



10 key soundbites from KPMG's Cyber Open Day



"Agents are now the apex predators."



AI is giving attackers capabilities that once required nation-state resources, transforming the speed, scale and economics of cyberattacks.

But AI can also shift the economics of defence. For decades, the economics of cybersecurity favoured the attacker: attacks were cheap; defence was expensive. AI is beginning to rewrite that equation.

As the economics of attack change, security testing must change with them, uncovering weaknesses before adversaries can exploit them.

Build cyber confidence

with KPMG's AI-Assisted Security Testing to test your defences against evolving threats and identify weaknesses earlier.

"27 seconds is now an eternity."



Last year, the fastest recorded adversary breakout time fell to just 27 seconds, down from 51 seconds the year before. With frontier AI, adversaries can now take over a network almost immediately, making 27 seconds feel like an eternity.

Cyber defence is becoming a race measured in seconds. When the speed of cyberattacks is compressing the time available to detect, assess and respond, continuous visibility across IT and operational technology assets is critical to identifying vulnerabilities before they can be exploited.

Build cyber confidence

with KPMG's Asset Management & Vulnerability Management solution a solution developed with ServiceNow to help organisations identify exposure earlier, prioritise vulnerabilities and respond with greater confidence.

"Invisible agent actions are creating invisible risks."



AI agents don't just generate answers. They act. They call tools, access systems, trigger processes and use memory. And when those actions are invisible, so is the risk.

As agents become more autonomous, visibility must extend beyond prompts and model outputs to the actions they take across tools, processes, memory and underlying systems. Without that visibility, organisations cannot reliably identify when an agent steps outside its approved boundaries.

Trust starts with visibility. Because you cannot control what you cannot see.

Build cyber confidence

with KPMG's Agentic AI Runtime Governance, a solution that helps organisations observe agent behaviour, monitor actions and intervene when activity moves outside defined parameters

"AI agents should have KPIs and retirement plans."



As AI agents become part of the workforce, they need to be managed like one.

Every agent should have a clear purpose, an accountable owner, defined responsibilities, access boundaries and lifecycle controls. And when an agent no longer performs as intended, it should be improved, constrained or retired, with a clear record of why.

The principle is simple: If AI agents are joining the workforce, they need job descriptions, managers, performance reviews and clear exit plans.

Build cyber confidence

with KPMG's Identity & Access Management and Non-Human Identity, a solution that helps organisations govern agents from deployment through to retirement.

"The autonomous enterprise changes the trust model."



An AI agent is no longer just software you use. It is an identity you authorise to act. When software starts acting on your behalf, trust can no longer be assumed. It must be proven. Policies alone cannot provide assurance over autonomous activity.

Organisations require verifiable evidence of what an AI agent did, what it accessed and whether it operated within its authority. In an autonomous enterprise, trust is not a policy. It is evidence.

Build cyber confidence

with KPMG's Agentic Control Assurance, a solution that embeds control and evidence into agent-enabled workflows, supporting clearer accountability and auditability.

"Human oversight plus agents is the new operating model."



Work can be automated.
Accountability cannot.

AI agents can increasingly execute complex, multi-step processes without constant human intervention. But autonomy cannot become an excuse for abdication.

The answer is not to have humans approve every step. It is to put them on the loop: setting objectives and boundaries, defining when an agent must escalate, and reviewing the outcomes. AI can take over the work, but it cannot take over accountability.

Build cyber confidence

with KPMG's Agentic AI and Security Governance Blueprint, a solution that helps organisations establish clearer roles, guardrails and accountability as AI agents become part of the workforce.

"It is a false choice to move safely or quickly. You can have both."

Speed without control produces mistakes faster. A wrong answer delivered at machine speed is still a wrong answer. That is why the choice between moving quickly and moving safely is a false one.

Controls should not be barriers added after innovation happens. They should be built into how AI operates from the start. Safety and speed are not opposites when controls are designed in from the start.

The goal isn't to slow AI down. It's to make speed safe.

Build cyber confidence

with KPMG's AI Governance in the Age of Shadow AI, a solution developed with CrowdStrike that helps organisations govern AI usage while continuing to innovate.

"More than ever, defence is the best offence."



Don't wait for an attack to find out whether your defences work.

Adversaries will use every technology and technique available to find a way in. Organisations need to apply the same mindset to defence, testing critical environments as an attacker would to uncover weaknesses before they can be exploited.

To build a stronger defence, you must test it like an attacker.

Build cyber confidence

with KPMG's SAP Security solution with SecurityBridge, a solution that helps organisations improve visibility, identify vulnerabilities and strengthen protection across critical SAP environments.

"Legacy thinking will not address frontier challenges."



The greatest emerging risks are often the ones organisations have the least time to prepare for.

Quantum computing, for example, could challenge the encryption methods organisations rely on today. Waiting until that threat materialises may leave insufficient time to understand exposure and prepare a response. The same applies to frontier AI.

The fundamentals of governance still hold, but they must operate continuously as agents create code, access data, make decisions and take action. You don't need to reinvent governance for every new technology. You need it to keep pace with it.

The fundamentals haven't changed.
The frontier has.

Build cyber confidence

In Taming Schrödinger's cat: Why firms should integrate quantum readiness into their digital strategy now, Gerry Chng, Partner and Head of Cyber at KPMG in Singapore, explains why quantum readiness should be incorporated into digital strategy now.

"Cyber confidence cannot stay in the tech department."



Every supplier, system, operation and critical business relationship can create risk. So cyber can no longer be managed as a standalone technology issue. Confidence must be built across the enterprise, connecting how organisations defend against threats, govern cyber and AI risk, and scale transformation securely.

Cyber risk follows the business, so cyber confidence has to as well.

Build cyber confidence

with KPMG's Third-Party Trust Intelligence, a solution that uses AI agents to support a more connected and responsive approach to third-party risk management.

Experience cyber confidence. Speak to our cyber experts.



Gerry Chng

Partner, Head of Cyber, Advisory
KPMG in Singapore



Eddie Toh

Partner, Cyber, Advisory and Head of
Forensic Technology, Asia Pacific, Advisory
KPMG in Singapore



Wendy Lim

Partner, Cyber, Advisory
KPMG in Singapore



Lee Ser Yen

Partner, Cyber, Advisory
KPMG in Singapore



kpmg.com/sg

© 2026 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Document Classification: KPMG Public