January 2024

Decoding CEO Sentiments: The CISOs' guide to the 27th PwC CEO Survey

pwc

pwc.nl/ceosurvey

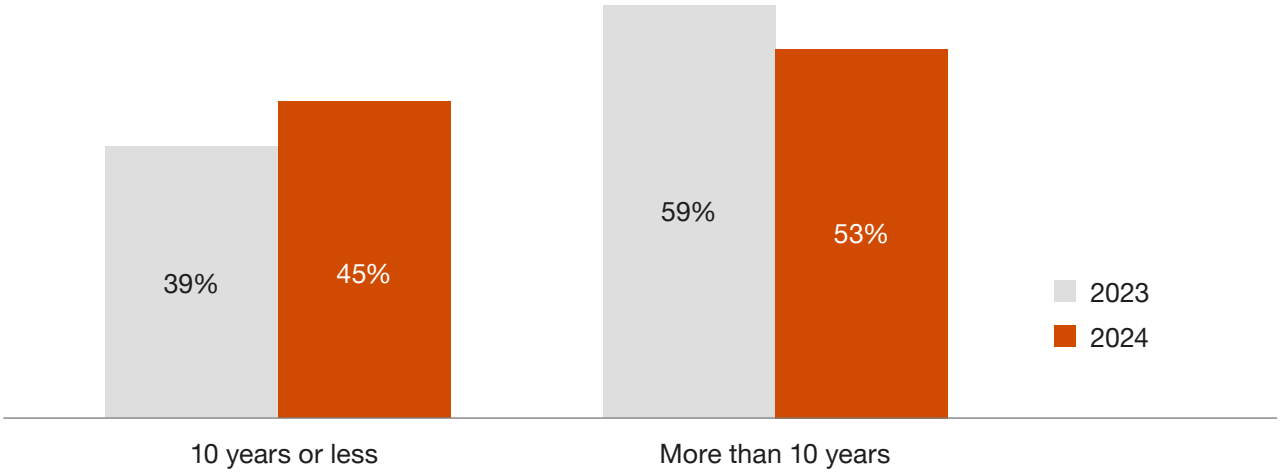
The PwC CEO survey, an annual barometer of executive sentiment, provides multiple data points that capture the viewpoints of CEOs on important topics impacting their businesses. The 27th edition, published on January 15 2024, paints a picture of CEOs navigating through economic uncertainties and recalibrating priorities. It also provides key insights that can help cybersecurity teams and CISOs understand the direction their organisation is headed in and current sentiments on cyber risk.

In this paper, we highlight 5 metrics from the survey that speak directly to the theme of cyber, and their implications for the CISO function. We also share recommendations for CISOs to take action based on these insights.

Metric 1: The reinvention imperative

The reinvention imperative appears to be accelerating

Question: if your company continues running on its current path, for how long do you think your business will be economically viable?



Note: Percentages shown for a given year may not total 100 due to rounding.

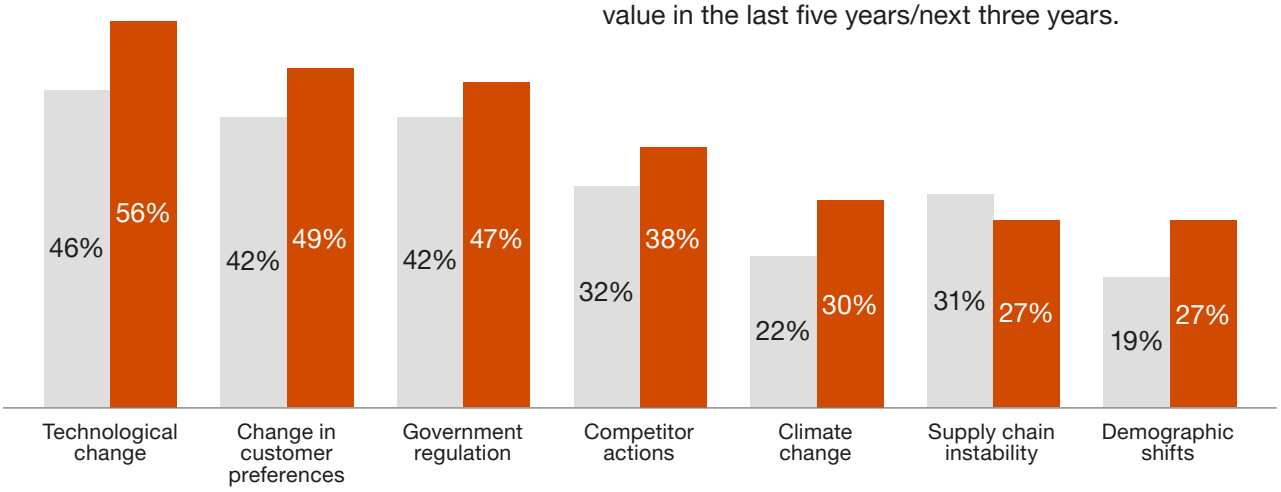
CEOs perceive a heightened sense of urgency in embracing accelerations in mega trends, and navigating the disruptive forces of climate change. The survey indicates a growing realisation among CEOs that their businesses may no longer be viable within the next decade, signaling a need for transformation. For CISOs, this underscores the inevitability

of organisational change, where business and operating models may undergo profound changes. The key takeaway for security teams is clear: to maintain relevance and influence, CISOs should anticipate and prepare for changes within their organisations.

Metric 2: External Pressures drive this imperative

The impetus to reinvent is intensifying

Question: Please indicate the extent to which the following factors have driven/will drive changes to the way your company creates, delivers and captures value in the last five years/next three years.



Showing only to a 'large extent' and 'to a very large extent' responses.

CEOs are bracing for increased pressure from external factors, ranging from technological advancements to evolving customer preferences and impending regulatory changes. Technological changes and government regulations are particularly relevant for security organisations.

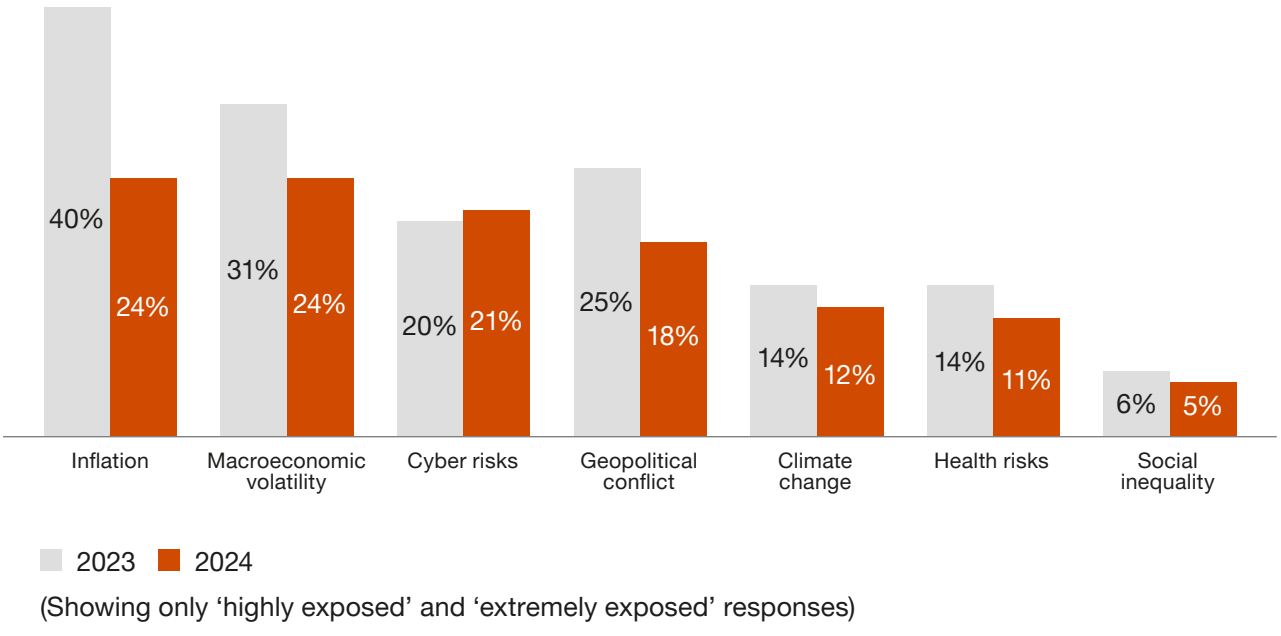
For CISOs, this metric rings alarms and presents an opportunity. On the technological front, it's crucial to anticipate how innovations like Artificial Intelligence (AI) will impact the competitive landscape (more on that later in the paper). Simultaneously, new (and changing) regulatory requirements in different facets of the business require an efficient, integrated and proactive approach to compliance. Some legislations like NIS2, the Cyber Resilience Act and DORA have a major security focus, while others like the DSA, DMA, DAC7 and the AI Act have broader business implications, which also mandate security requirements.

Security teams should actively engage CEOs and Chief Compliance Officers (CCOs) in conversations about impending regulations. The role of CISOs should be to act as solution providers, facilitating the understanding of the executives on the expectations arising from the different regulations with security requirements, and integrating these compliance requirements with their security framework, simplifying the process of showing compliance to regulations on security and other domains.

Metric 3: Cyber remains a top concern

Over the near term, CEOs are feeling less threatened

Question: How exposed do you believe your company will be to the following key threats in the next 12 months?



(Showing only 'highly exposed' and 'extremely exposed' responses)

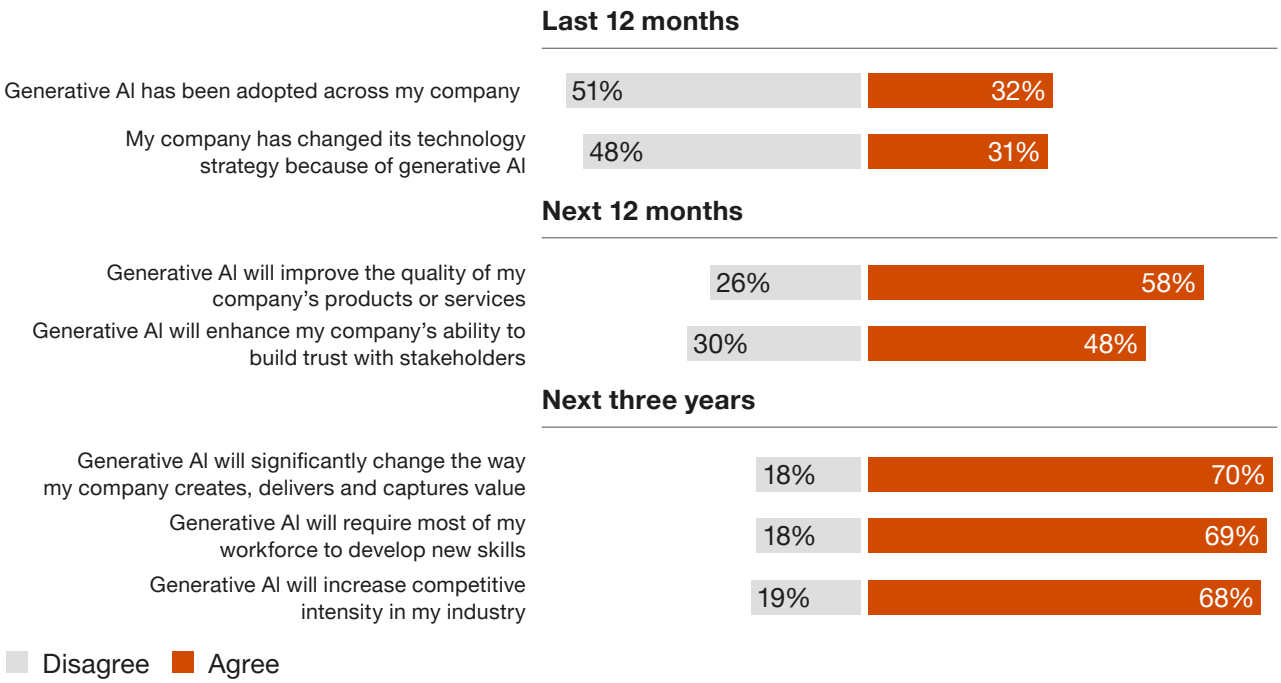
While CEOs have gradually shifted their concerns from macroeconomic issues, the survey indicates that cyber threats still loom large in their considerations, with cyber risks being the only top concern from 2023 that saw an increase this year. Geopolitical conflicts also rank high among CEOs' concerns, and given the extension of conflicts into the realm of cyber warfare, companies now face an elevated level of cyber risk exposure.

From a CISO's perspective, understanding these changing threat perceptions is crucial. It provides an opportunity to collaboratively define the next iteration of the cyber strategy for the organisation. Initiating conversations with CEOs about their perceptions of cyber risks and aligning on gaps in the organisation's security posture becomes imperative. CISOs must not only provide clear visibility into the cybersecurity status but also collaborate with CEOs to proactively address emerging threats.

Metric 4: The AI opportunity

Although generative AI adoption and strategic integration has been somewhat limited, CEOs anticipate greater impact ahead

Question: To what extent do you agree or disagree with the following statements about generative AI?



Note: Disagree is the sum of 'slightly disagree,' 'moderately disagree' and 'strongly disagree' responses; Agree is the sum of 'slightly agree, 'moderately agree' and 'strongly agree' responses.
Source: PwC's 27th Annual Global CEO Survey | www.ceosurvey.pwc | © 2024 PwC. All rights reserved.

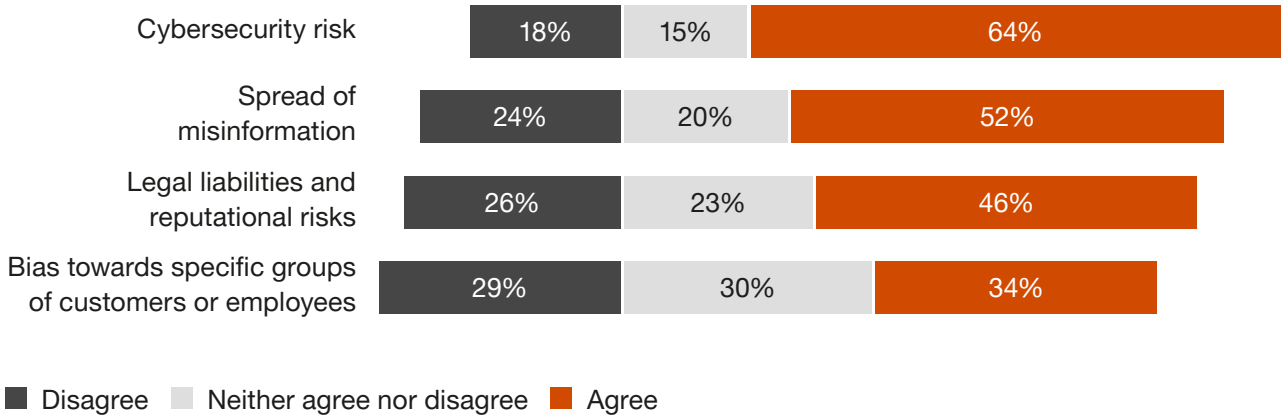
Generative AI is emerging as a transformative force, with CEOs recognising its potential to disrupt traditional business models. Expectations include increased competition, changes to business models, and the need for new skills within the workforce. For CISOs, aligning security strategies with the organisation's AI adoption journey is paramount. Notably, technological shifts are expected to not only intensify competition but also necessitate a reinvention of the way businesses operate.

CISOs should actively participate in discussions with Chief Technology Officers (CTOs) and other technology-focused executives to understand the organisation's current stage of AI adoption. This will enable security teams to take the appropriate steps. Initiating (and continuing) dialogue on securing AI use-cases and facilitating secure adoption should be at the forefront of every CISO's agenda.

Metric 5: CEO Concerns about Generative AI's Impact on Cyber Risk

When it comes to generative AI risks, CEOs are most concerned about cybersecurity

Question: To what extent do you agree or disagree that generative AI is likely to increase the following in your company in the next 12 months?



Note: Disagree is the sum of 'slightly disagree', 'moderately disagree' and 'strongly disagree' responses; Agree is the sum of 'slightly agree,' 'moderately agree' and 'strongly agree' responses. Percentages shown may not total 100 due to rounding. Source: PwC's 27th Annual Global CEO Survey | www.ceosurvey.pwc | © 2024 PwC. All rights reserved.

A striking revelation from the survey is that CEOs' biggest concern regarding Generative AI is its potential impact on their cyber risk posture. This emphasises the intricate relationship between technological advancements and cybersecurity challenges, and why cybersecurity should be considered as part of every business change discussion.

CISOs must seize this opportunity to engage with the organisation, gaining insights into ongoing AI initiatives. Developing robust security strategies to counter potential biases, misinformation, and cyber threats associated with AI adoption becomes a critical mandate. This metric underscores the need for security teams to be not just reactive but proactive architects of secure technological integration.

Key Takeaways for the CISO

As we decode the CEO sentiments, several key takeaways emerge for CISOs and their teams.

1. Discuss the findings with your CxOs.

- To understand where your company lands on some of the survey results and what that could mean for the future plans of the organisation. Take the opportunity to discuss anticipated external pressures, technological shifts and possible changes to the organisation's business or operating model.

2. Initiate conversations on regulations with the CCO:

- Analyse applicable security-focused regulations and collaborate with enterprise compliance teams on broader regulations to identify requirements towards the organisation from a security perspective.
- Integrate requirements from each regulation into a security risk and control framework (factoring overlaps between requirements from different regulations), and identify key initiatives to be executed to meet the identified requirements. This will result in reduced implementation (compliance) costs, improved efficiency and clarity for the organisation.
- Establish interfaces with the enterprise compliance program (and framework) to ensure that security compliance efforts support the attainment (and proof of evidence) of compliance with broader regulations like the DAC7.

3. Align Security Strategies with AI Adoption:

- Collaborate with the CTO, CEO and business unit leaders to understand the current level of AI adoption within the organisation and planned actions for the future.
- Identify and communicate security use cases for AI that will improve the effectiveness and efficiency of the security organisation.
- Evolve your security strategy to include measures for mitigation of threats arising as a result of AI adoption in the organisation, and advancement of security capabilities utilising AI, enabling the organisation to unlock anticipated benefits.

4. Educate CxO Colleagues:

- Elevate awareness among CxO colleagues about the pivotal role of cybersecurity in business reinvention and digitisation.
- Highlight proactive measures taken by the security team to address evolving threats and contribute to organisational success.
- Position cybersecurity not just as a protective shield but as an enabler of innovation and secure business practices.

PwC contacts

Angeli Hoekstra
Cybersecurity & Identity Partner
E: hoekstra.angeli@pwc.com

Bram van Tiel
Cybersecurity & Privacy Partner
E: bram.van.tiel@pwc.com

Mimoent Haddouti
Cybersecurity Partner
E: mimoent.haddouti@pwc.com

Peter Avamale
Cybersecurity Director
E: peter.avamale@pwc.com

© 2024 PricewaterhouseCoopers B.V. (KvK 34180289). All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with nearly 364,000 people who are committed to delivering quality in assurance, advisory and tax services. At PwC in the Netherlands over 5,700 people work together. Find out more and tell us what matters to you by visiting us at www.pwc.nl.