Defense in depth is mandatory and educating developers, equipping them with right tools, and automated reporting is an essential step. The earlier security is built into the architecture and design, the less likely major issues are introduced."

- ❑ A single application development pipeline—ACF members suggested managing application development globally, given the shortage of high-quality developer talent. "Guardrails are important," said a member, "but what we really need are better skills," Standardized, automated controls and consistent points of enforcement were also identified as critical in maintaining scale cybersecurity compliance at scale

- ❑ "Make an unattractive target"—Members offered several suggestions for reducing the attack surface. Cloud VPN, or VPN as a service, can enable users to securely access a company's applications, data and files in the cloud through a website or via a desktop or mobile application that is part of the enterprise's cloud delivery infrastructure. A member called for maximum visibility into enterprise-wide identities, credentials and authentication standards.



“Imagine if we used a solution like ChatGPT for good! “

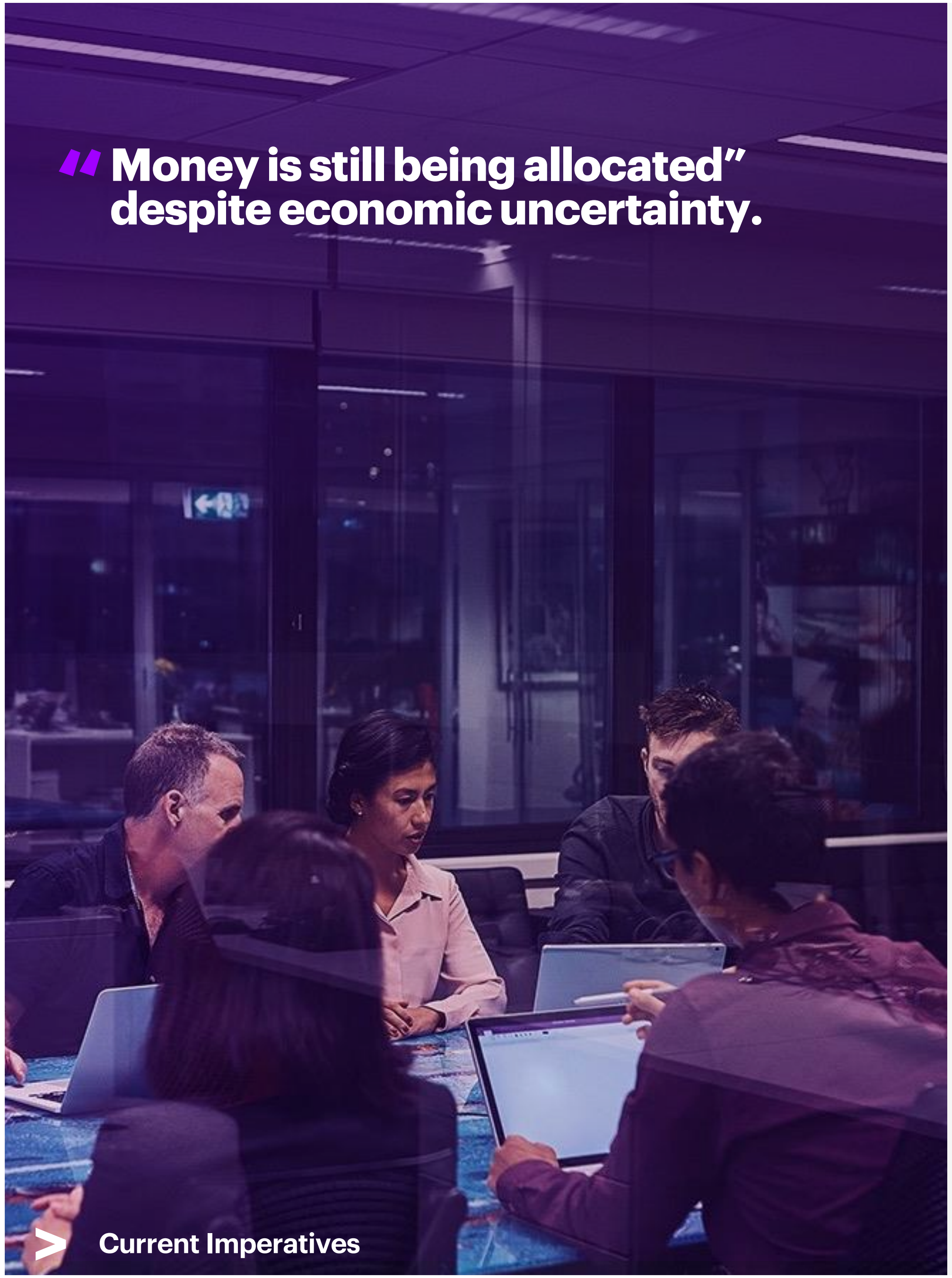
Preparing for the next wave

□ Know your crypto customer—Members noted that with regulators scrutinizing, and sometimes fining, crypto operators, the adage “know your customer” becomes even more important. “Don’t let your customers be anonymous,” said a member.

□ ChatGPT—Members noted a variety of concerns about large language models. Threat actors are already using those tools to create new phishing campaigns. Members are asking how ChatGPT is aiding in the misinformation of open-source intelligence which one member said the government is just now starting to accept as a method for data analysis.

One CISO reports “Our threat emulation teams are using the large language tools like CODEX and ChatGPT to generate novel attacks. The tools can generate not just plain language things like phishing emails, but also pieces of code that are sometimes novel, although there is a fairly high software error rate from the current tools.”

Another CISO added: “Imagine if we used a solution like ChatGPT for good! For example, having a trusted AI engine that could not only find vulnerabilities, but fix the vulnerabilities and design flaws in our code repositories. I think we are pretty close to this being a reality and something we need to be prepared for.”

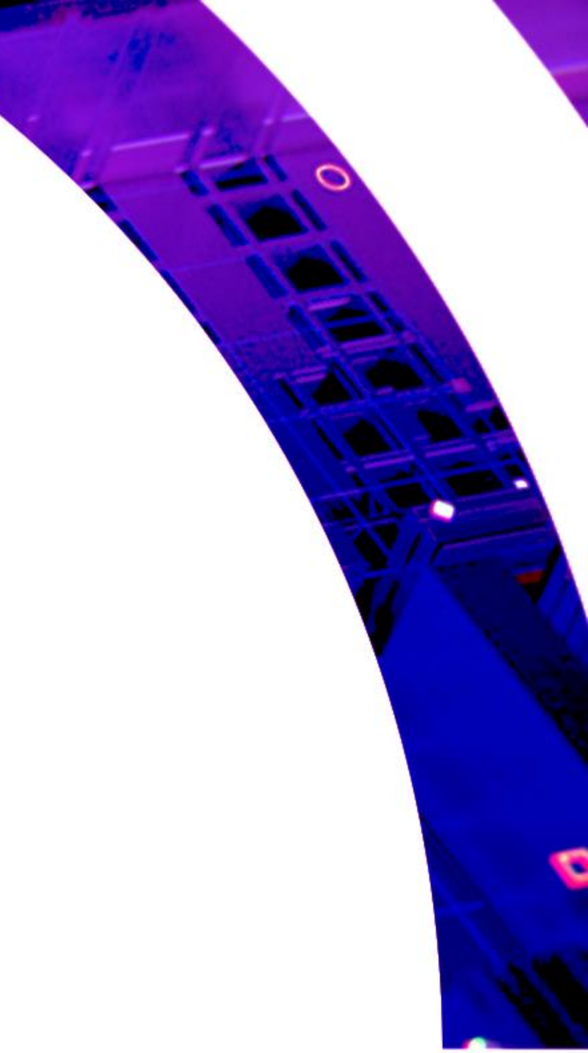


> “Money is still being allocated” despite economic uncertainty.

Preparing for the next wave (con’t)

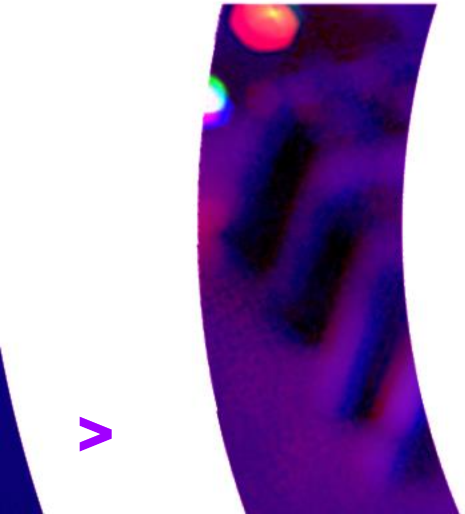
□ Evolving Board engagement—Board members discussed how boards are engaging differently about cybersecurity. One board member said that their enterprise is developing a “board elevator speech” with talking points that any board member can deliver when asked about cybersecurity. That responsibility is no longer the purview of just one technically oriented board member. Another board member said that concerns about cyber risk remain “on the top of the list. Money is still being allocated” despite economic uncertainty. A subject matter expert reported other changes in board engagement they are seeing. Specifically:

1. Boards are seeking a better understanding, beyond maturity and peer benchmarking, to understand how investments align with the enterprise risk appetite.
2. Boards are getting ongoing education about cyber, no longer relying on a single board member. This emphasis is driven at least in part by the SEC’s proposed rules regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
3. Boards are reaching beyond the CISO to hear directly from all members of the C-suite on how they are considering cyber risk within their priorities.
4. The topics boards are interested in are expanding—cloud, supply chain, ransomware, emerging tech, talent, geopolitical direction and cost optimization.



“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 global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Technology and Operations services and Accenture Song — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 721,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at 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. Follow us @AccentureSecure on Twitter, LinkedIn or visit us at accenture.com/security.