



Generative AI and Security

Accenture Cybersecurity Forum
Global Executive Leadership Network

1 August 2023
Session Summary



From the Accenture Leadership

An ACF member offered a troubling observation during our conversation about generative AI and security: “CISOs are already behind the eight ball in protecting the enterprise from employees who are using corporate data with consumer-based AI tools.” Another member, who serves on several boards, said: “Board members will be asking how enterprises will strike the right balance between enablement and protection.”

As we’ve seen with past transformational technologies—the Internet, cloud, SaaS—generative AI raises the bar for CISOs. In response to the challenge, and in light of time differences, on August 1, we held two forums, one for North America/European members and a second for APAC members. Both groups had many common questions and concerns. And they both shared their own experiences and ideas for navigating new challenges.

Thank you to all those who participated in the roundtable discussion. We hope you find the insights that emerged from the conversations useful as you address the opportunities and threats inherent in generative AI and large language models.

Cheers,



Paolo Dal Cin

Accenture Security Global Lead
ACF Executive Sponsor

[LinkedIn](#)

“Senior executive interest in generative AI is real. It is up to CISOs to help harness the hype and create value from this latest disruptive technology.”

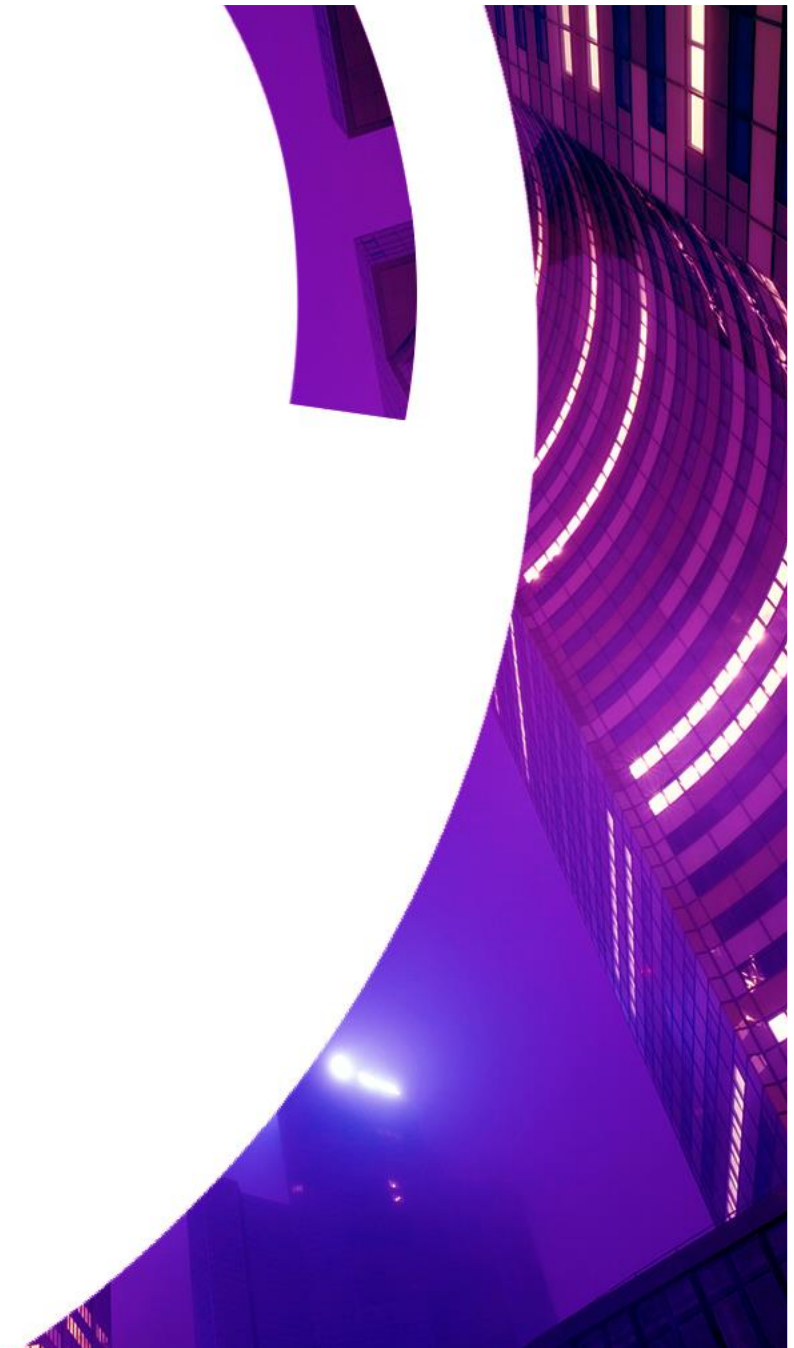


Kris Burkhardt

Accenture CISO
ACF Chair

[LinkedIn](#)

“CISOs are getting asked about a million questions a week about generative AI.”



Generative AI and Security



The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “Generative AI and Security” on August 1, 2023.

Forum members and their security operations face the challenges of both defending the enterprise from AI-enabled threat actors and in supporting the enterprise as it deploys AI-enabled solutions. AI enables threat actors with new weapons and requires improved defenses. Meanwhile the business and the enterprise seek to deploy AI to the advantage of the enterprise. And, the C-suite and the board want the CISO and the security organization to anticipate, monitor and mitigate the potential risks engendered by this new and evolving technology. What issues are CISOs facing in light of the rise of AI and what best practices might they deploy in light of the technology?

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.

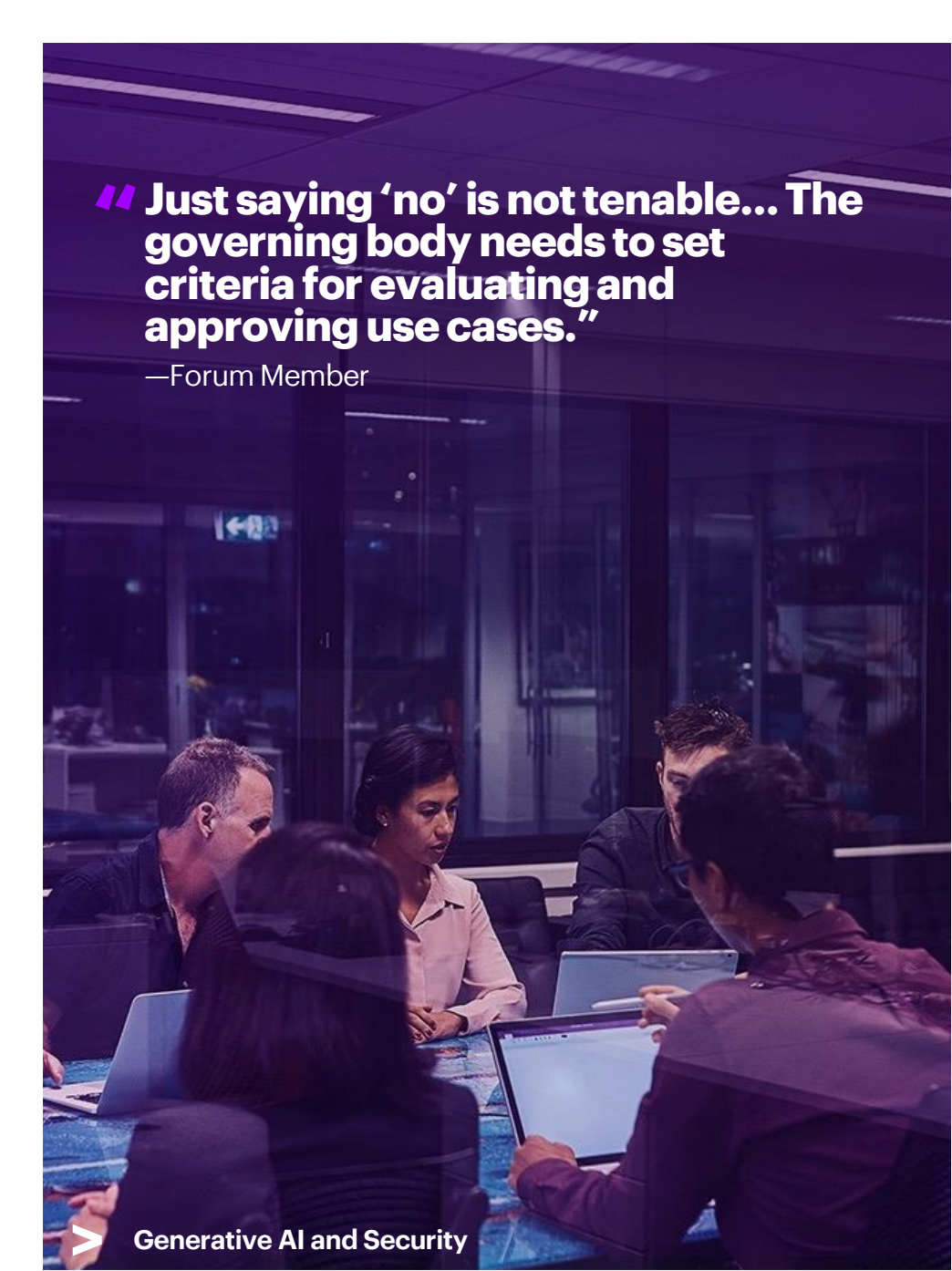
In this summary:

[Governance >](#)

[Education>](#)

[Defense >](#)

[Best Practices>](#)



“ Just saying ‘no’ is not tenable... The governing body needs to set criteria for evaluating and approving use cases.”

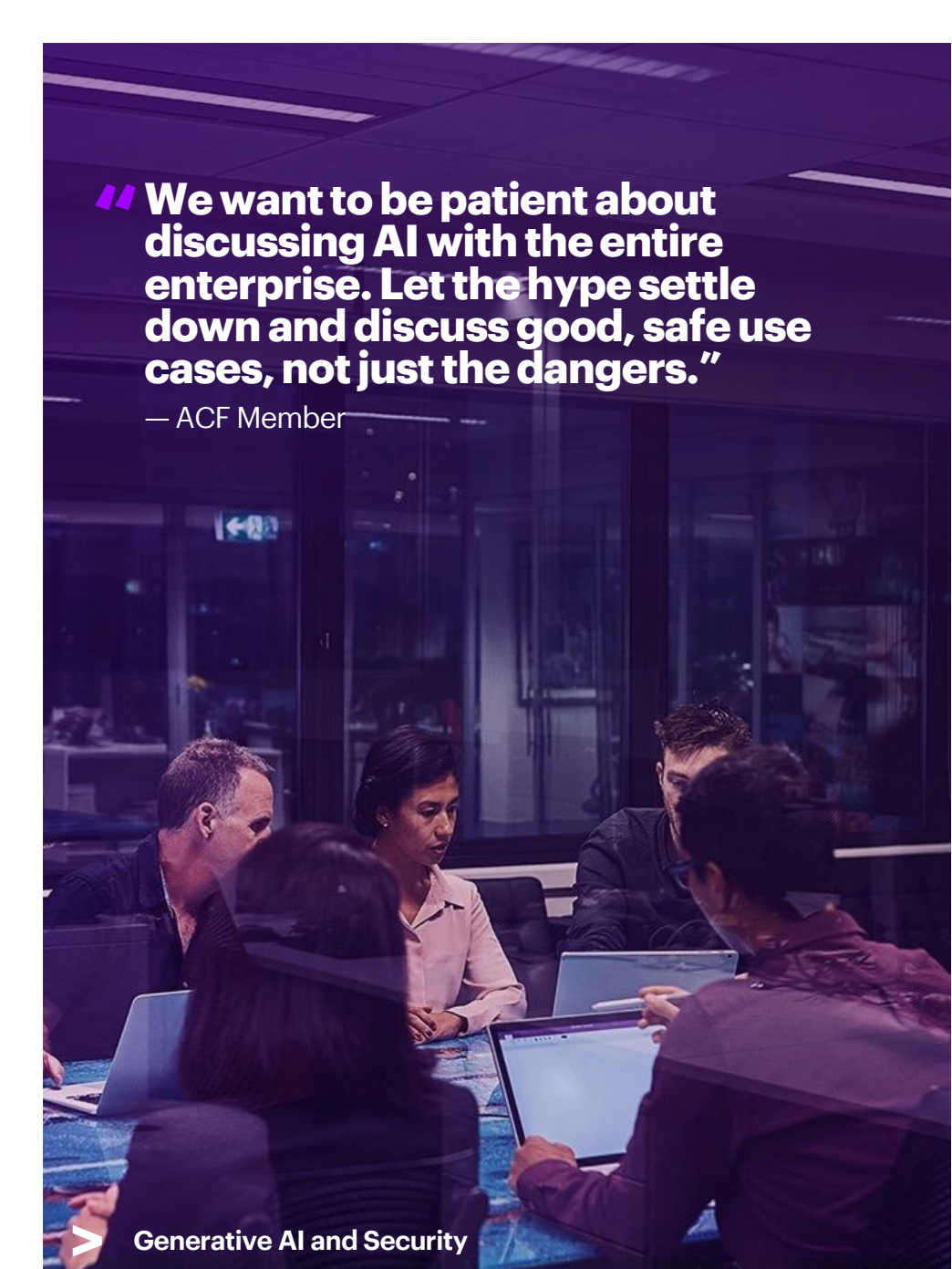
—Forum Member

Governance

CISOs and subject matter experts said getting generative AI governance right is critical in these early days of the latest transformational technology, particularly in light of the fact that ChatGPT and other tools are already in the public purview. Among their observations and recommendations:

- Create a cross-functional team including Legal, HR, IT, Risk and other functions to set guardrails and evaluate use cases for fit. One enterprise has an “Executive Information Management Committee”; another a “funnel group” for bi-weekly evaluation of use cases.
- The governance model should address regulatory requirements, particularly related to privacy and data security.
- “Just saying ‘no’ is not tenable,” said a Forum member. “The governing body needs to set criteria for evaluating and approving use cases.”
- Knowing data sources and data lineage are an important step in getting controls in place. A Forum member said: “Know your data and how it’s being used but accept that it will take time and a lot of fine tuning.”

A Forum member shared details about their approach to governance. “As part of our ‘response’ phase, I coordinated a three-day workshop with the response team (heads or senior leaders of Digital, Legal, IT, etc.) and invited consulting firms, technology firms (like Microsoft, to discuss Auto Pilot, Google, Open AI), external legal firms, and also government regulators from government. This was very helpful for us to understand different aspects on this issue and define the workgroups we needed to define policy and usage.”



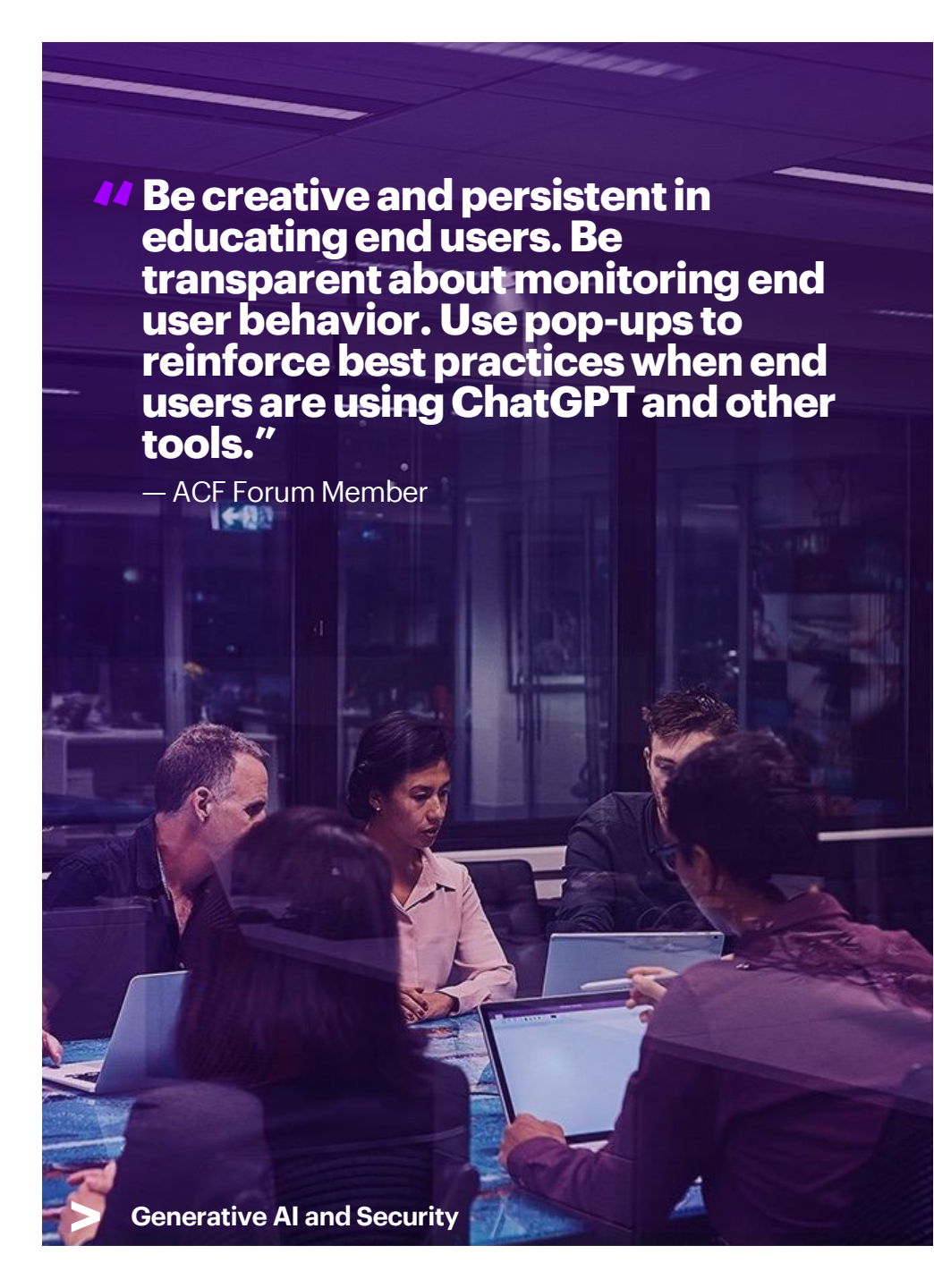
“ We want to be patient about discussing AI with the entire enterprise. Let the hype settle down and discuss good, safe use cases, not just the dangers.”

— ACF Member

Education – Part 1

Several Forum member said that education is the necessary foundation for implementing large language model applications. As one member said: “There’s a fundamental lack of understanding.” Among their suggestions:

- “The IT and security teams need a common language for discussing generative AI. We’ve brought in guest speakers to help the teams get on the same page.”
- “We want to be patient about discussing AI with the entire enterprise. Let the hype settle down and discuss good, safe use cases, not just the dangers.”
- Consider an event with the board to help them truly understand the enterprise-specific risks and opportunities of using generative AI.
- CISOs and CIOs should educate themselves about what’s coming next with large language models and watch internal and external business trends to gauge where the next opportunities and threats are coming from.



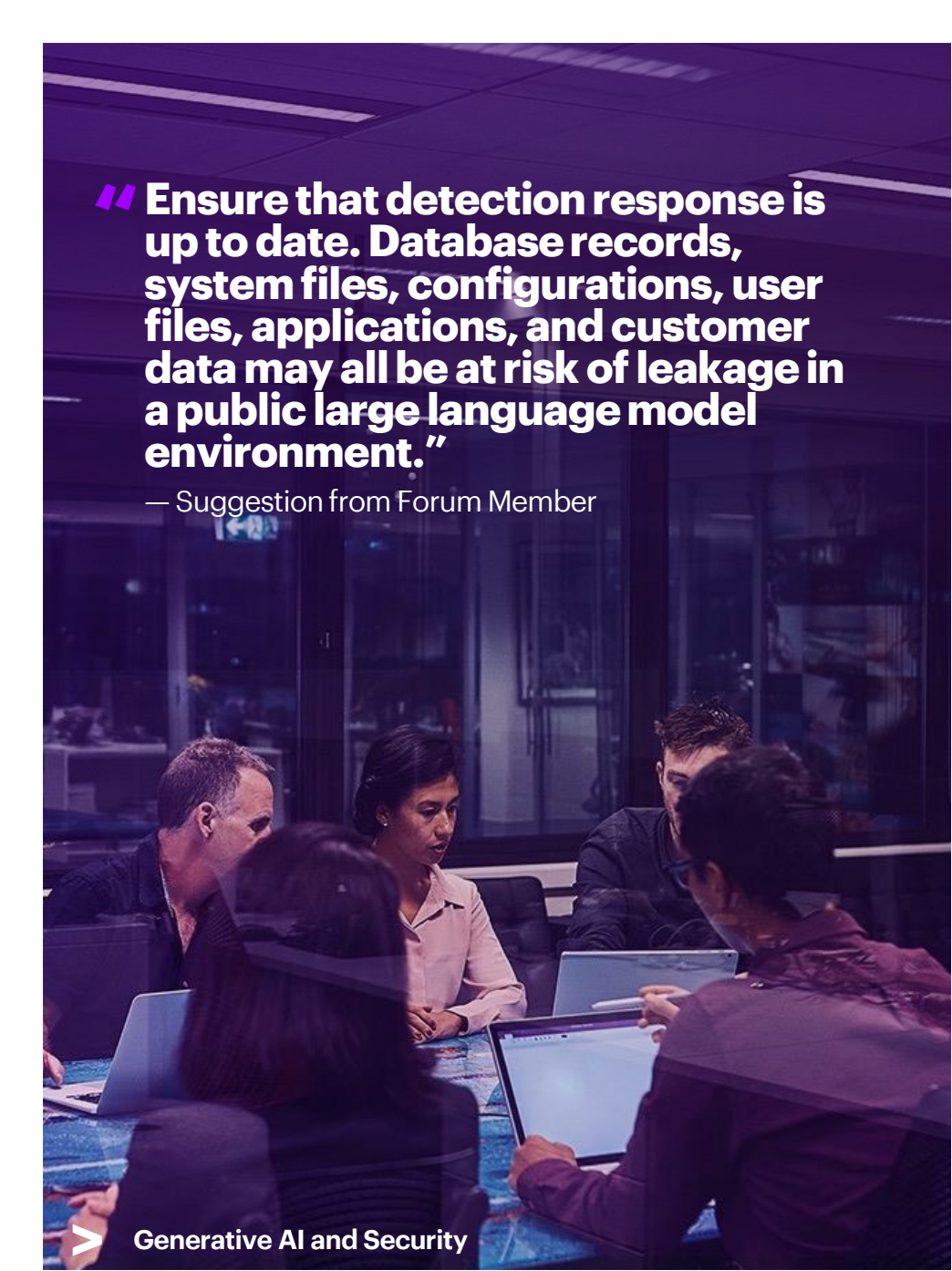
“ Be creative and persistent in educating end users. Be transparent about monitoring end user behavior. Use pop-ups to reinforce best practices when end users are using ChatGPT and other tools.”

— ACF Forum Member

Education – Part 2

Continued suggestions:

- Be creative and persistent in educating end users. Be transparent about monitoring end user behavior. Use pop-ups to reinforce best practices when end users are using ChatGPT and other tools. One Forum member said three of their last four monthly training sessions have been about generative AI.
- Another Forum member said: “We are encouraging people to experiment safely, such as using ChatGPT to plan the next holiday.”
- Be creative about educating the security team. One Forum member has asked everyone in the SOC for their thoughts on how AI will impact their jobs for both better and worse. Equip defenders with the skills to write effective prompts and queries. As one Forum member said: “Don’t let your IT team go crazy with AI without your lead.”
- A subject matter expert pointed to a recent article in Ars Technica, [“A jargon-free explanation of how AI large language models work,”](#) for ideas about how to communicate with other executives.



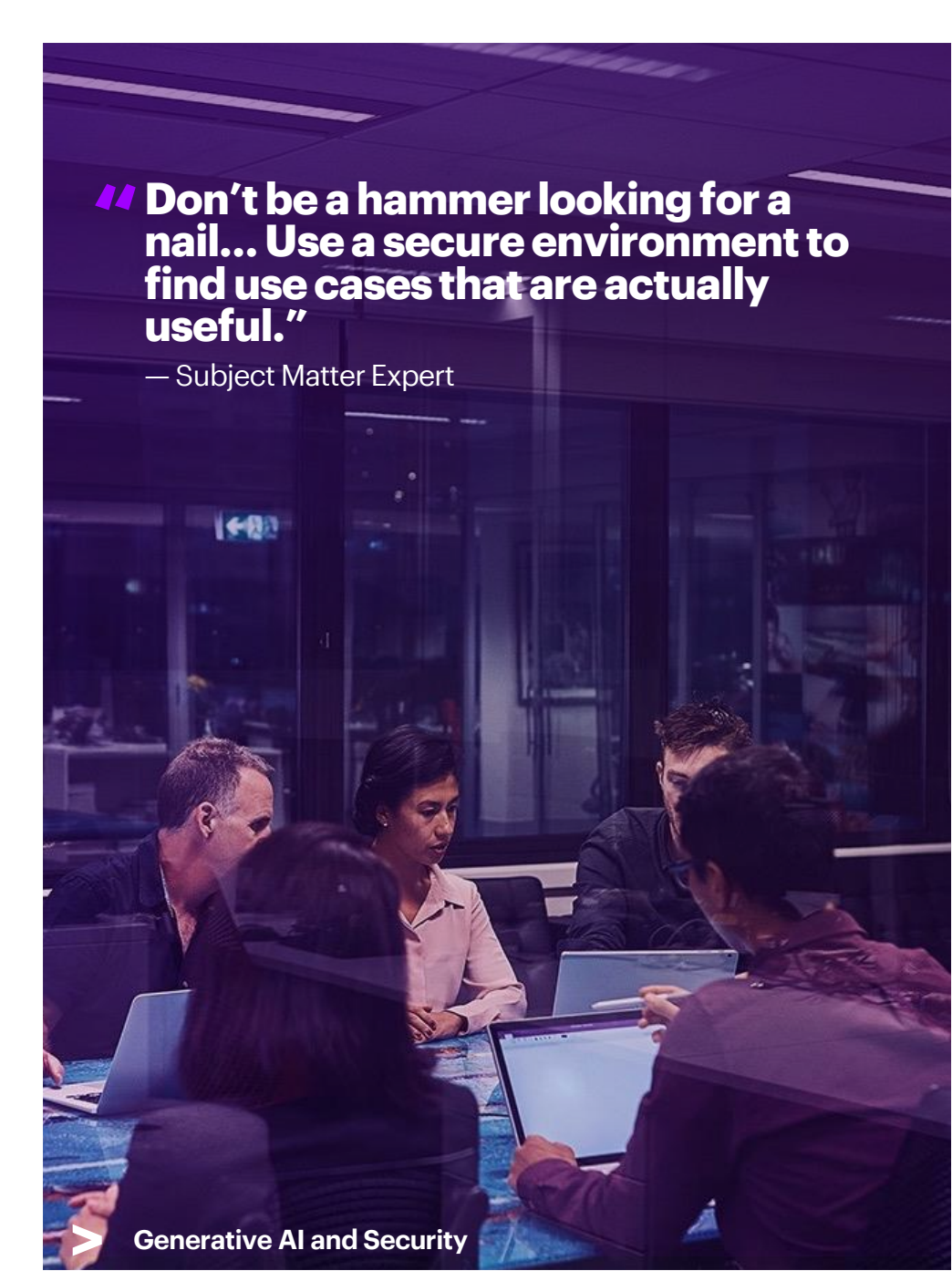
“ Ensure that detection response is up to date. Database records, system files, configurations, user files, applications, and customer data may all be at risk of leakage in a public large language model environment.”

— Suggestion from Forum Member

Defense

The basics of good hygiene still matter, perhaps more than ever, said a Forum member. Threat actors may be able to write more effective phishing campaigns more quickly, or reverse engineer patches to create new vulnerabilities, and enterprise defenses need to keep pace. Among the suggestions from Forum members:

- Revisit and revise the response playbook, particularly as it relates to human error data leakage.
- Ensure that detection response is up to date. Database records, system files, configurations, user files, applications, and customer data may all be at risk of leakage in a public large language model environment.
- Monitor threat intelligence about threat actor tools such as WormGPT.
- Address the fact confidential data may be widely available throughout the enterprise. Ensure your capabilities to detect abnormal behaviors are strong. Strengthen data and network access controls.



“ Don’t be a hammer looking for a nail... Use a secure environment to find use cases that are actually useful.”

— Subject Matter Expert

Best Practices – Part 1

- Create a secure enclave for experimenting with generative AI tools, use cases and controls. Several Forum members stressed the importance of a controlled environment. “Don’t be a hammer looking for a nail,” said a subject matter expert. “Use a secure environment to find use cases that are actually useful.” Don’t wait to get started. Another member added: “If we don’t disrupt ourselves, we won’t have control over our own destiny.”
- Develop use cases to demonstrate to the CEO, the board and other leaders what’s possible with generative AI. Also, highlight the privacy and intellectual property risks and propose criteria for evaluating the value of use cases that will inevitably be brought forward by other areas of the business.
- Create a defense plan that updates the response playbook. Control how users access tools. Set guidelines or policy about sharing internal information externally.



// Don't tell the board you're blocking the use of ChatGPT. There are too many avenues for users to gain access and it is not practical to close them all."

—Forum Member

Best Practices – Part 2

- Monitor network traffic and shadow models to prevent data from leaving the enterprise. As a subject matter expert said, "Users don't understand this, but once corporate data is out in the public environment, you're not getting it back."
- Don't think you can easily legislate the use of commonly available tools. A subject matter expert said: "Don't tell the board you're blocking the use of ChatGPT. There are too many avenues for users to gain access and it is not practical to close them all."
- Test how generative AI can ease burdens on the SOC, for example in writing incident reports.
- Expect the White House to issue an executive order on AI, as was done in May 2021, with the "Executive Order on Improving the Nation's Cybersecurity."



**“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 © 2023 Accenture All rights reserved.
Accenture, and its logo are trademarks of Accenture.

