AI & Security

Accenture Cybersecurity Forum
Global Executive Leadership Network

March 20, 2024
Session Summary

From the Accenture Leadership

Across all industries, Accenture found 40% of all working hours can be impacted by large language models like GPT-4. This is because language tasks account for 62% of the total time employees work, and 65% of that time can be transformed into more productive activity through augmentation and automation.

While this potential of AI is attractive, we heard in our latest Accenture Cybersecurity Forum that CISOs need to be the adults in the room.

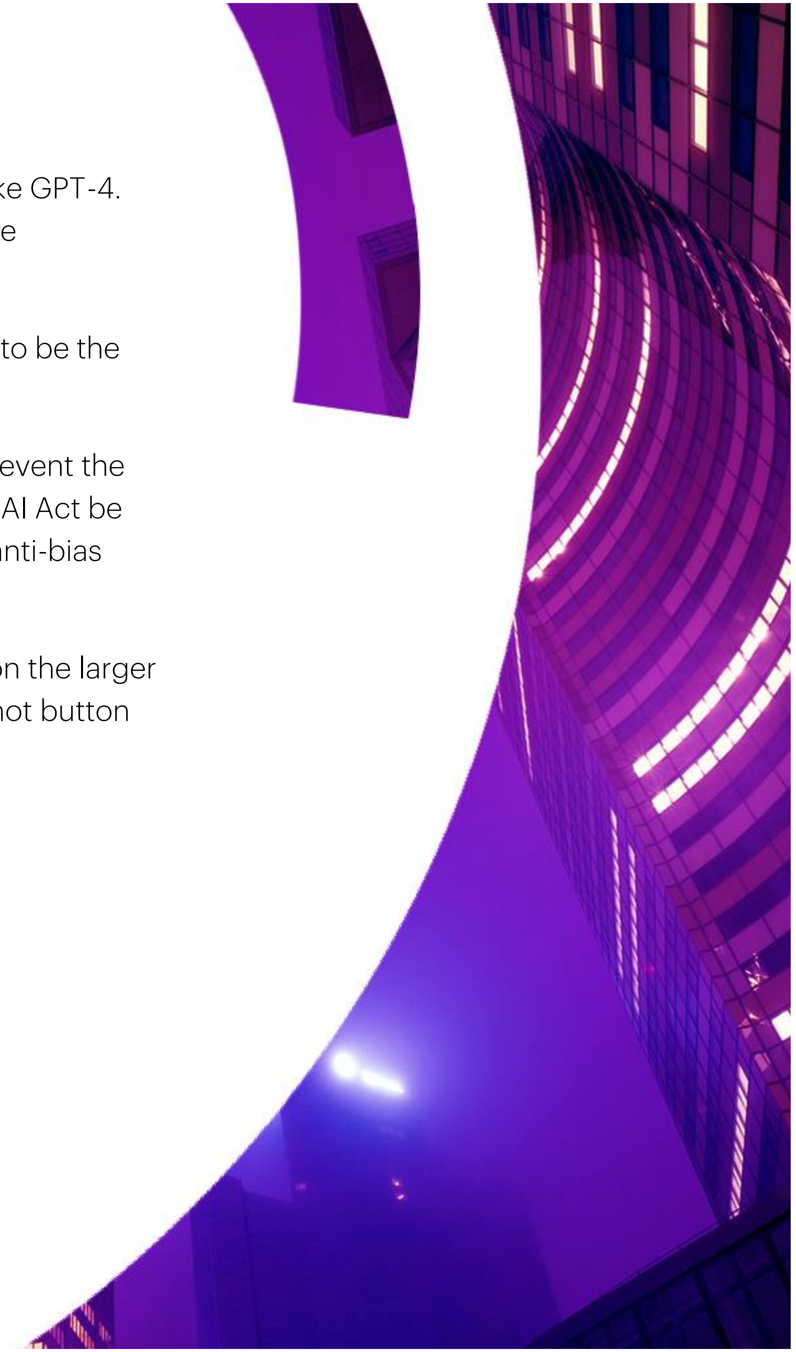
The rapid adoption of AI raises important questions for CISOs. How will the business protect its own IP and prevent the inadvertent breach of third-party copyright in using pre-trained foundation models? How will laws like the EU AI Act be incorporated in the way data is handled, processed, secured and used? What about in anti-discrimination or anti-bias considerations?

Our recent Accenture Cybersecurity Forum provided an opportunity for members to compare perspectives on the larger issue of "AI & Security." Our thanks to all the participants who shared questions and valuable insights on this hot button issue.

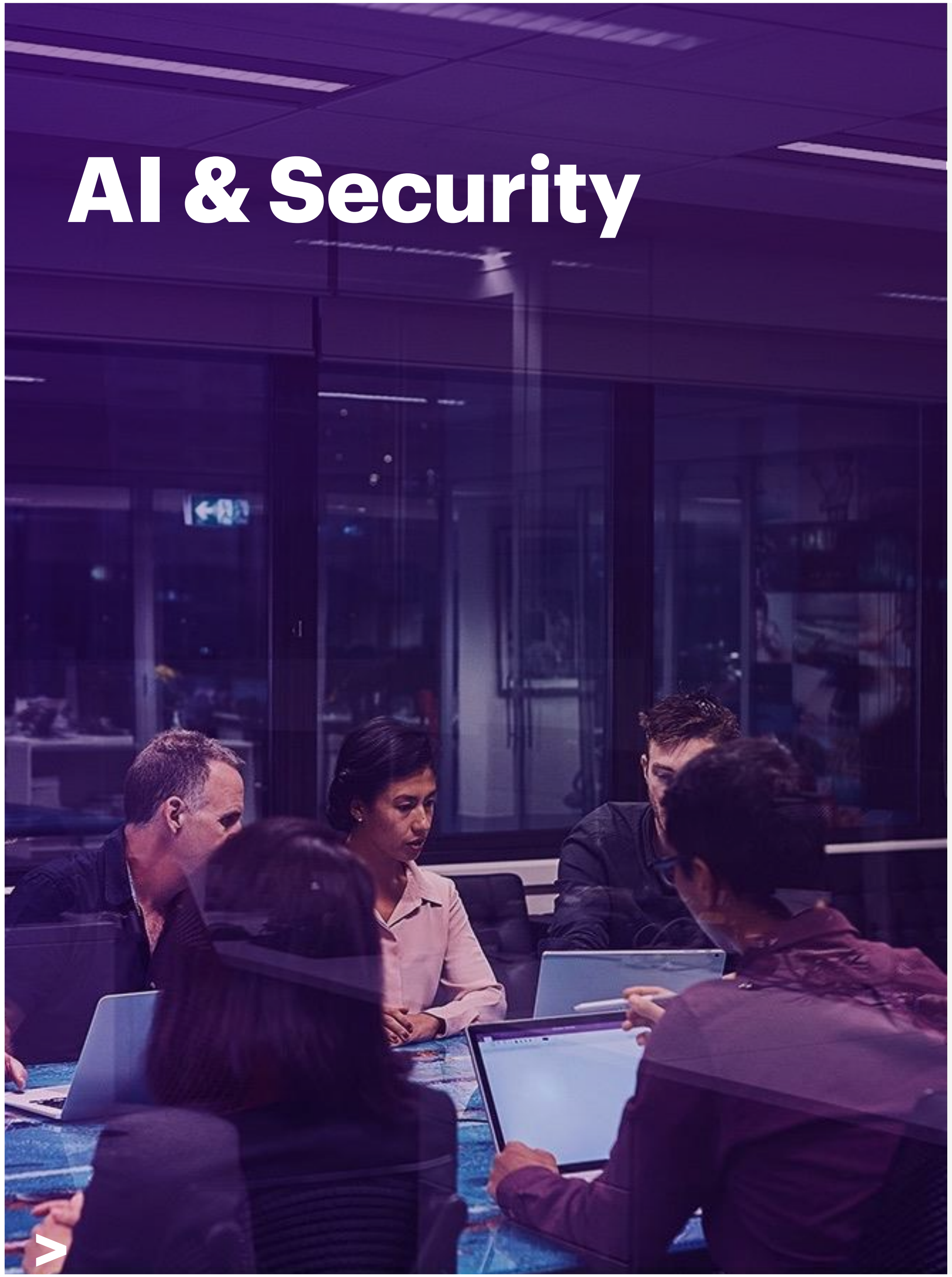
Cheers,

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

Kris Burkhardt
Accenture CISO
ACF Chair
LinkedIn



AI & Security



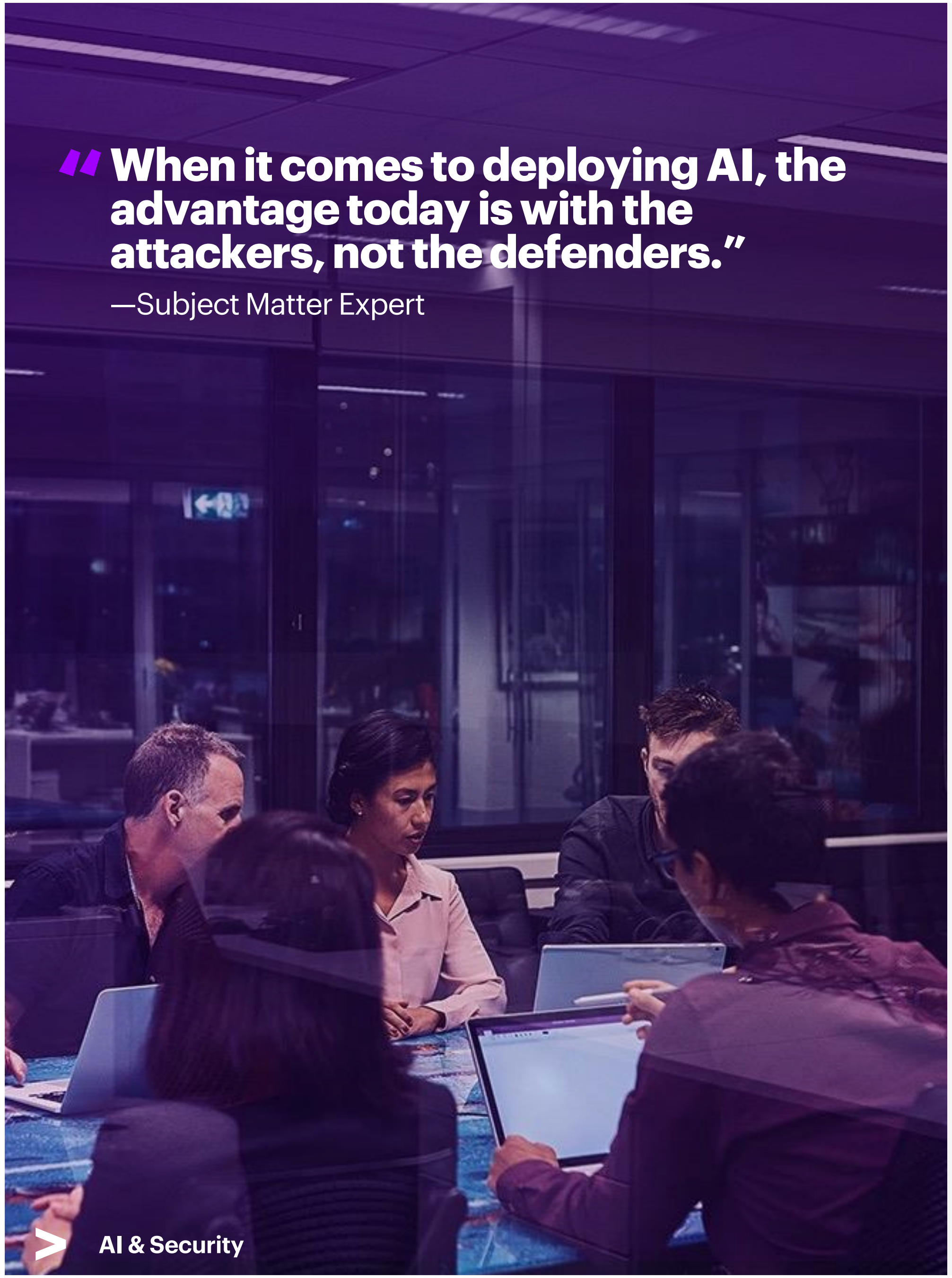
The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled “AI & Security” on March 20, 2024.

Our discussion focused on three key questions:

- How are threat actors leveraging AI?
- How are defenders responding, and,
- As we continue to expand our use of AI-based solutions across the business, how are defenders protecting the enterprise?

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:

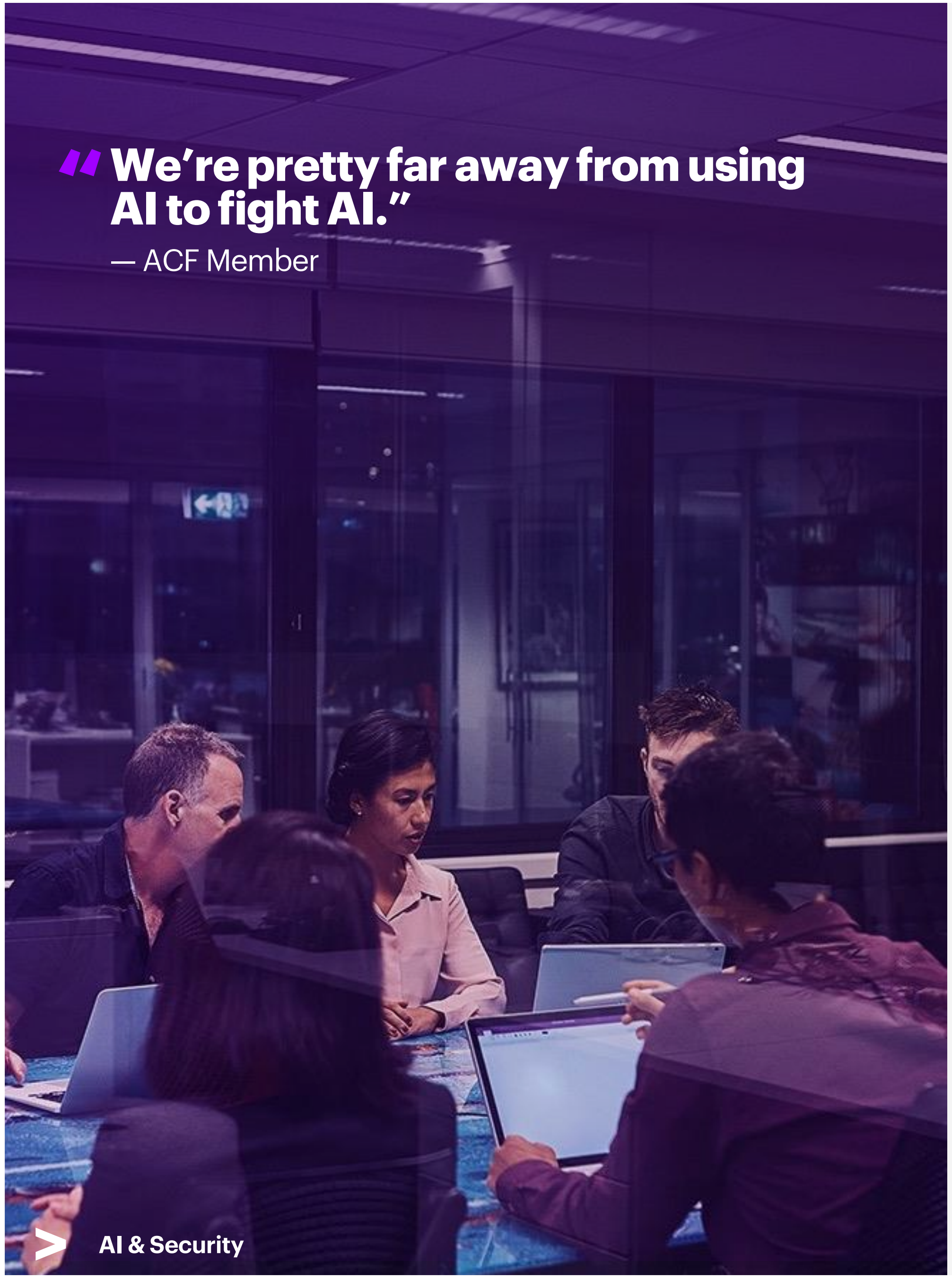


> **“When it comes to deploying AI, the advantage today is with the attackers, not the defenders.”**
>
> —Subject Matter Expert

Enterprises “are bringing a knife to a gun fight”

Threat actors are currently winning the arms race, according to subject matter experts. “When it comes to deploying AI, the advantage today is with the attackers, not the defenders,” said a subject matter expert. An ACF member added: “Attackers are writing code 10 times faster than they could before. They are accelerating their social engineering campaigns.”

Attackers are also using AI in their disinformation and misinformation campaigns incorporating deep fake imagery, natural language processing and highly targeted phishing.

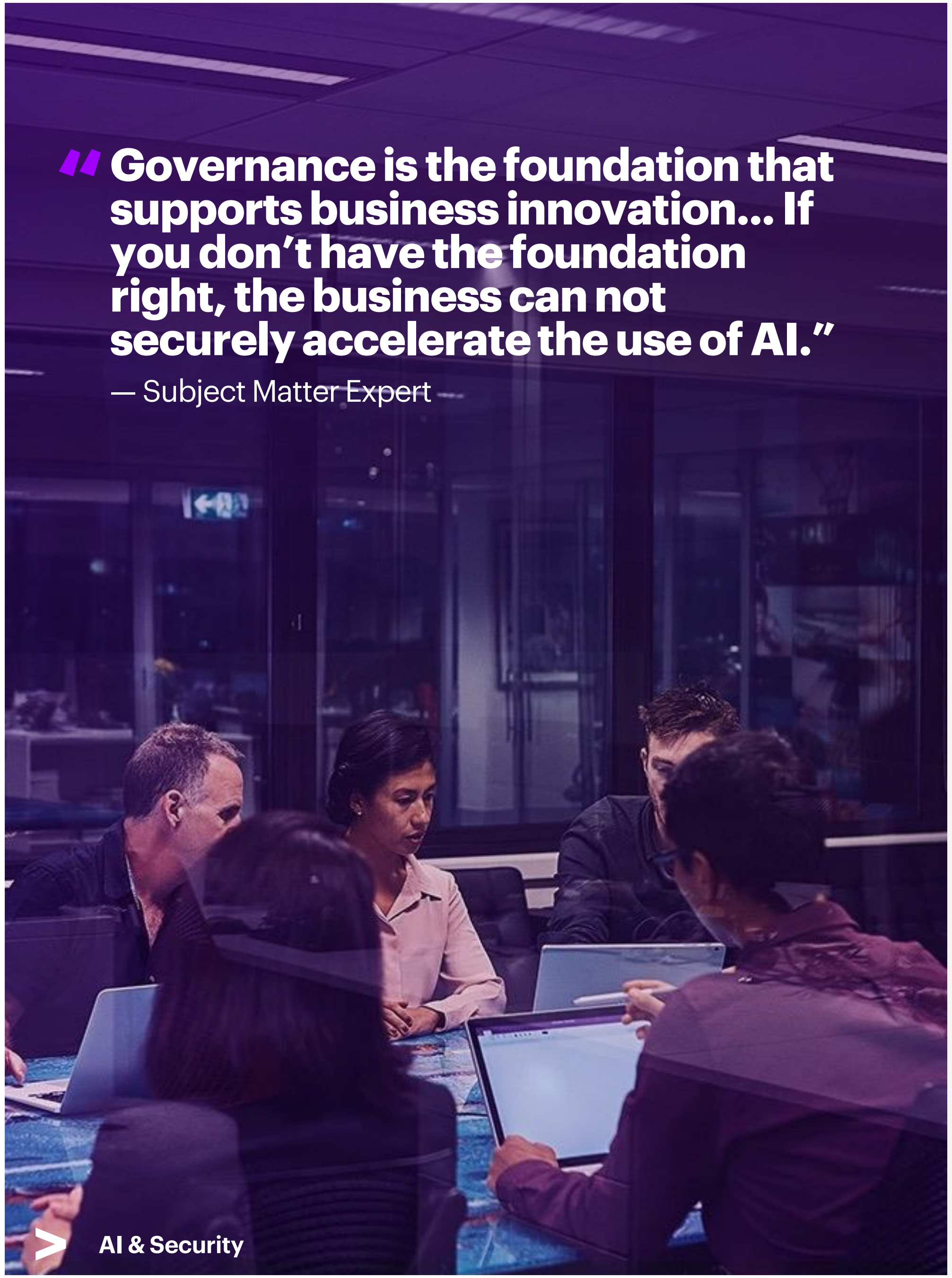


> “We’re pretty far away from using AI to fight AI.”
>
> — ACF Member

Using AI to secure the enterprise

“We’re pretty far away from using AI to fight AI,” said an ACF member. A variety of factors make CISOs skeptical about the current state of AI as a cybersecurity tool:

- “Today we see AI as an add-on. We can’t swap it out with our traditional tools.”
- “We know GenAI makes things up.”
- “We don’t know how the tool got the answer.” One ACF member shared the experience of using AI to write their resume, only to find that the resume claimed they had won an Olympic swimming medal. Despite their best attempts, it was never clear how the tool drew that false conclusion.
- “You can’t just turn it on and expect to get completely right answers.”



> “Governance is the foundation that supports business innovation… If you don’t have the foundation right, the business can not securely accelerate the use of AI.”
>
> — Subject Matter Expert

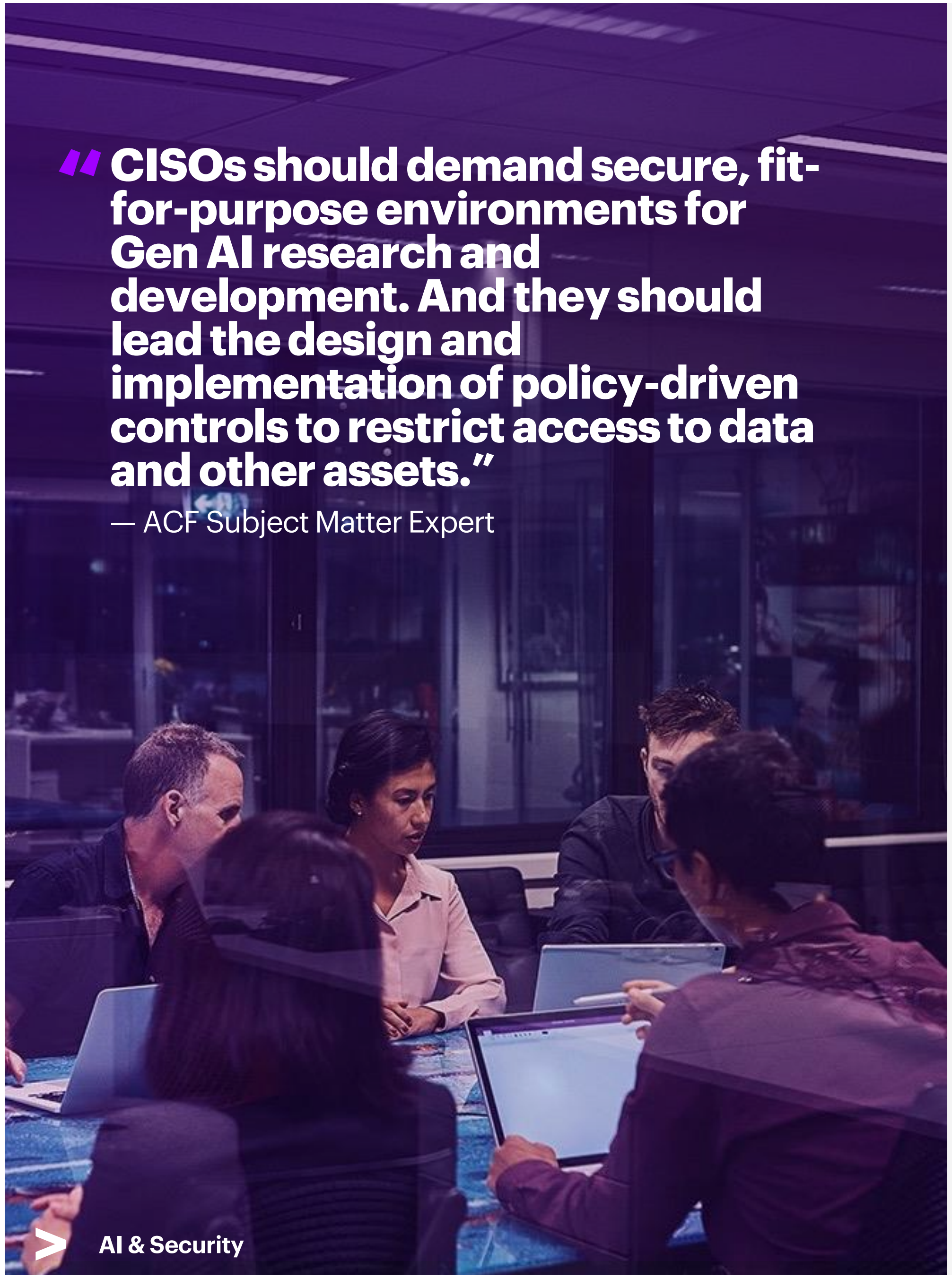
Supporting AI-based business initiatives (part 1)

A subject matter offered a three-tiered framework for helping the business use AI responsibly and effectively: Govern, protect, defend.

Governance is the foundation that supports business innovation, said a subject matter expert. If you don’t have the foundation right, the business can not securely accelerate the use of AI.

The outcomes of sound governance should include clear, consistent policies for Gen AI usage throughout the enterprise and legal, privacy and compliance review processes. Reaching those outcomes requires **governance frameworks** for oversight, review and reporting and **training and awareness** that promotes responsible AI usage.

For example, an ACF member said their 16-person governance committee was unwieldly and ineffective. A six-person committee, incorporating legal, security, data, information governance and one representative of the business has proven to be much more effective.

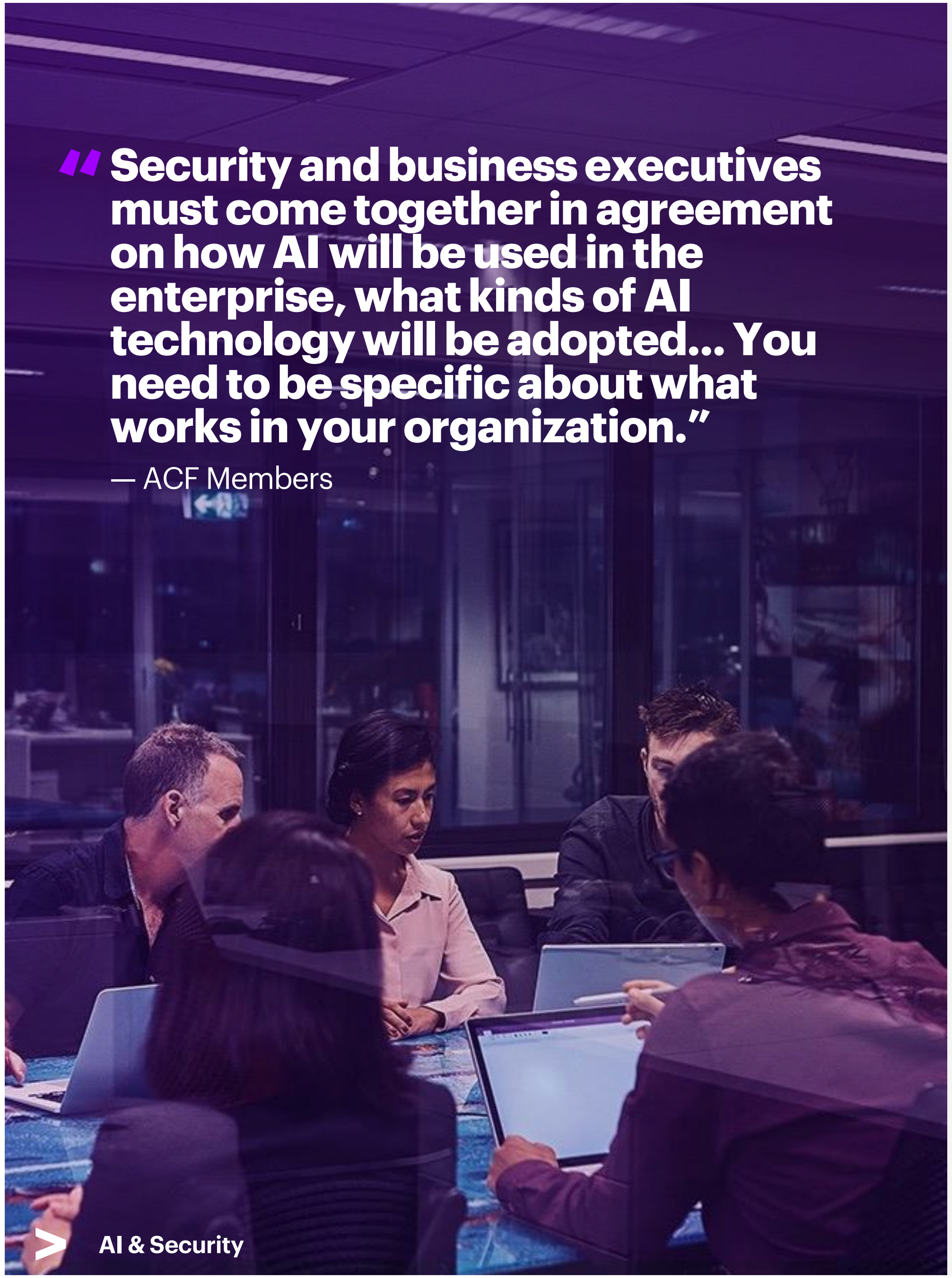


> “CISOs should demand secure, fit-for-purpose environments for Gen AI research and development. And they should lead the design and implementation of policy-driven controls to restrict access to data and other assets.”
>
> — ACF Subject Matter Expert

Supporting AI-based business initiatives (part 2)

Protection calls for securing Gen AI environments to reduce risks and enhance user experience while reinforcing Gen AI audit and traceability requirements. CISOs should demand secure, fit-for-purpose environments for Gen AI research and development. And they should lead the design and implementation of policy-driven controls to restrict access to data and other assets.

Defense priorities should include improved business continuity and resiliency and safeguarded Gen AI models and applications. Use Managed extended detection and response (MxDR) tools to monitor, detect and respond for Gen AI capabilities and technologies. Red team **exercises can help proactively identify and mitigate potential security risks and vulnerabilities.**



> **"Security and business executives must come together in agreement on how AI will be used in the enterprise, what kinds of AI technology will be adopted... You need to be specific about what works in your organization."**
>
> — ACF Members

Best practices

Forum members identified the following best practices:

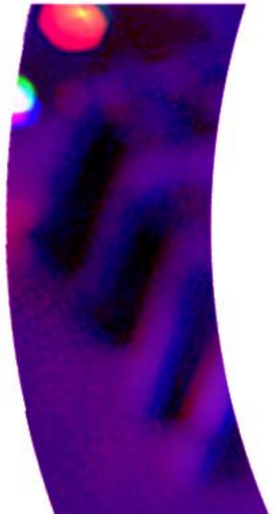
- **Security needs to lead in setting guardrails.** A subject matter expert spoke about the importance of an AI solutions architecture to guide application ideation, development, delivery, and scale.
- **Define "solutions architecture" for your business.** Security and business executives must come together in agreement on how AI will be used in the enterprise, what kinds of AI technology will be adopted. "You need to be specific about what works in your organization," said a subject matter expert.
- **Accelerate end user training.** "The train has left the station," said an ACF member. Security professionals need to take a lead role in helping their business-side colleagues respect the guardrails.
- **Focus on the details.** For example. a CISO stressed the value of reevaluating access controls and deploying safe zones to enable training and experimentation.
- **Don't wait for perfect.** AI is being found useful in the software development life cycle, for producing meeting summaries and for accelerating detection during red team exercises.
- **Find answers with your partners.** "Learn together with your partners to shape what is happening and how outcomes will look together," said a subject matter expert. That collaboration can possibly address concerns expressed about tech partners delivering trusted AI tools and models.

> **“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.