



2026 Global Digital Trust Insights

Switzerland edition

New world, new rules:
Cybersecurity in an era of uncertainty



Agenda

- 
- 1 The global overview
 - 2 Risk and threat landscape
 - 3 Cyber strategy and operations
 - 4 Artificial intelligence
 - 5 Quantum computing readiness
 - 6 Cyber leadership

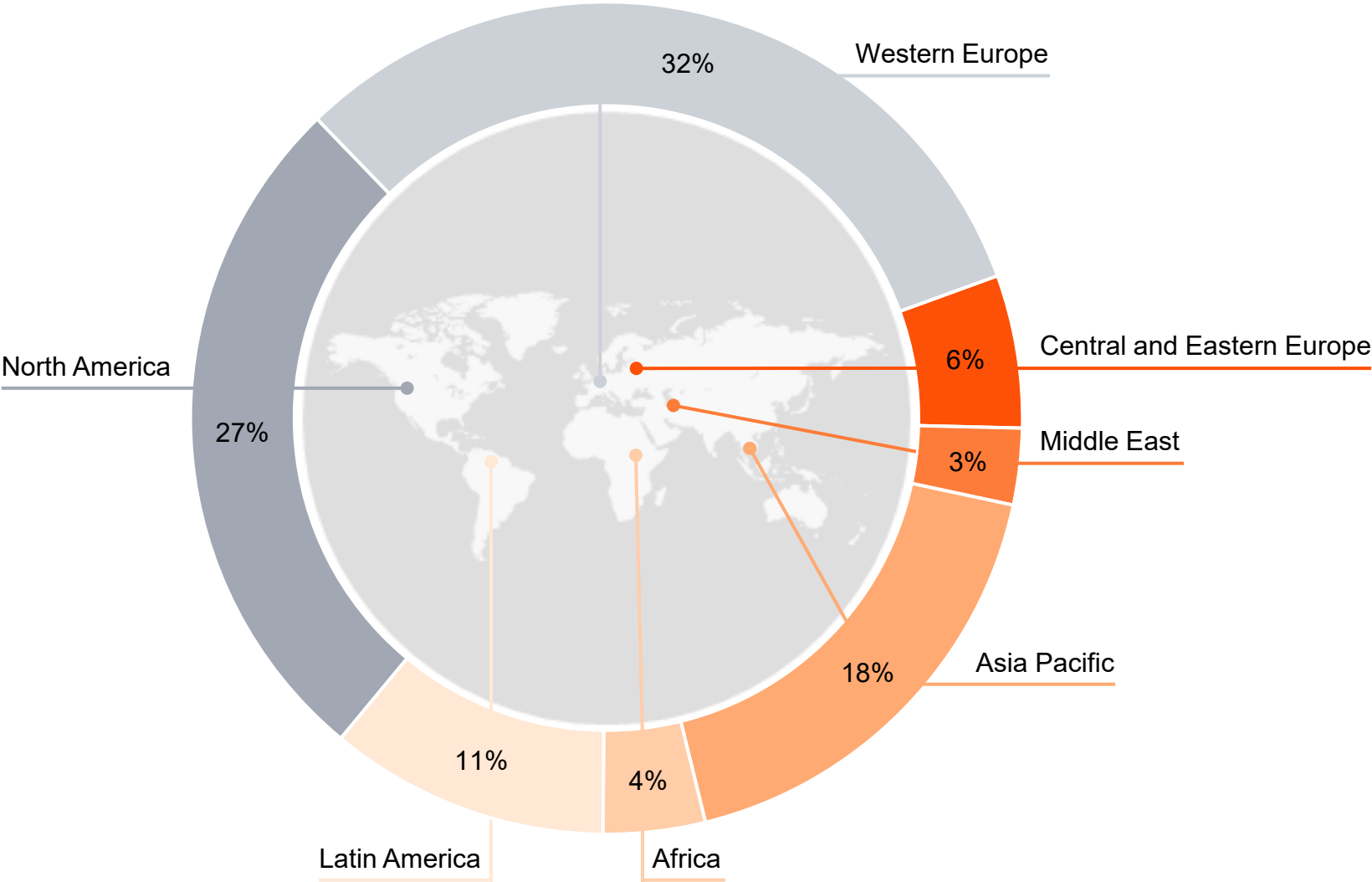


The global overview

**Where investment meets
impact**

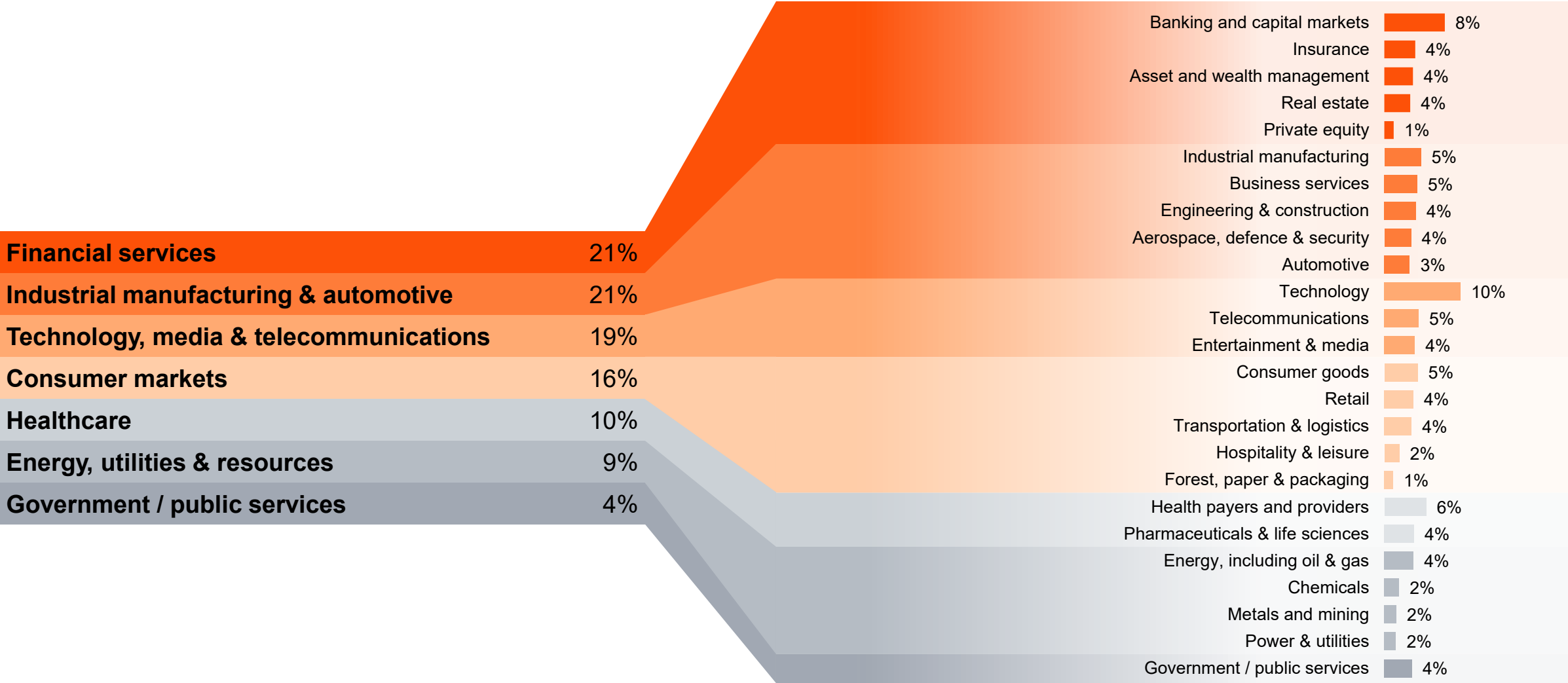
Global representation across 7 regions

Region



Base: All respondents=3887

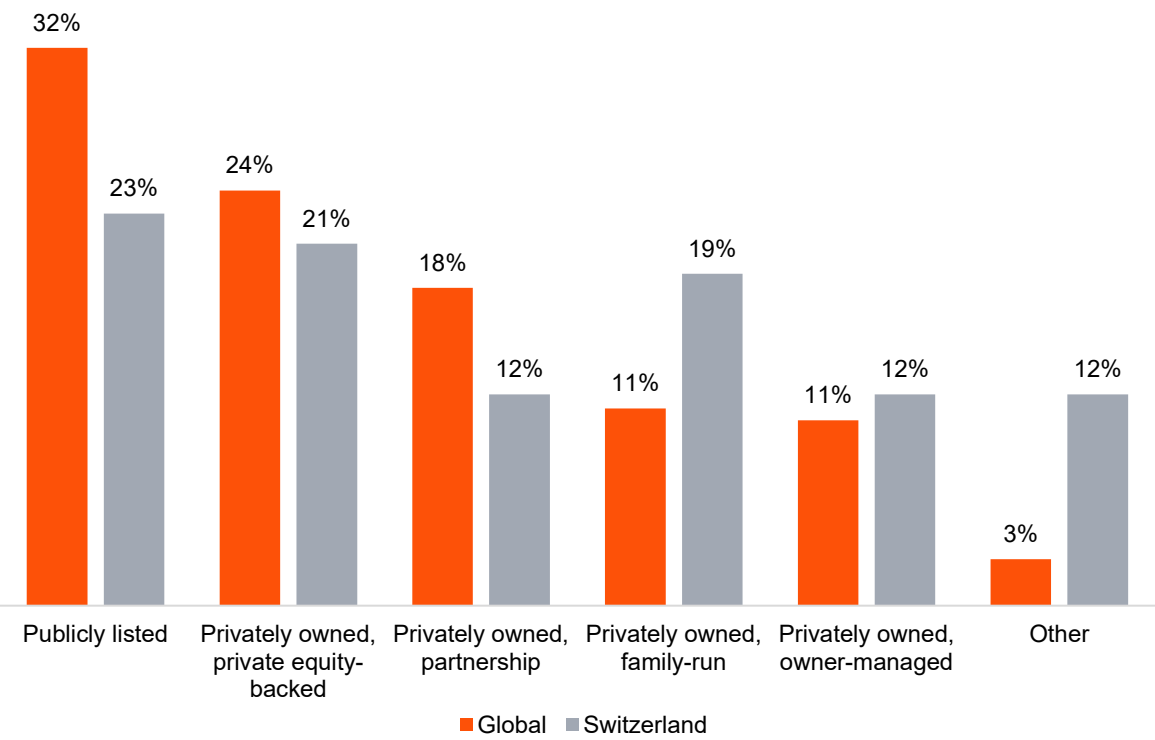
A spread of survey responses across sectors



S4. Which of the following best describes your organisation's industry? Base: All respondents=3887

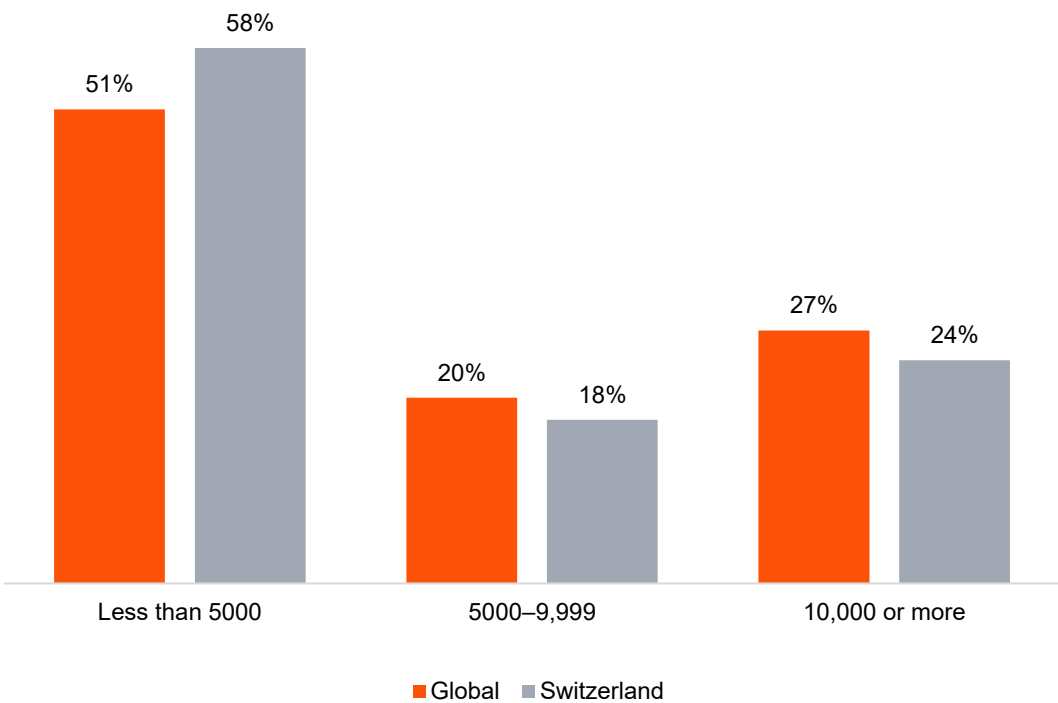
Profile of survey participants

Company ownership



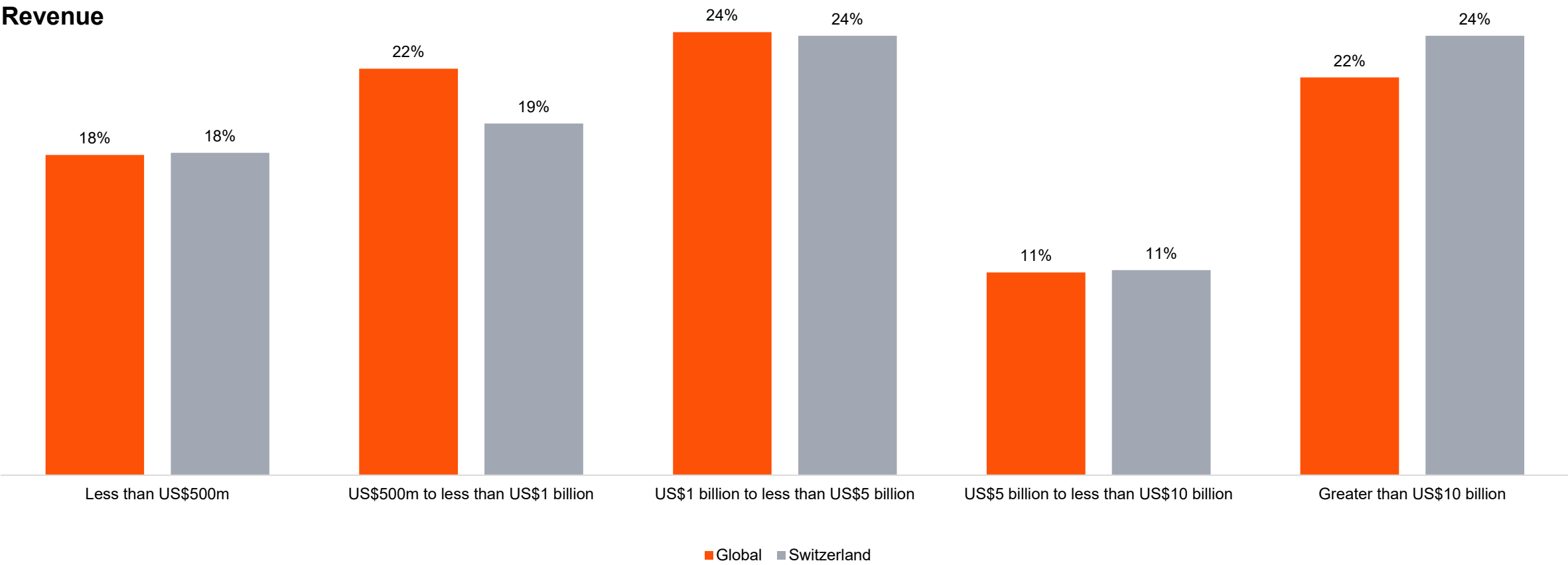
S8. Which of the following best describes the ownership status of your company? Base: All respondents excluding G&PS=3740, Switzerland respondents excluding G&PS=57

Employee headcount



S7. Please confirm your organisation’s global employee headcount. Base: All respondents=3887, Switzerland respondents=62

Profile of survey participants



S5. Please confirm your organisation’s global revenue in the last fiscal year (in US dollars). Base: All respondents=3887, Switzerland respondents=62

Key findings for Switzerland

New world, new rules: Cybersecurity in an era of uncertainty

52% of Swiss firms are increasing cyber risk investments in response to geopolitical volatility.

Just **33%** of Swiss firms have implemented data controls across the entire data lifecycle.

Only **11%** of Swiss firms have implemented quantum readiness measures.

56% of Swiss organisations say technology modernisation is the top driver of cyber spend.

The **top 3** hurdles to implementing AI in cyber defence are unclear risk appetite, skills shortages, and knowledge gaps.

50% of Swiss executives engage with their CISO monthly, but only one in four involve them strongly in transformation initiatives.

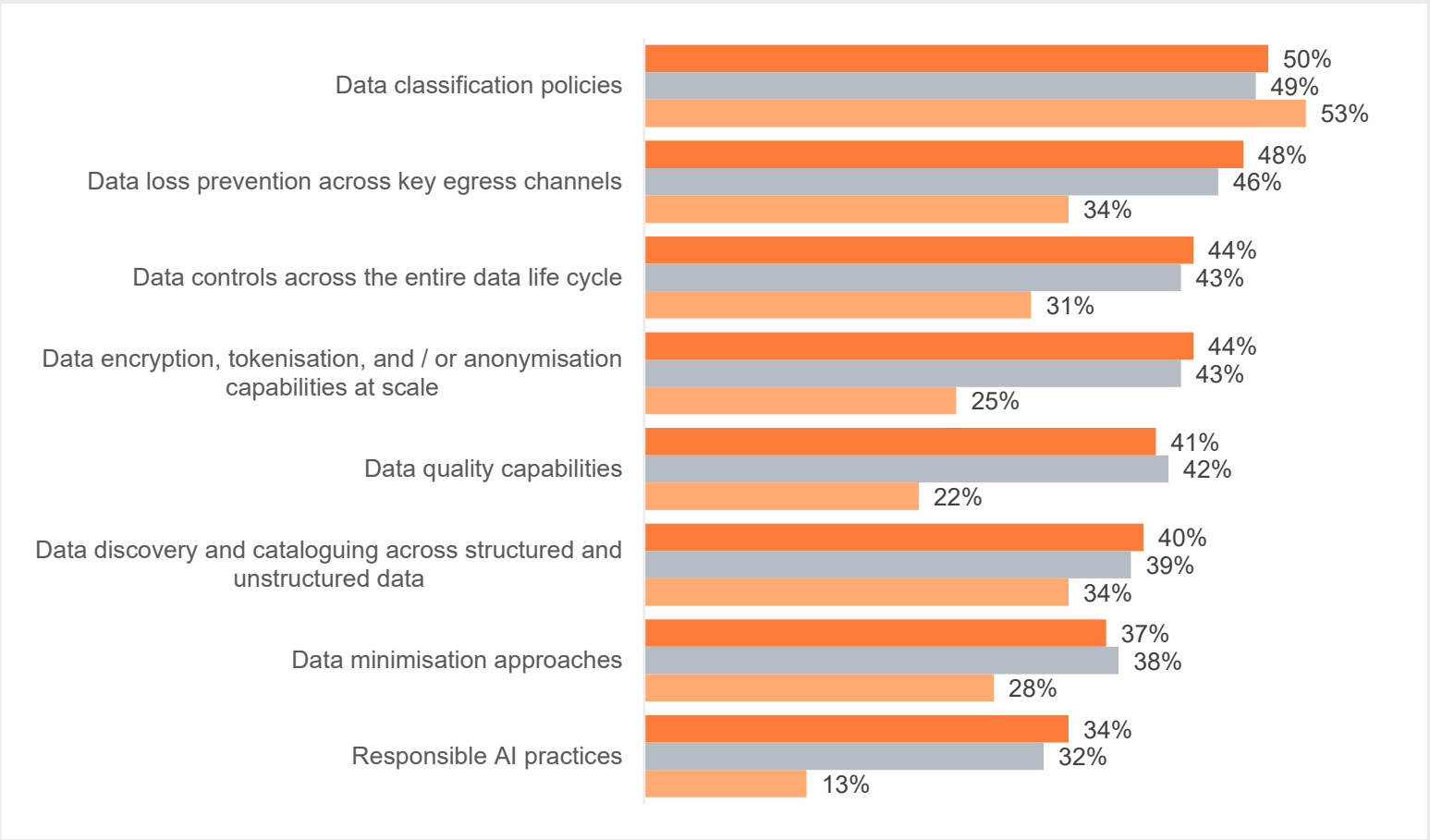
Risk and threat landscape

Global tensions drive new focus on cyber risk



Data risk mitigation in Swiss organisations

Swiss organisations lead the world with data classification, but are far behind global peers in implementing data protection controls



53%

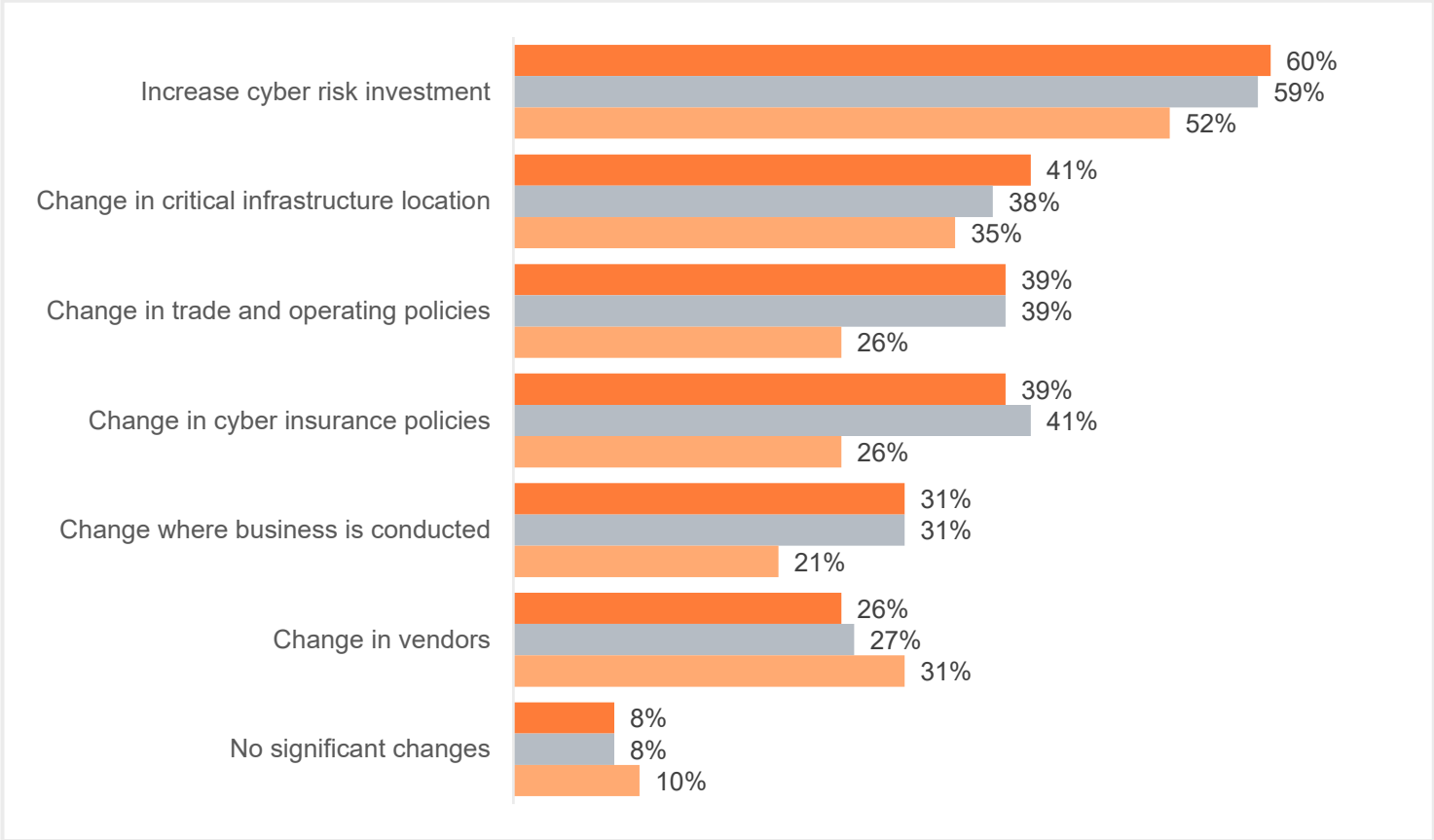
of the Swiss respondents, have implemented data classification policies across their organisations.

- Global
- Western Europe
- Switzerland

Q5. To what extent has your organisation implemented or is planning to implement any of the following measures to address data risk across the enterprise?
Showing % who selected 'implemented across the organisation'

Swiss organisations are adapting their cyber strategies to rising geopolitical uncertainty

Fewer Swiss organisations are increasing cyber investment than global ones, but markedly more are changing vendors in response to geopolitics



52%

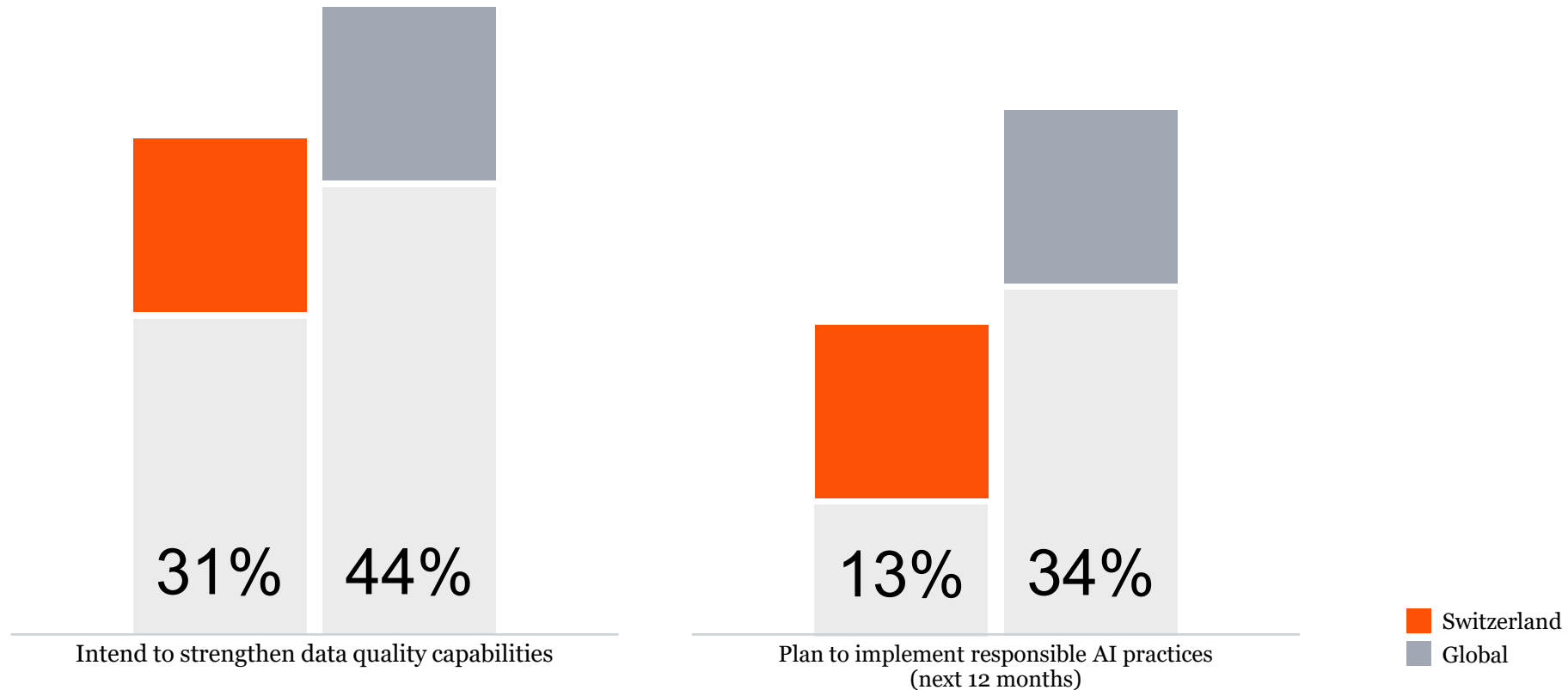
of Swiss firms are increasing cyber risk investments in response to geopolitical volatility.

- Global
- Western Europe
- Switzerland

Q2. Over the next 12 months, which of the following areas of your organisation’s cyber strategy is changing in response to the current geopolitical landscape?

Switzerland's drive to strengthen data risk management and AI practices

Swiss organisations, long lagging global peers on data risk management, plan substantial investment in the coming months as a necessity for investment in responsible AI



Switzerland's Drive to Strengthen Data Risk Management and AI Practices

Switzerland currently trails in data risk management
but demonstrates strong ambition to close the gap in the coming year.



38% plan to implement responsible AI practices in the next 12 months



31% intend to strengthen data quality capabilities



Only half of Swiss firms are stepping up cyber spend – far too few, given that criminals never stop investing. The low figure is partly due to advanced financial services investing more slowly, but it leaves vulnerable sectors such as healthcare, critical infrastructure and small(er) businesses even further behind.



Urs Küderli, Partner and Leader
Cybersecurity and Privacy, PwC Switzerland



Building trust in a world of uncertainty

**Don't wait for threats to decide for you –
invest in data and AI resilience now to secure
tomorrow's competitiveness.**

Cyber investment is no place for hesitation. Swiss organisations need enterprise-wide action on data protection, encryption, and responsible AI. Only by closing the gap with global peers can they safeguard trust, protect critical infrastructure, and remain competitive in the future.



Cyber strategy and operations

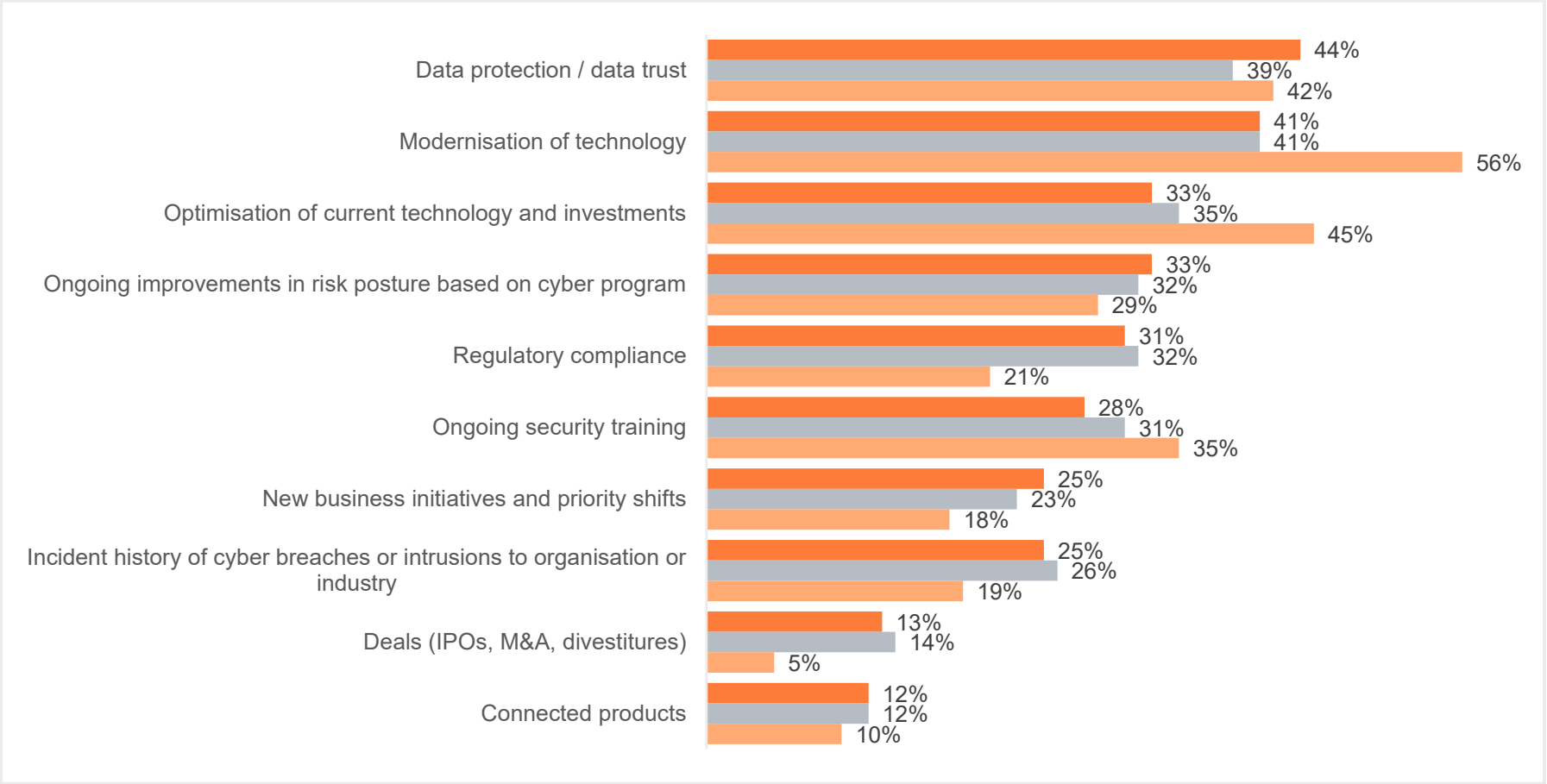
**Modernisation fuels cyber investment,
but resilience gaps remain**

Technology modernisation leads cybersecurity spending in Switzerland

56%

of Swiss organisations say technology modernisation is the top driver of cyber spend – ahead of regulatory compliance and above the global average.

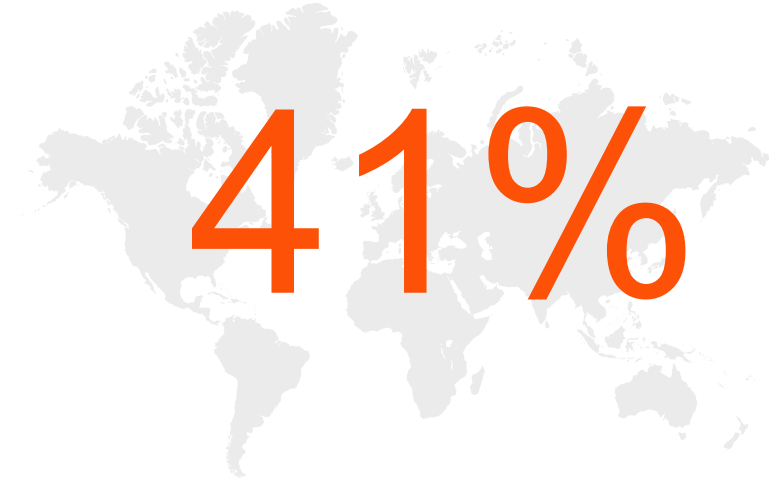
Global
Western Europe
Switzerland



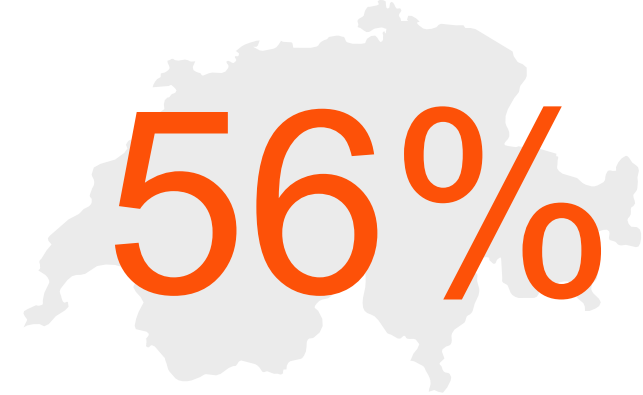
Question: Which of the following factors are influencing your cyber spend priorities over the next 12 months?

Swiss organisations prioritise technology modernisation and investment optimisation in cyber strategies

Global



Switzerland



Swiss organisations are putting technology modernisation and optimisation of existing investments at the centre of their cyber strategies. Over half cite modernisation as their main driver of cyber spending, well above the global average of 41%. Optimisation of current investments is also more important in Switzerland (45% vs. 33% globally).

Question: Which of the following factors are influencing your cyber spend priorities over the next 12 months?

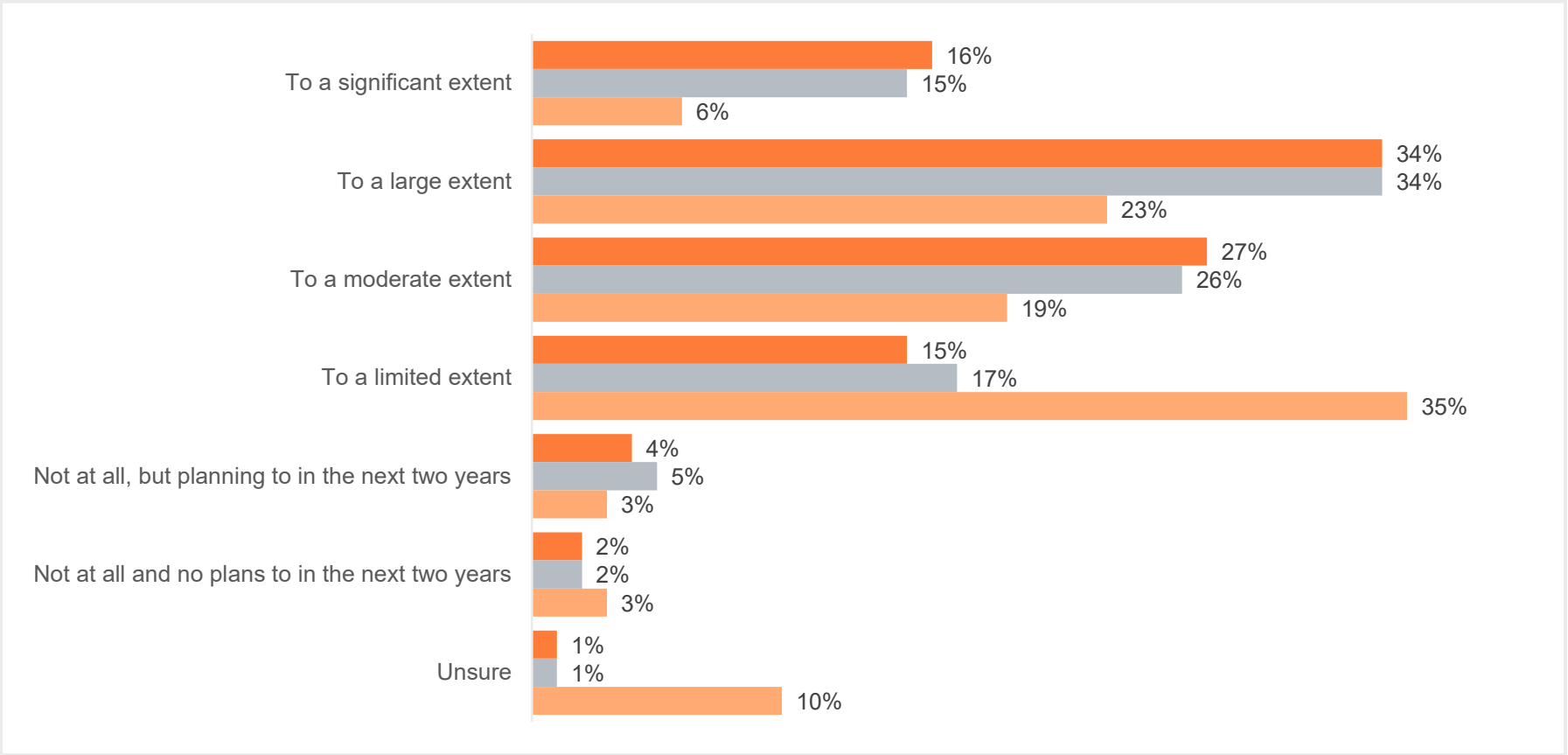
Cyber risk quantification practices in Switzerland

Swiss organisations are notably farther behind Western peers in understanding and modelling the financial impact of cyber risks.

35%

of Swiss organisations only measure the financial impact of cyber risks to a limited extent

Global
Western Europe
Switzerland



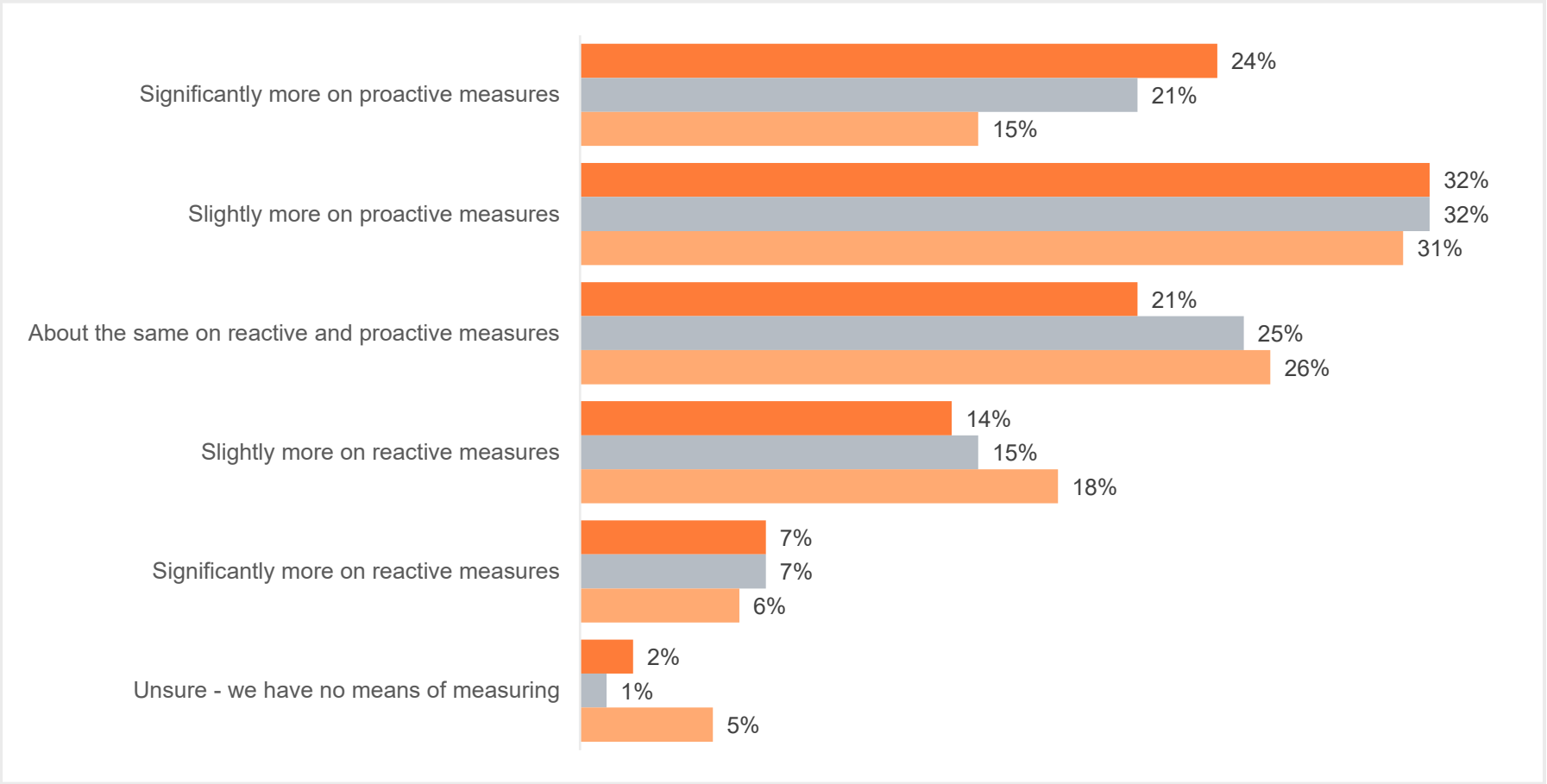
Question: To what extent is your organisation currently measuring the potential financial impact of cyber risks (i.e., risk quantification)?

Switzerland's balance in cybersecurity resource allocation

26%

of Swiss organisations allocate resources equally to both reactive and proactive cybersecurity measures.

Global
Western Europe
Switzerland



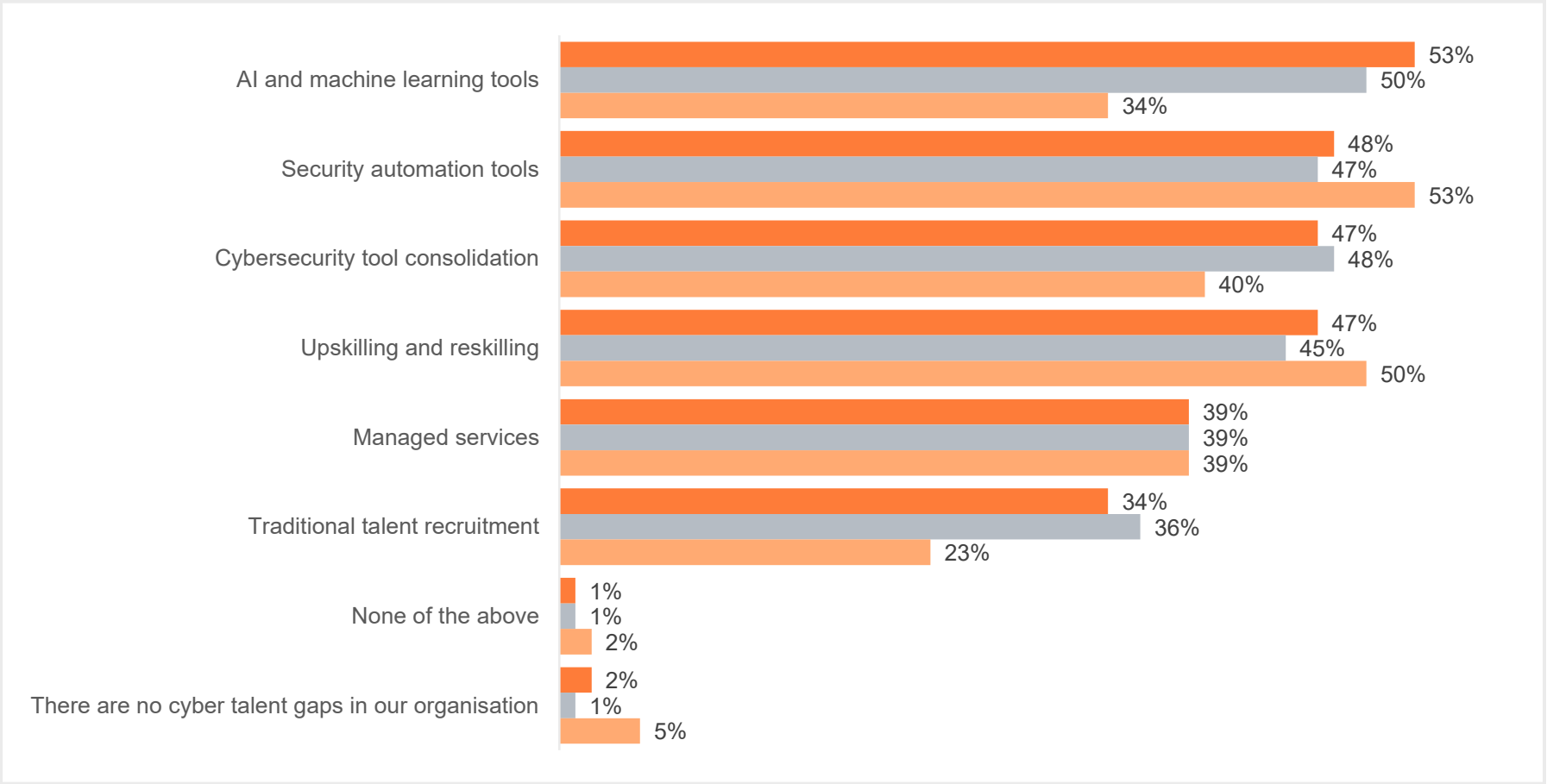
Question: Is your organisation spending more resources on reactive or proactive cybersecurity measures?

Addressing cyber talent gaps in Switzerland

53%

of Swiss organisations prioritise security automation tools to address cyber talent gaps over the next 12 months.

Global
Western Europe
Switzerland



Question: Which of the following is your organisation prioritising to address cyber talent gaps over the next 12 months?



Swiss firms are clearly investing in modernisation, but the challenge is ensuring that spend translates into measurable resilience. Technology alone won't solve the problem; it takes a well trained and governed organisation, hardened fundamentals, rehearsed playbooks, and the ability to respond and recover at speed.



Johannes Dohren, Partner and Head of Cyber Resilience and Defence, PwC Switzerland



Building trust in a world of uncertainty

Don't just spend on cyber target investments to reduce the most risk, and build a foundation for secure AI.

Swiss firms are showing strategic maturity by building security into their modernisation initiatives — a clear sign of security by design. The next step is building on this strategy by strengthening capabilities through automation and AI-driven learning, and improving the quantification of cyber risk to ensure the most valuable security investments are chosen. By investing time to model and understand their exposure accurately, leaders can make more informed decisions and turn resilience into a source of trust and competitiveness.

Artificial intelligence

**Governance, not skills,
is the main barrier**

4

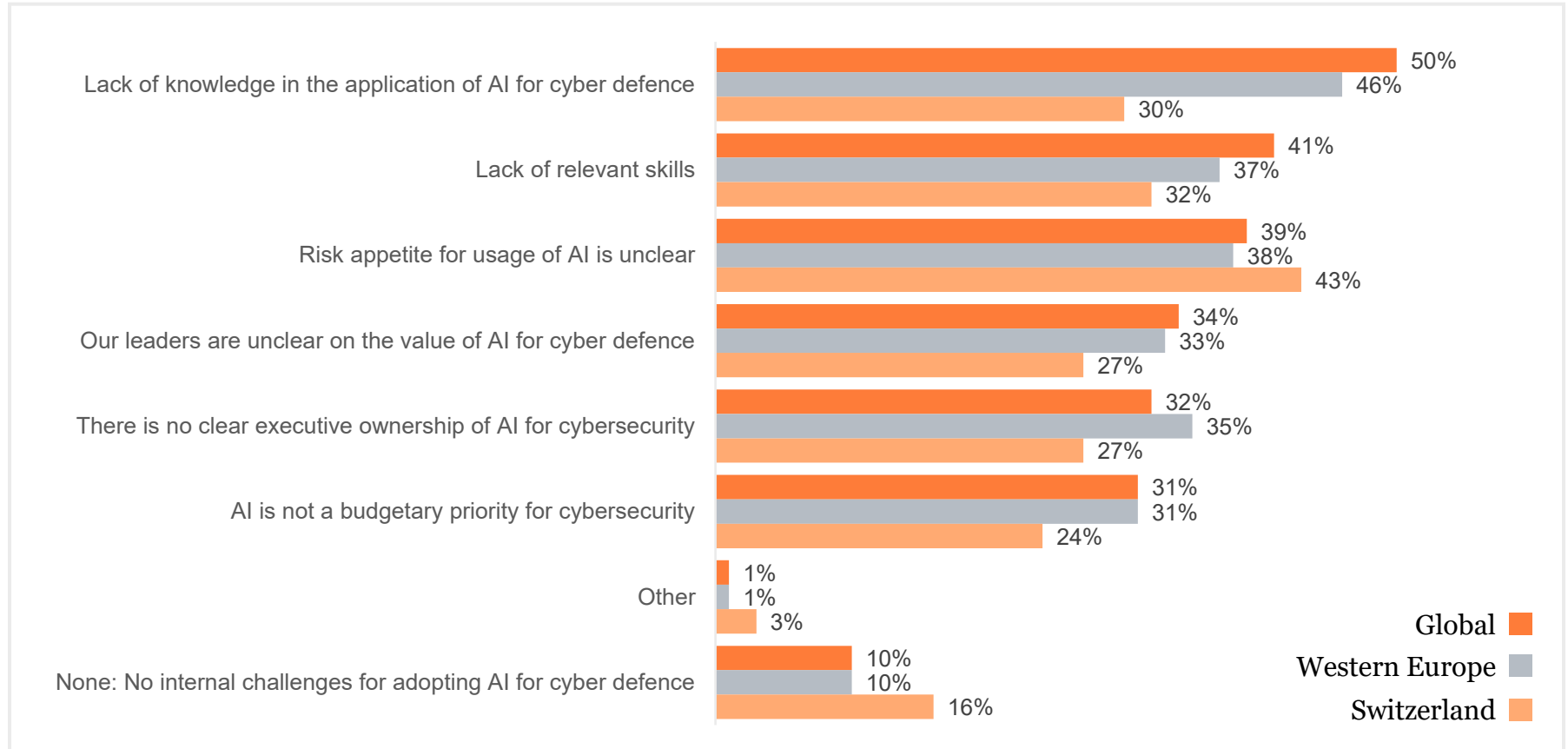
The top three hurdles to implementing AI in cyber defence are unclear risk appetite, skills shortages, and knowledge gaps.

40%

of organisations focus on cloud security, data protection, and cyber defence operations – reflecting a strong push to reinforce the core pillars of resilience.

43%

of the swiss respondent thinks that the main barrier to using AI in cyber defence is not a lack of expertise, but uncertainty over governance. An unclear risk appetite tops the list of challenges.



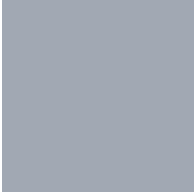
Question: What have been your organisation's biggest internal challenges to implementing AI for cyber defence over the last 12 months?

AI implementation challenges in cyber defence in Switzerland



13%

plan to implement responsible AI practices in the next 12 months



16%

of Swiss firms using AI for cyber defence report no internal implementation challenges – more than the global average of 10%.

At the global level, organisations are most concerned about AI-powered malware, supply chain attacks, and deepfake-enabled social engineering. To counter these risks, they prioritise AI threat hunting, vulnerability scanning and assessments, and identity and access management. When it comes to using agentic AI, around 40% of organisations focus on cloud security, data protection, and cyber defence operations – reflecting a strong push to reinforce the core pillars of resilience.

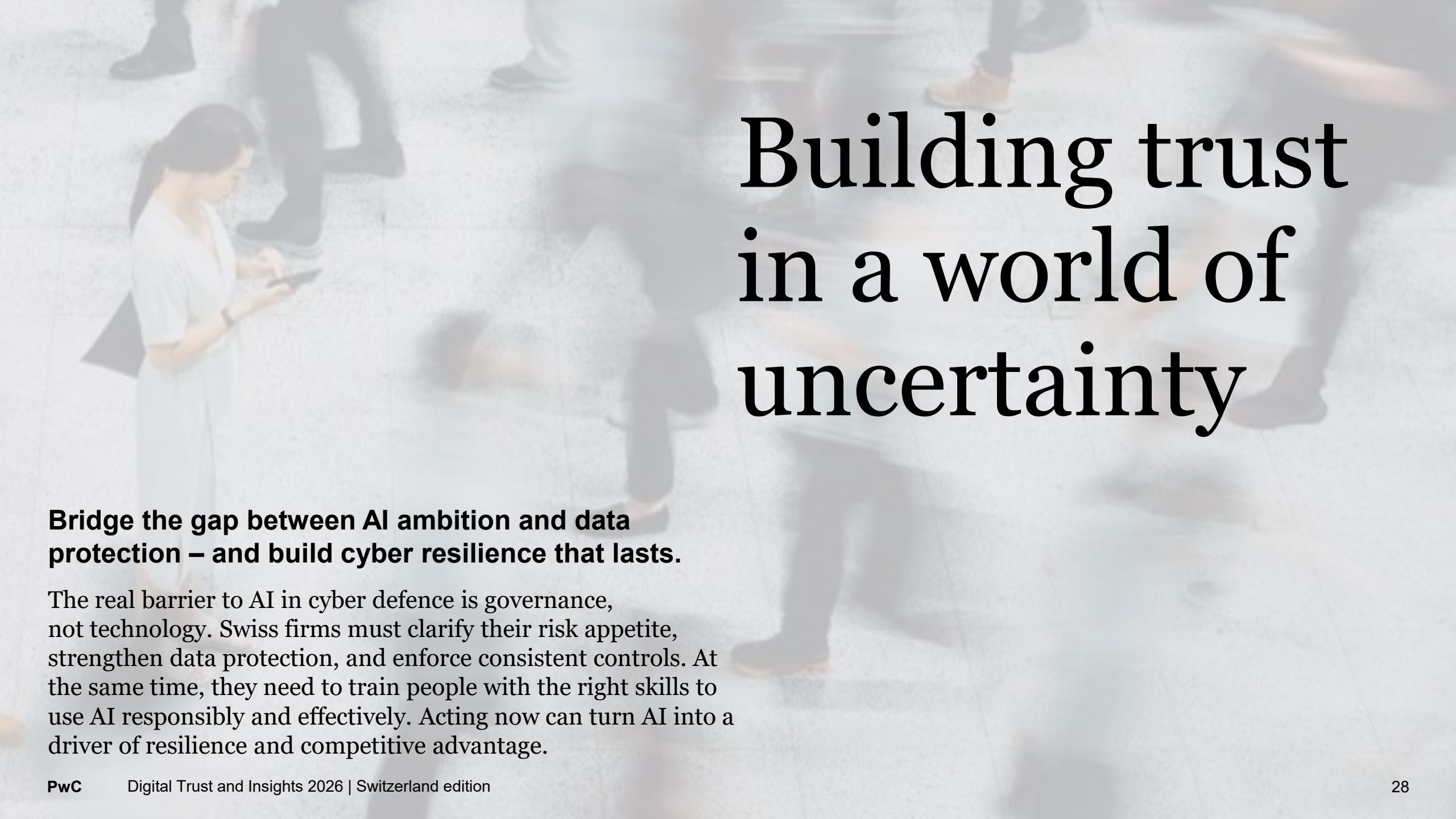
Together, these findings suggest that Swiss organisations experimenting with AI in cyber defence often have strong technical expertise and face fewer skills or knowledge gaps than peers. But adoption remains selective, with governance and risk appetite the main sticking points. Globally, by contrast, the emphasis is shifting towards tackling AI-driven threats and embedding agentic AI into critical security functions.

“

Swiss companies face a mismatch between their ambitions to use AI and the maturity of their data protection. Without a clear appetite to apply AI, robust controls, and the right skills, many are not yet prepared to manage data securely in an AI-driven world.



Yan Borboën, Partner and Leader, Digital Assurance & Trust, PwC Switzerland



Building trust in a world of uncertainty

Bridge the gap between AI ambition and data protection – and build cyber resilience that lasts.

The real barrier to AI in cyber defence is governance, not technology. Swiss firms must clarify their risk appetite, strengthen data protection, and enforce consistent controls. At the same time, they need to train people with the right skills to use AI responsibly and effectively. Acting now can turn AI into a driver of resilience and competitive advantage.

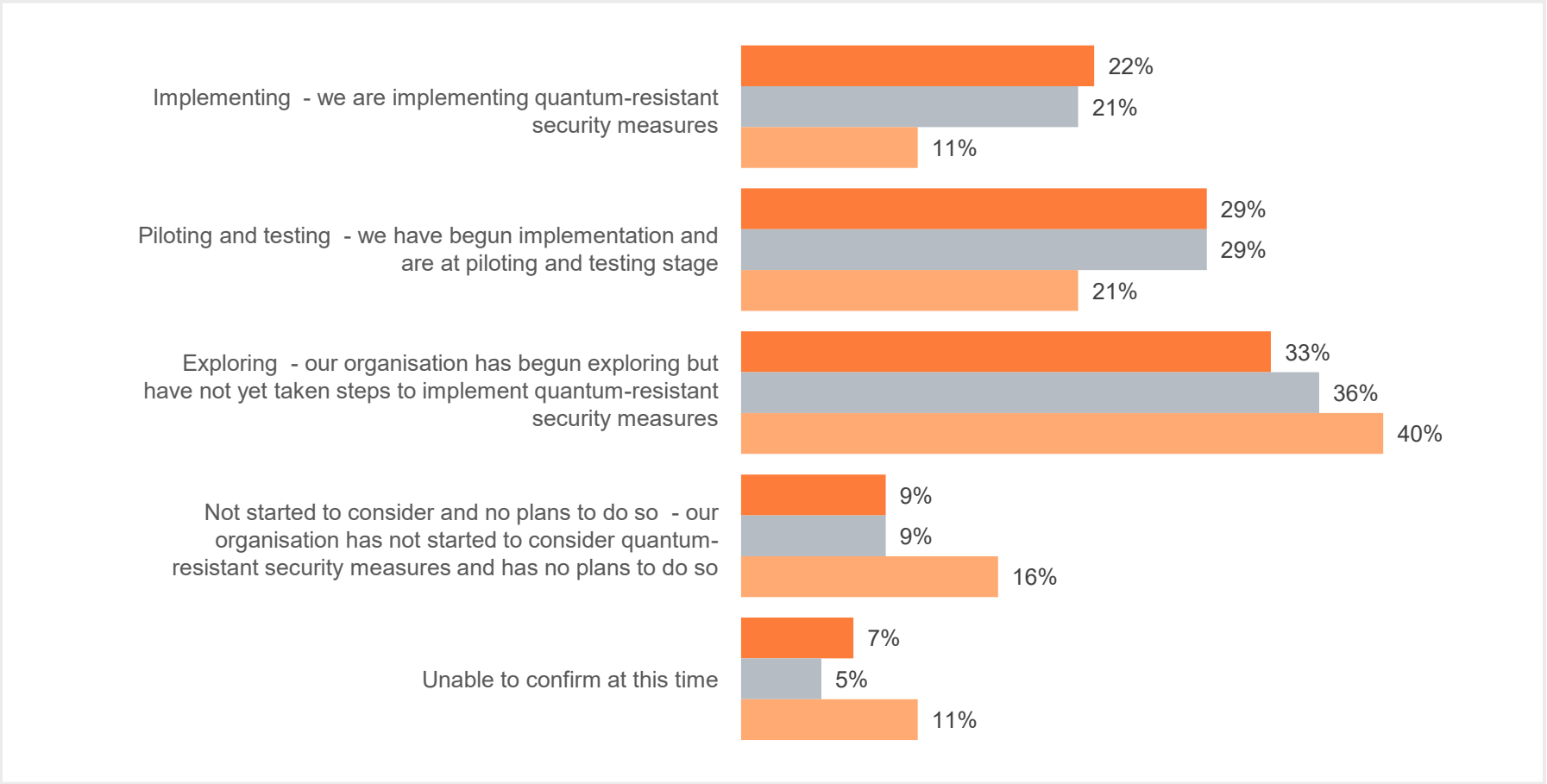
Quantum computing readiness

Exploration dominates while global peers advance

Swiss organisations lag in quantum-resistant security adoption

Only 11%
of Swiss firms have implemented quantum readiness measures, while 40% are still in the exploring phase – leaving them well behind global and European peers.

Global
Western Europe
Switzerland



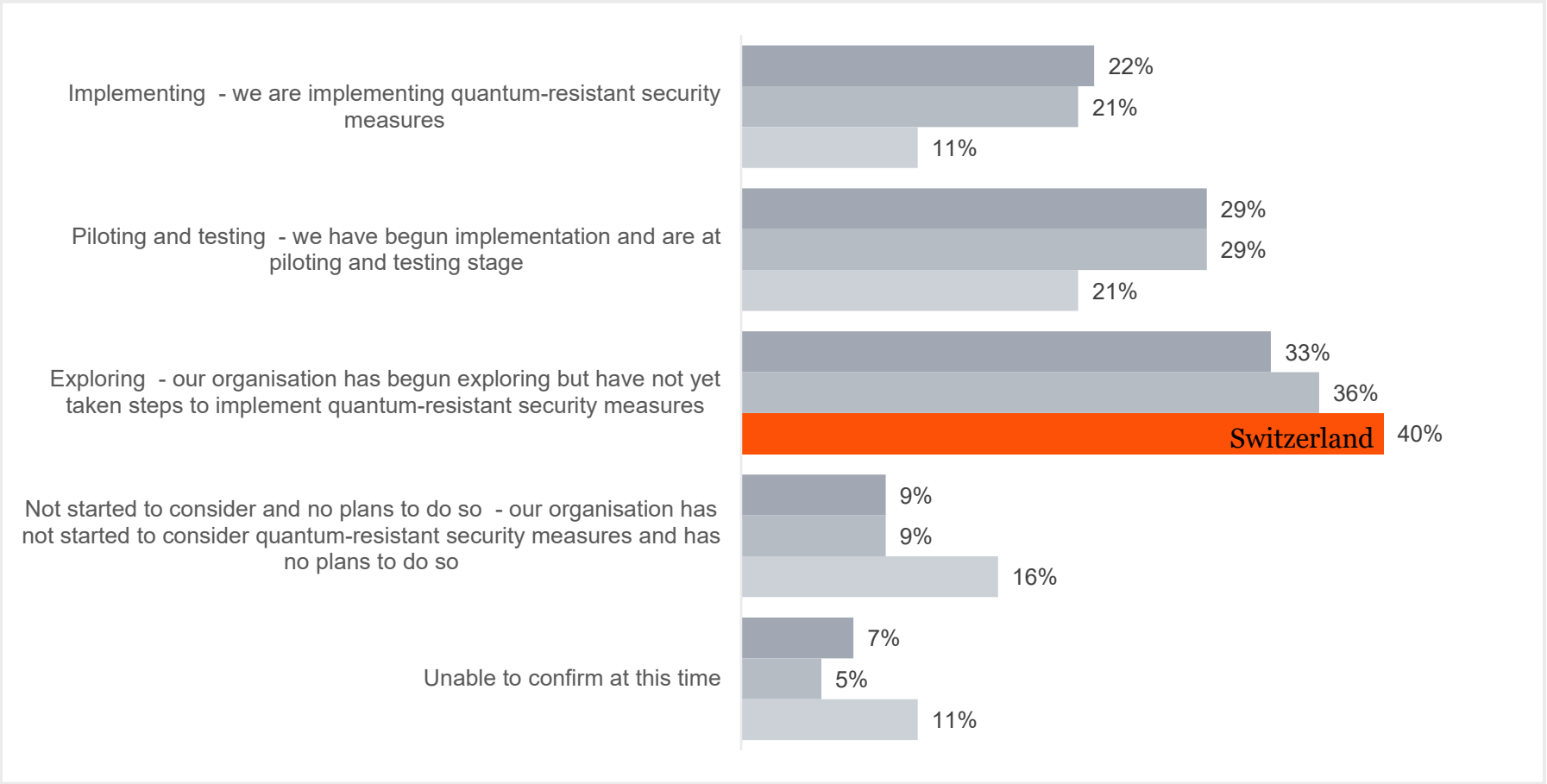
Question: How far along is your organisation when it comes to quantum-resistant security measures?

Progress in Quantum-Resistant Security Measures

40%

of Swiss organizations are currently exploring quantum-resistant security measures, compared to 33% globally.

Global
Western Europe
Switzerland



Question: How far along is your organisation when it comes to quantum-resistant security measures?



Quantum may still seem like a future issue, but preparation must start now. The steps organisations take today – building awareness, assessing exposure, and planning mitigation – will determine how resilient they are tomorrow.



Chris Girling, Partner Cybersecurity and Privacy, PwC Switzerland



Building trust in a world of uncertainty

Quantum readiness starts now – protect today's data against tomorrow's risks.

Quantum readiness needs to move from exploration to execution. It should be treated as part of the wider digital and cyber strategy: strengthening data protection today while laying the foundations for quantum-safe security tomorrow. Acting early allows organisations to shape standards, lifecycle mitigations into the organisation, and secure an edge in a rapidly changing risk landscape.



Cyber leadership

CISO access is high, but influence low

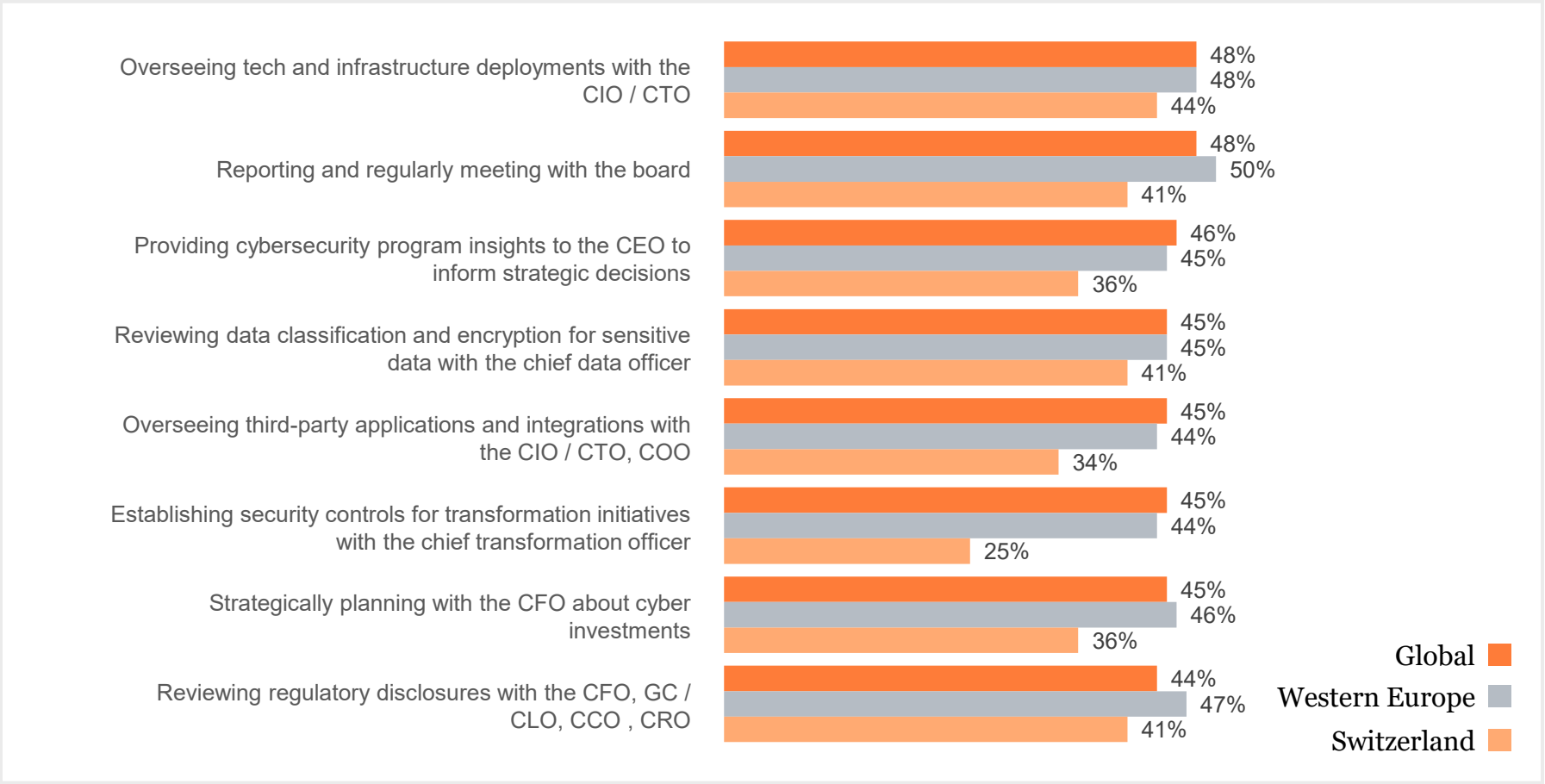
Swiss CISO engagement: Navigating strategic collaboration with C-suite

Only 25%

of Swiss organisations' CISOs are involved in establishing security controls for transformation initiatives with the chief transformation officer, highlighting an area for increased strategic collaboration.

36%

of Swiss organisations' CISOs are engaged in strategic planning with the CFO about cyber investments, suggesting room for growth in financial alignment within cybersecurity strategies.

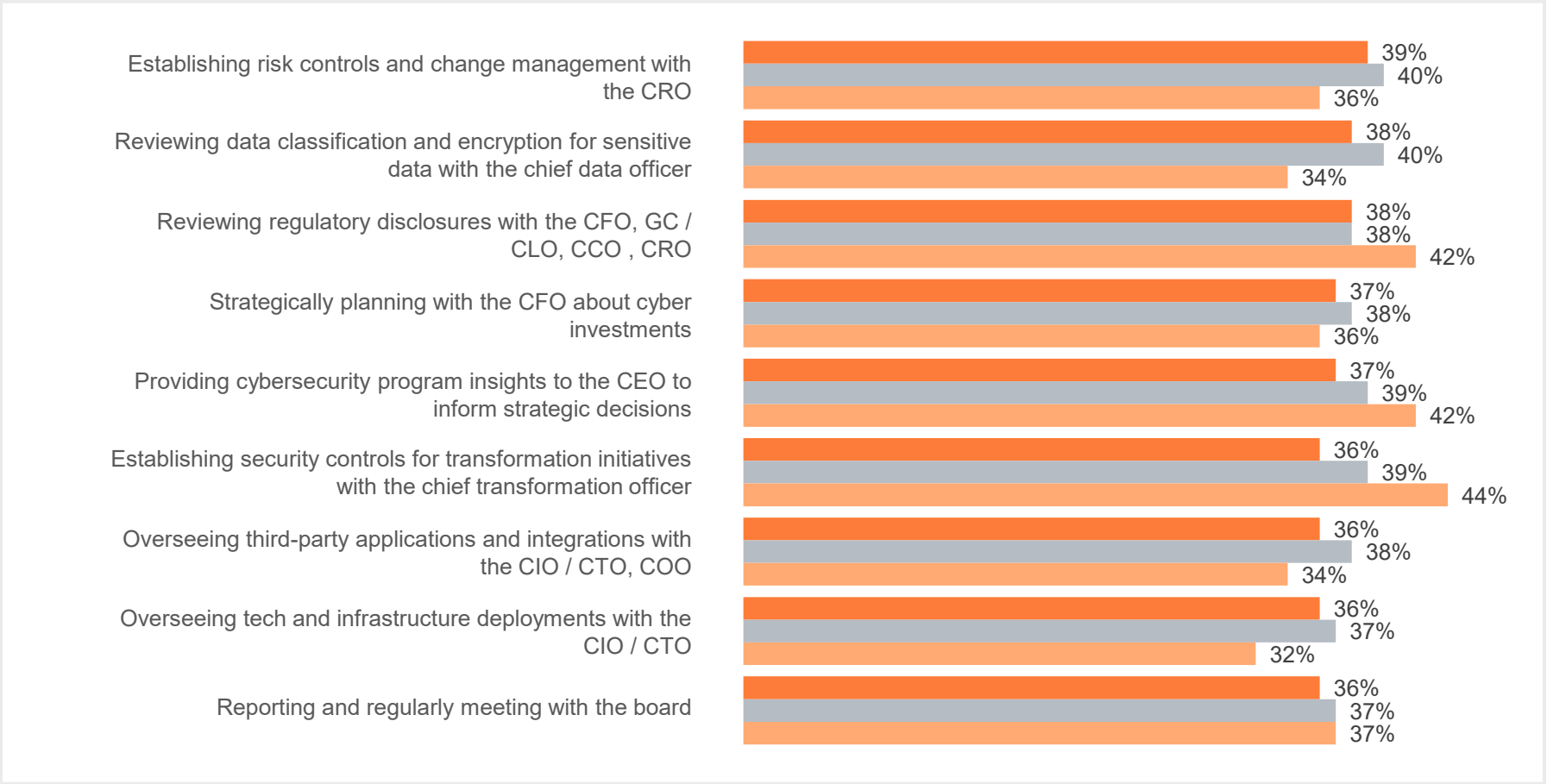
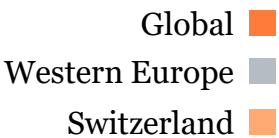


Question: To what extent does your CISO work with the C-suite in the following areas?

Moderate contributions: Swiss CISO's role in C-suite regulatory compliance efforts

42%

of Swiss organisations' CISOs are moderately involved in reviewing regulatory disclosures with the C-suite, compared to 38% globally and in Western Europe, indicating a stronger focus on compliance in Switzerland



Question: To what extent does your CISO work with the C-suite in the following areas?



Swiss CISOs may have recurring access to the C-suite, but they are engaged to a lesser degree in business transformation. While regular meetings tick the box, their influence on change and value creation remains below international peers – a missed opportunity to shape resilience and growth across the business value chain.



Ashish Gupta, Partner Cybersecurity and Privacy, PwC Switzerland



Building trust in a world of uncertainty

Elevate your CISO from advisor to partner – and turn cybersecurity into a driver of resilience and growth.

For Swiss leaders, the message is clear: regular meetings with the CISO are not enough. True resilience requires bringing CISOs into transformation, investment, and board-level decisions. Elevating them as strategic partners turns cybersecurity into a driver of trust, resilience, and growth.

A man and a woman, both wearing light blue shirts, are standing in a factory or industrial setting. The man is holding a tablet and pointing at it, while the woman looks on. In the background, there is a yellow robotic arm and other industrial equipment. The title 'About the survey' is overlaid on the right side of the image in a large, black, serif font.

About the survey

The 2026 Digital Trust Insights Survey reflects the views of business and tech leaders around the world on the challenges and opportunities to improve and transform cybersecurity in their organisation in the next 12 months – covering topics including risk and threat landscape, cyber strategy, artificial intelligence, quantum computing and cyber leadership.

3,887 survey responses were achieved from **business and tech leaders** across **72 territories**.

Survey responses are from a **range of industry sectors and organisation sizes**, with over half from \$1billion+ organisations. Survey responses were obtained between 7 May and 15 July 2025.

Contact us



**Urs
Küderli**

Partner
Leader Cybersecurity
and Privacy,
PwC Switzerland

urs.kuederli@pwc.ch



**Johannes
Dohren**

Partner
Head of Cyber Resilience
and Defence,
PwC Switzerland

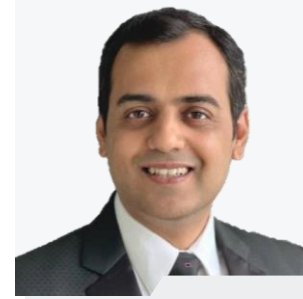
johannes.dohren@pwc.ch



**Chris
Girling**

Partner
Cybersecurity and
Privacy,
PwC Switzerland

chris.girling@pwc.ch



**Ashish
Gupta**

Partner
Cybersecurity and
Privacy,
PwC Switzerland

ashish.kv.gupta@pwc.ch



**Yan
Borboën**

Partner
Leader, Digital
Assurance & Trust,
PwC Switzerland

yan.borboen@pwc.ch

Thank you

A woman with dark hair tied back, wearing a white lab coat over a striped shirt, is looking down at a tablet computer. She is in a modern office or laboratory setting with blurred background lights and equipment.

<https://www.pwc.ch/en/insights/cybersecurity/global-digital-trust-2026.html>

pwc.ch

© 2025 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.