The Leadership Agenda

Explore now

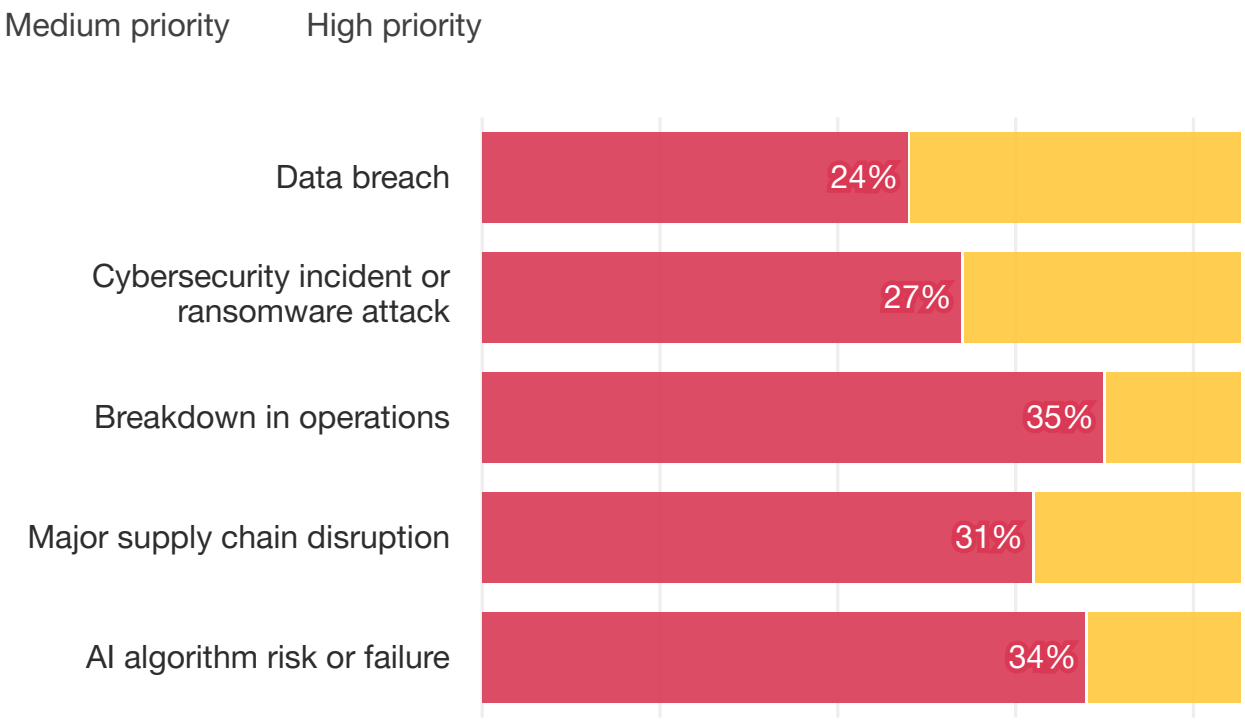
Seven crucial actions for managing AI risks

Executives need to give higher priority to the fast-evolving risks of generative AI. They can start with a few key trust-building actions.

Data 2 minute read

Share

Executives' top risk priorities



Percentages are the share of 500 business executives surveyed.
Q: How is your company prioritising its efforts to reduce the likelihood of the following happening?
Source: PwC 2023 Trust Survey

When PwC's 2023 Trust Survey asked 500 executives how they prioritised major risks that could erode trust in their company, the threats associated with AI fell well below other cyber-related ones like a data breach or a ransomware attack. The findings suggest that many business leaders have yet to grasp the urgency of the challenges that generative AI poses. To name just a few: offensive or misleading content; deepfakes intended to spread misinformation or urge stakeholders to share sensitive information; authoritatively presented information that's wholly inaccurate; the exposure of anonymised stakeholders' identity; content reproduced illegally from copyrighted material; inadvertent sharing of intellectual property—the list is formidable and growing.

How can companies harness the revolutionary power of generative AI—which, among other uses, can help automate customer service and high-volume tasks, provide useful summaries of proprietary or public data and research, and even write software code—without imperilling the trust of stakeholders? They can start by making the following moves:

Set risk-based priorities. Some generative AI risks are more important to your stakeholders than others. Adjust or establish escalation frameworks so that governance, compliance, risk, internal audit and AI teams give the greatest attention to the greatest risks.

Revamp cyber, data and privacy protections. Update cybersecurity, data governance and privacy protocols to help mitigate the risks of malicious actors' generative AI inferring private data, unravelling identities or conducting cyberattacks.

Address opacity risk. With some generative AI systems, the "foundation model," or neural network, used to produce outputs isn't disclosed or readily accessible to users, making it impossible to unravel why a certain system generated certain results. Identify these systems, and consider what practices can support their fairness, accuracy and compliance.

Equip stakeholders for responsible use and oversight. Teach employees the basics of how generative AI works—and also when to use it and when not to. They'll also need to learn when and how to verify or modify outputs. Provide compliance and legal teams with skills and software to identify intellectual property violations

and other related risks, reinforcing AI governance guidelines and other governance structures (e.g., privacy and cybersecurity) that may already be in place.

Monitor third parties. Know which of your vendors provides content or services that use generative AI, how they manage the related risks and what your possible exposure may be.

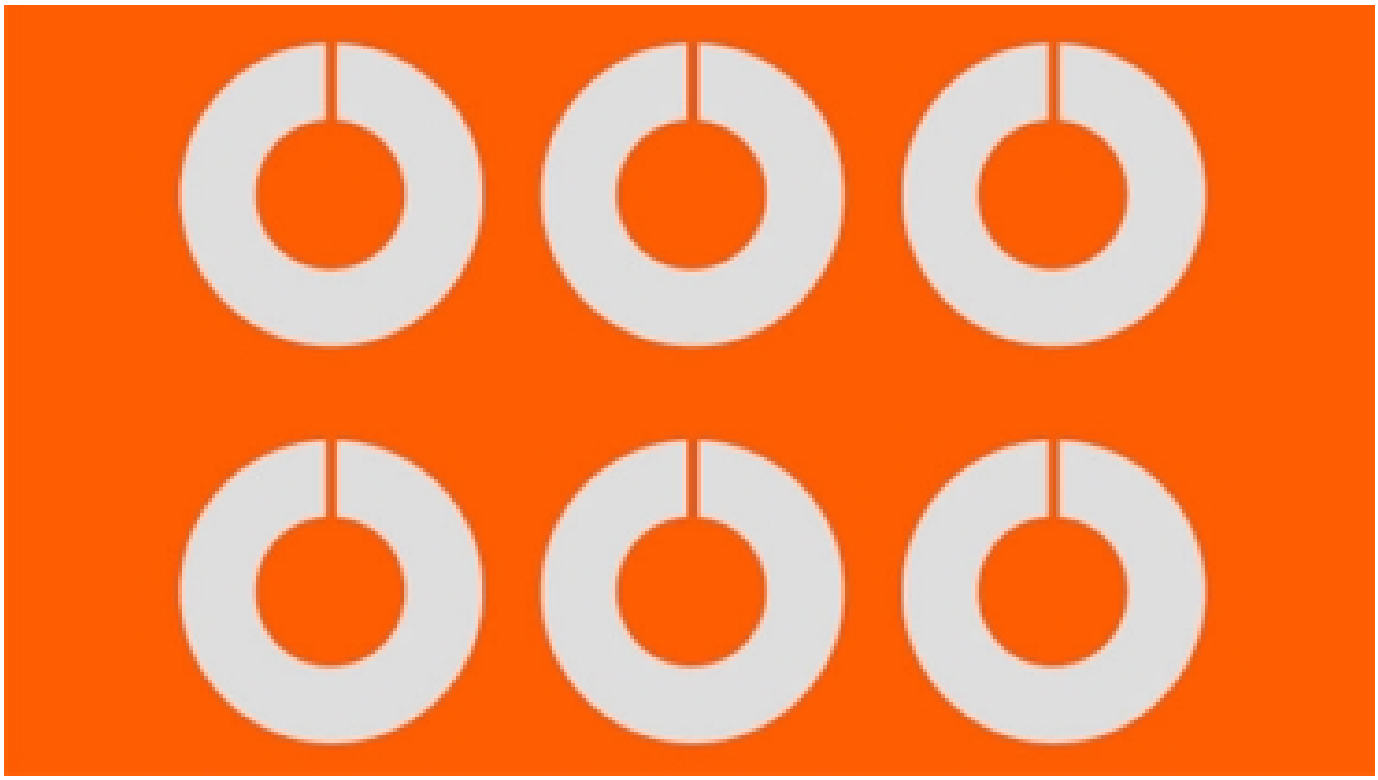
Watch the regulatory landscape. Policymakers around the world are issuing more and more guidance on AI development and usage. This guidance is still a patchwork, not a complete regulatory framework, but new rules are continually emerging.

Add automated oversight. With generative-AI-created content ever more common, consider emerging software tools to identify AI-generated content, verify its accuracy, assess it for bias or privacy violations, and add citations (or warnings) as needed.

These actions are the foundation of responsible AI, and they should become a fundamental part of your company's AI playbook.

Learn more ways that companies can harness the power of generative AI responsibly.

Read more

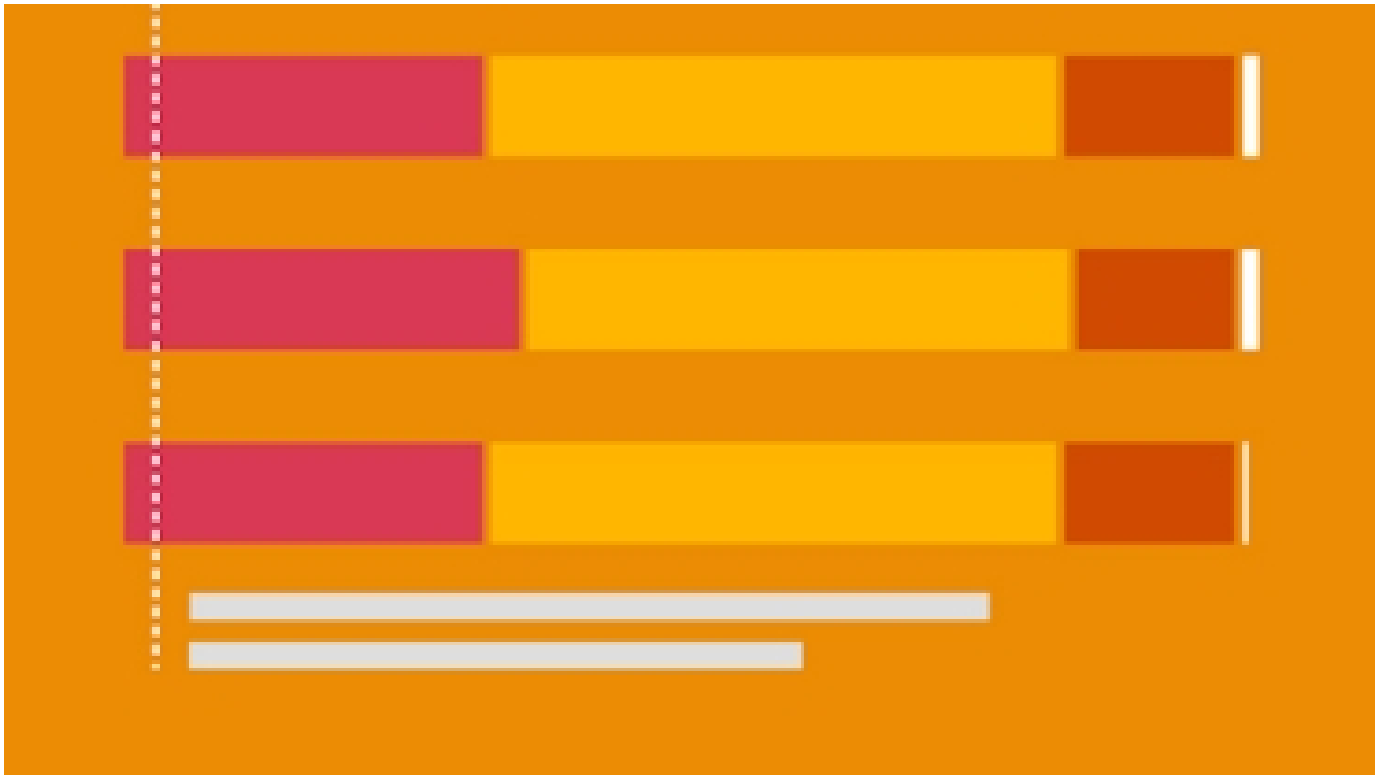


Companies face a big trust gap on data security

A global PwC survey shows that a large share of consumers are very worried about what happens with their data. Businesses should be too.

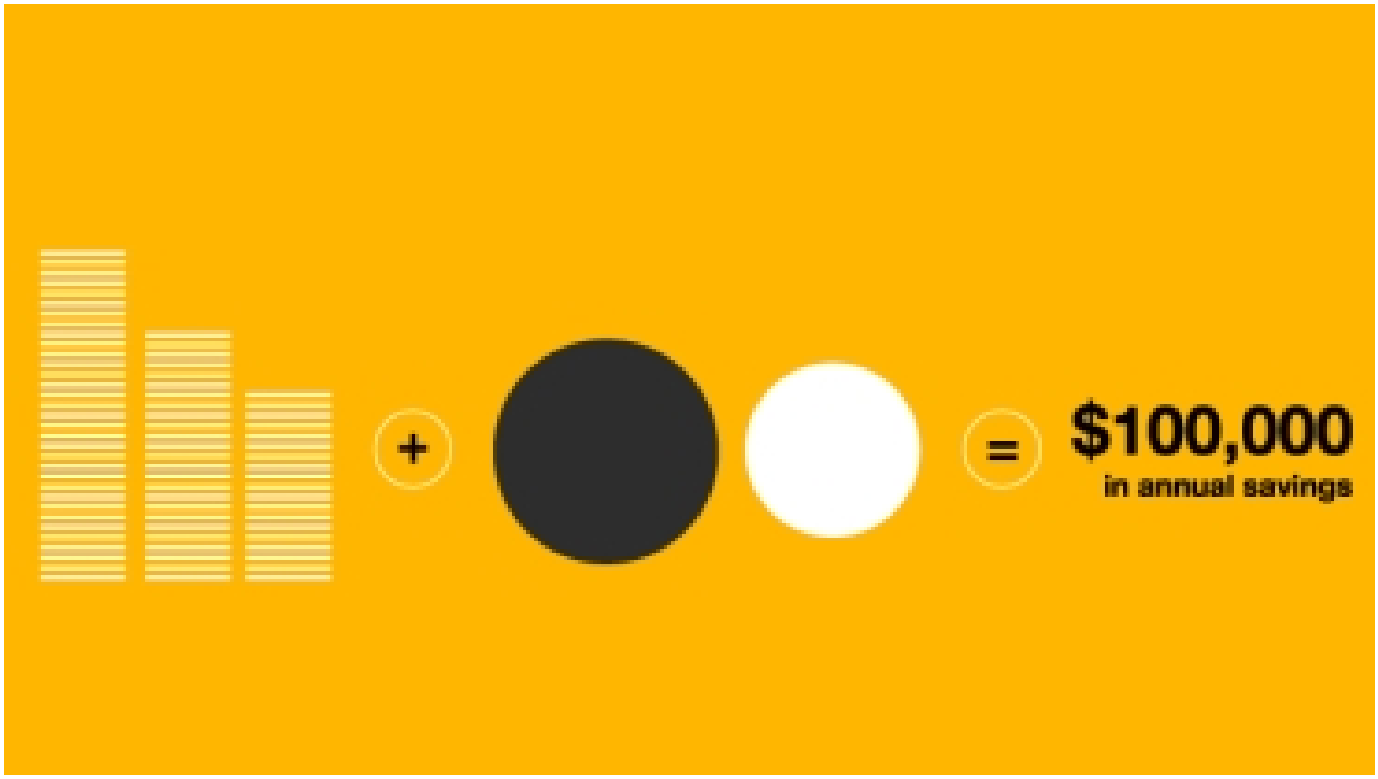
Geopolitical conflict requires a new cyber toolkit

Senior executives are upping their investment in cybersecurity in the face of global instability, according to PwC's latest CEO Survey, and rightly so.



Effective cybersecurity starts at the top

The results of PwC's latest Global Digital Trust Insights Survey show that today's cyber risks are too big for CISOs to handle on their own.



How AI can crush the paperwork problem

Automating data extraction may not be as sexy as chatbots, but it's got massive potential to reduce costs and boost productivity.

Contact us

Ilana Golbin

Director and Responsible AI Lead, PwC US

Email

Mir Kashifuddin

Data Risk & Privacy Leader, PwC US

Email

Jennifer Kosar

Trust and Transparency Solutions Leader, PwC US

Email