In collaboration with Accenture

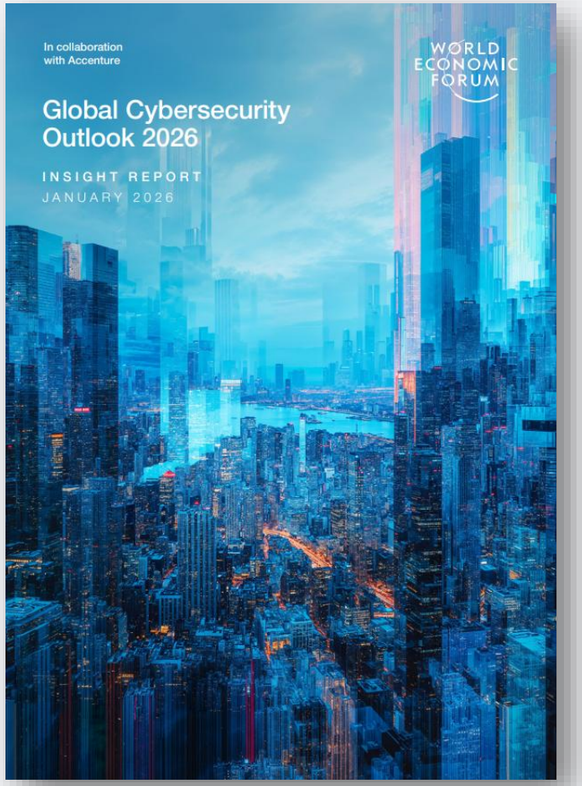
WORLD ECONOMIC FORUM

Global Cybersecurity Outlook 2026

INSIGHT REPORT JANUARY 2026

Global Cybersecurity Outlook 2026

INSIGHT REPORT JANUARY 2026



The World Economic Forum's *Global Cybersecurity Outlook 2026*, written in collaboration with Accenture, examines the cybersecurity trends that will affect economies and societies in the year to come.

The report explores how accelerating AI adoption, geopolitical fragmentation and widening cyber inequity are reshaping the global risk landscape. As attacks grow faster, more complex and more unevenly distributed, organizations and governments face rising pressure to adapt amid persistent sovereignty challenges and widening capability gaps. Drawing on leaders' perspectives, the report provides actionable insights to inform strategy, investment and policy.

Table of Content

The 5-Year Evolution of Global Cyber Risk

The 5-Year Evolution of Global Cyber Risk (2022–2026)

WORLD ECONOMIC FORUM

2022

2022: The Connectivity Crisis

- **Focus:** Adaptation to rapid, pandemic-driven digitalization.
- **Key Challenge:** Widening capability gaps leaving smaller nations and institutions vulnerable.

2023

2023: The Geopolitical Pivot

- **Focus:** Cybersecurity becomes inseparable from global politics.
- **Key Challenge:** Escalating instability and complex supply chain interdependencies.

2024

2024: The Great Polarization

- **Focus:** Growth of the cyber economy vs. human inequity.
- **Key Challenge:** Deepening "Cyber Inequity" between well-resourced leaders and those falling behind.

2025

2025: Compounding Complexity

- **Focus:** An era of extreme unpredictability.
- **Key Challenge:** The intersection of regulatory proliferation, geopolitical tension, and rapid tech adoption.

2026

2026: Systemic Fragility & Strategic Resilience

- **Focus:** Managing "Global Cascading Consequences."
- **Key Challenge:** Shifting from technical defense to aligning policy, ethics, and mandatory collaboration.

Executive Perception in Cyber landscape 2026

Executive Perception in Cyber landscape 2026

WORLD ECONOMIC FORUM

Executive Perception in Cyber landscape 2026

Threat landscape

CEOs shifted:

- They now worry more about **financial loss** and **AI threats**.

CISOs stayed firm:

- They remain focused on **ransomware** and **operational uptime**.

Which cyber risks concern you most for your organization?				
Rank	Chief executive officer (CEO)		Chief information security officer (CISO)	
	2025	**2026**	2025	**2026**
1	Ransomware attack	**Cyber-enabled fraud and phishing**	Ransomware attack	**Ransomware attack**
2	Cyber-enabled fraud and phishing	**AI vulnerabilities**	Supply chain disruption	**Supply chain disruption**
3	Supply chain disruption	**Exploitation of software vulnerabilities**	Cyber-enabled fraud and phishing	**Exploitation of software vulnerabilities**

Which cyber risks concern you most for your organization?	High resilience (rank)	Insufficient resilience (rank)
AI vulnerabilities	1	4
Cyber-enabled fraud and phishing	2	1
Supply chain disruption	3	7
Exploitation of software vulnerabilities	4	3
Ransomware attack	5	2
Insider threat	6	6
Denial-of-service attacks	7	5

CEO Risk Ranking:

- As a company gets stronger (more "resilient"), its leaders stop worrying about common scams and start focusing on **advanced threats like AI**.

Executive Perception in Cyber landscape 2026

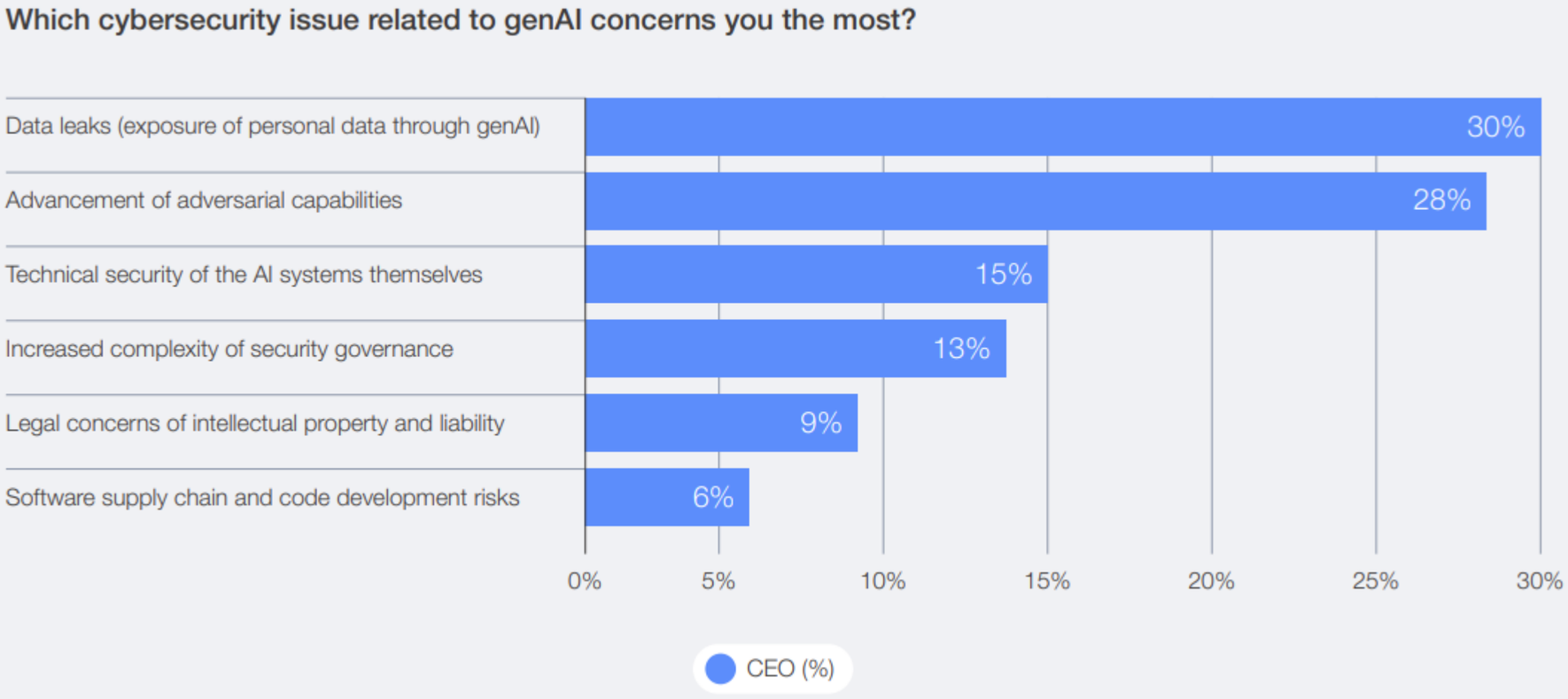
AI risks

AI Risks Focus

- For CEOs, the biggest AI fears aren't just "robots taking over"—they are specifically worried about

Data leaks

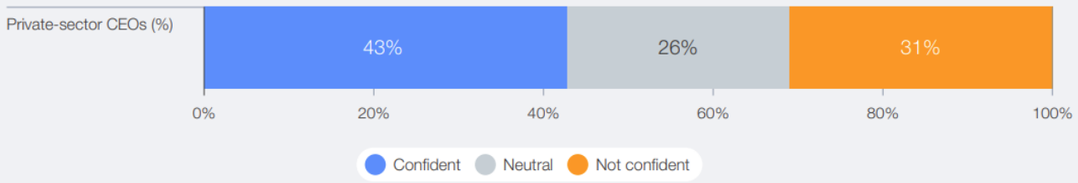
Advancement of adversarial capabilities



Executive Perception in Cyber landscape 2026

Geopolitics

How confident are you in the preparedness of the country in which you are based to respond to major cyber incidents targeting critical infrastructure?



Less than **45%** of CEOs feel confident that their country can handle a major attack on critical infrastructure.

Teamwork is Key:

- High-resilience firms are **8x more likely** to collaborate with government agencies than low-resilience ones (48% vs. 6%).

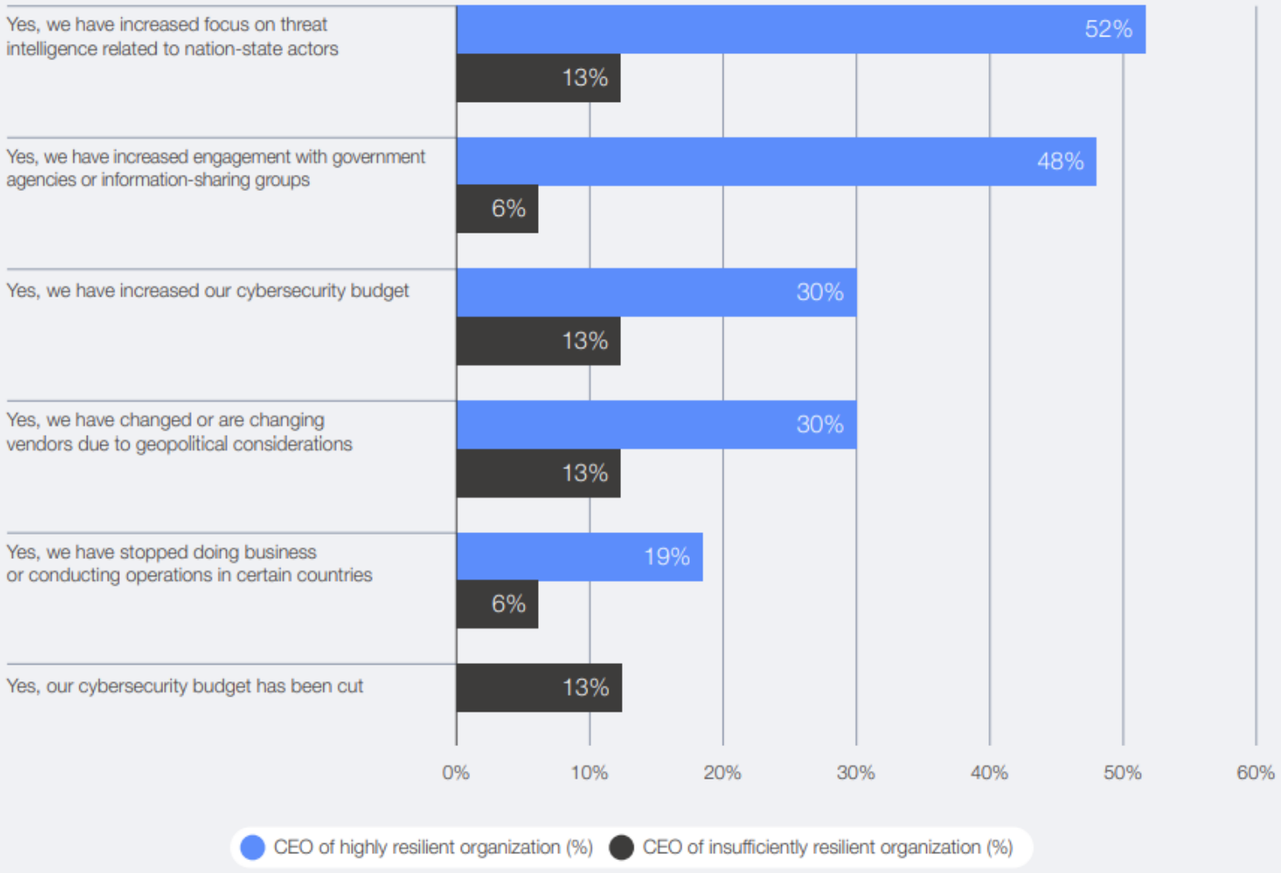
Watching Nation-States:

- 52% of top CEOs track state-sponsored threats, compared to just 13% of their less-prepared peers.

Evolving Risks:

- As companies get stronger, they move from worrying about "scams" to managing "sophisticated tech" like AI.

Has your organization's cybersecurity strategy evolved because of geopolitical volatility? (select all that apply)



Executive Perception in Cyber landscape 2026

Resilience

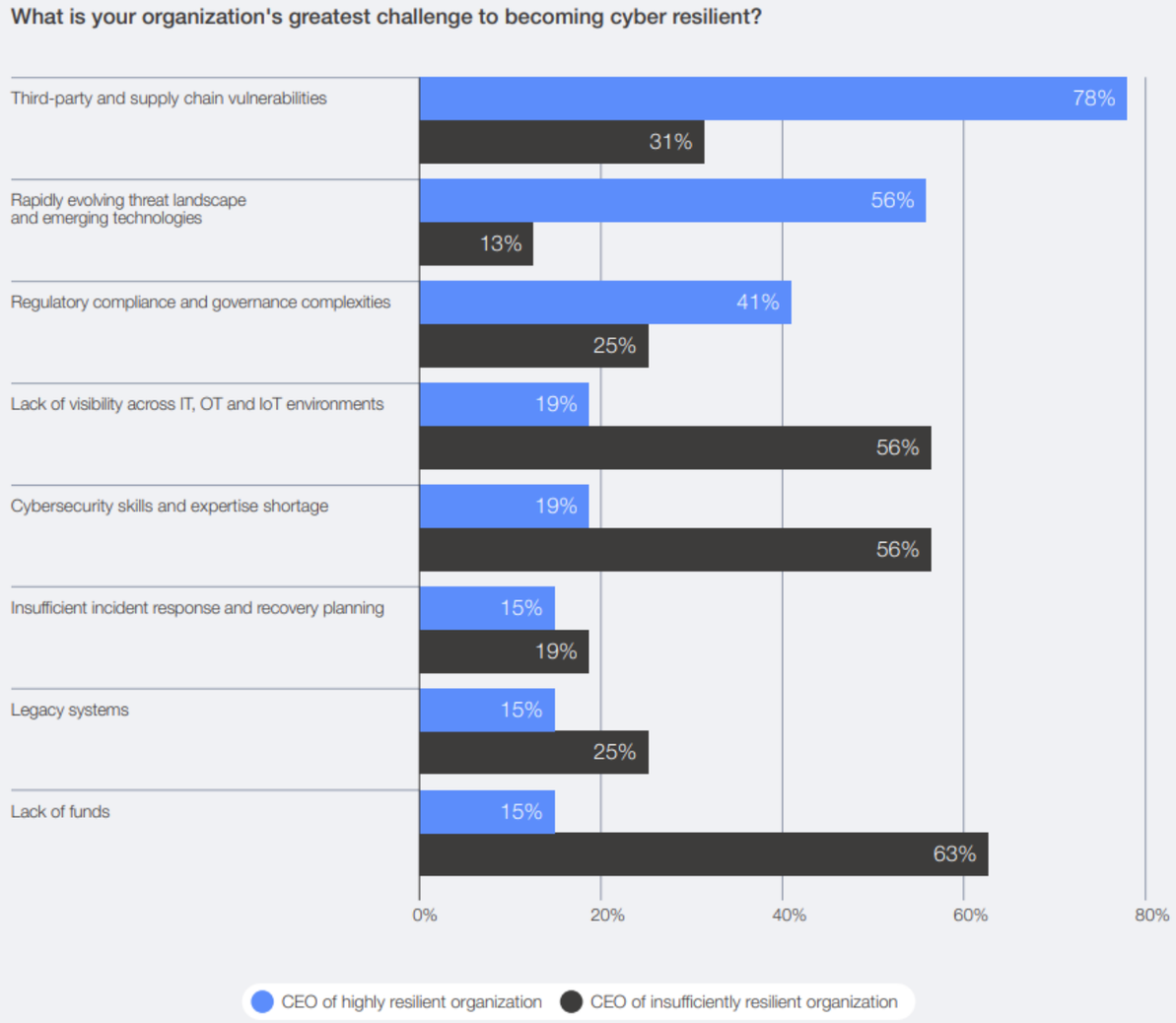
Resilience Level	Top Challenges	Key Concern
Highly Resilient	**78%** cite supply chain and third-party risks.	**The External Ecosystem:** Managing risks from partners and vendors.
Less Resilient	**63%** cite lack of funds; **56%** cite skills shortages.	**Internal Resources:** Not enough money or trained staff.

From Inside to Outside:

- As companies get stronger, they stop worrying about internal "basics" like budget and staffing and start focusing on **external dependencies**.

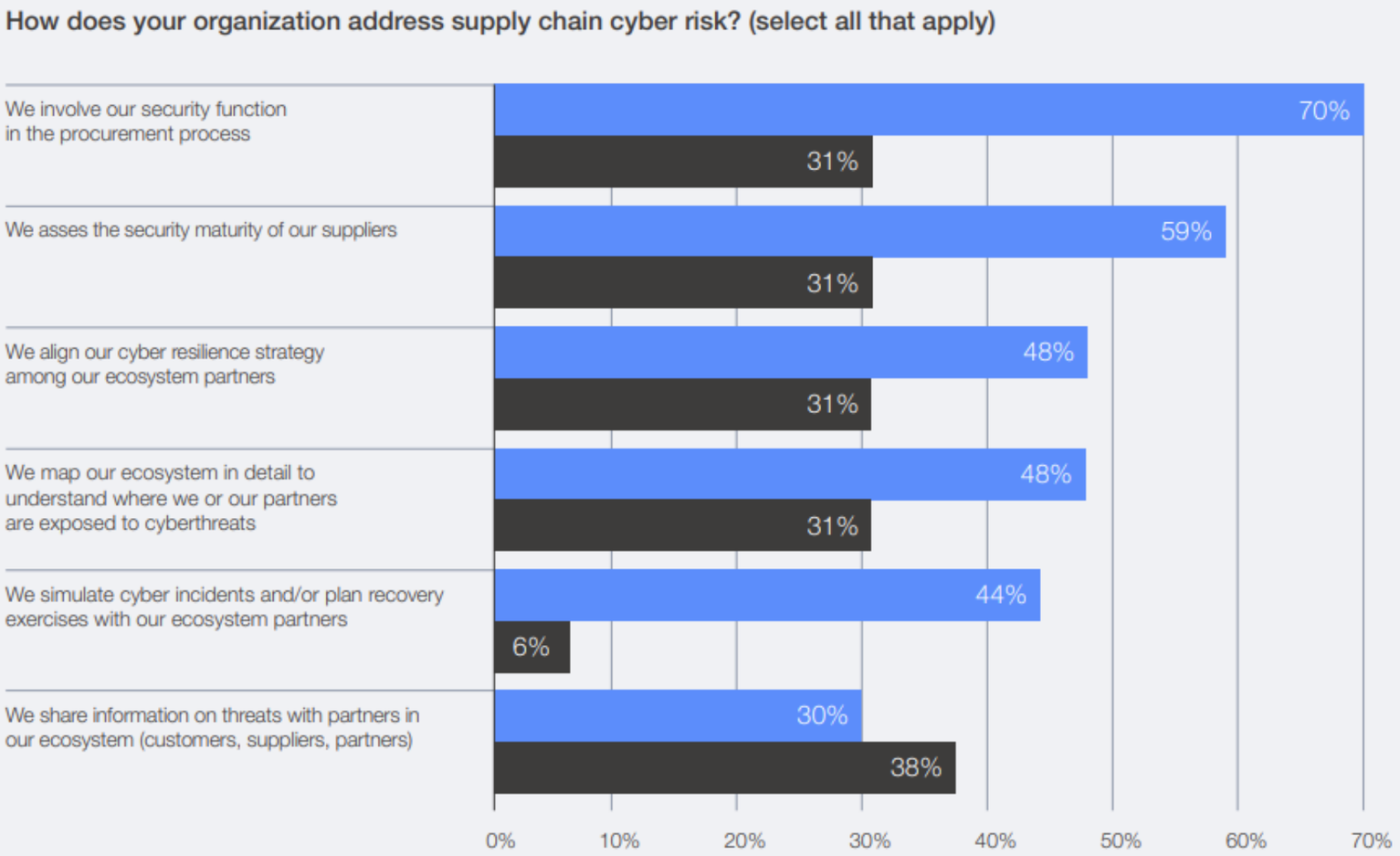
The "Network" Risk:

- For top-tier companies, the biggest threat is no longer their own team, but the **supply chain** they rely on.



Executive Perception in Cyber landscape 2026

Supply chain



Supply Chain Risk

Highly resilient companies don't just hope their partners are safe; they **look over them early** and make security a **requirement for doing business**.

- We involve our security function in the procurement process
- We assess the security maturity of our suppliers

Executive Perception in Cyber landscape 2026

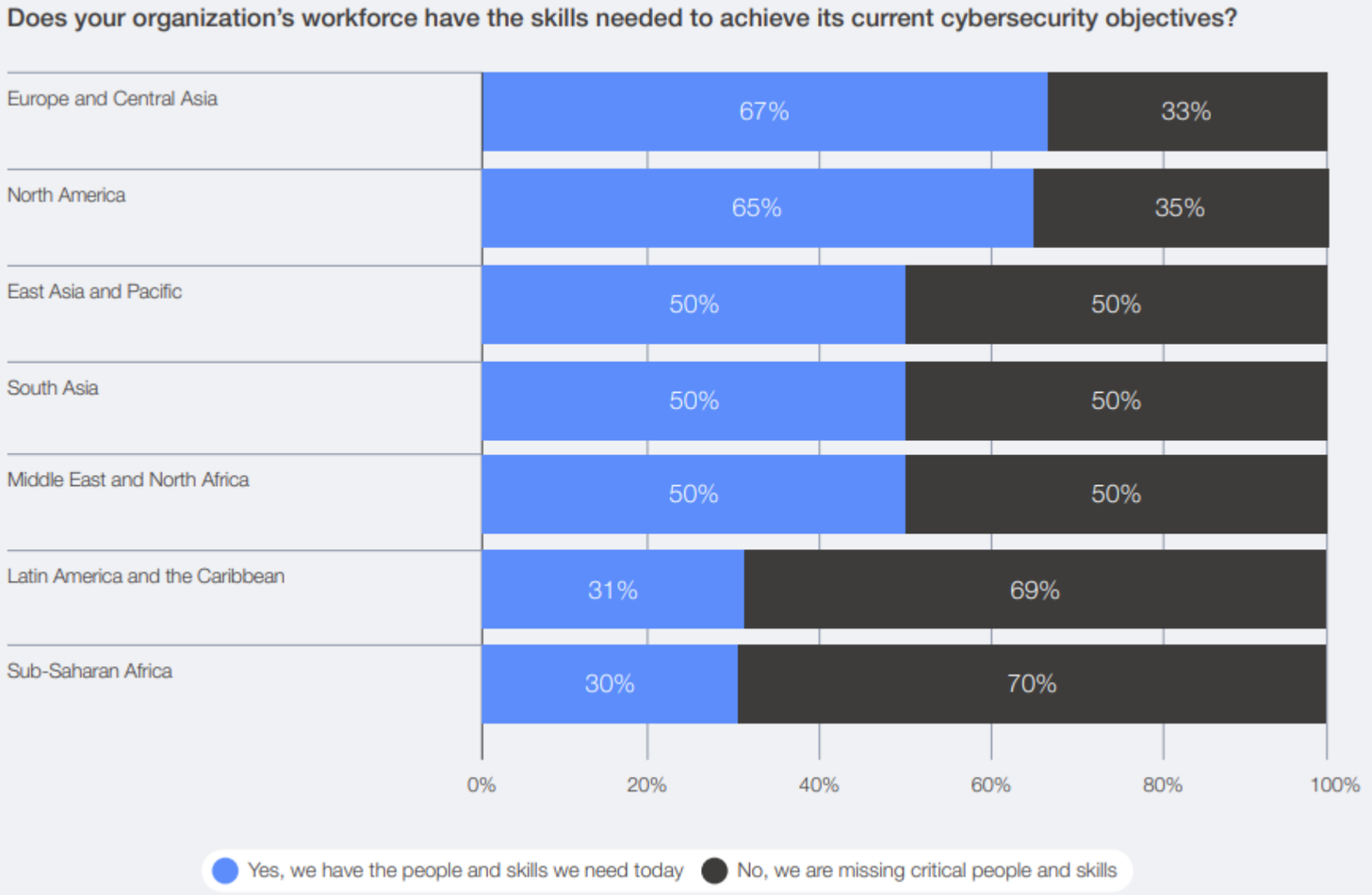
Inequity

The Talent Crisis:

- In many parts of the world, over half of CEOs say they simply **don't have the people** needed to meet their security goals.

Regional Disparity:

- While Europe and North America have more resources, **Sub-Saharan Africa** and **Latin America** face the steepest climb to find qualified cyber talent.



Cybersecurity Trends: The 2026 Risk Landscape

Cybersecurity Trends: The 2026 Risk Landscape

WORLD ECONOMIC FORUM

Inequity

Global Risks Changing by AI

Geopolitics as a Security Driver

The Evolution of Cybercrime, AI, Fraud

Resilience as Economic Value

The Supply Chain Transparency Crisis

The Widening Cyber Inequity

The Rise of "Silent" Threats

Global Risks Changing by AI

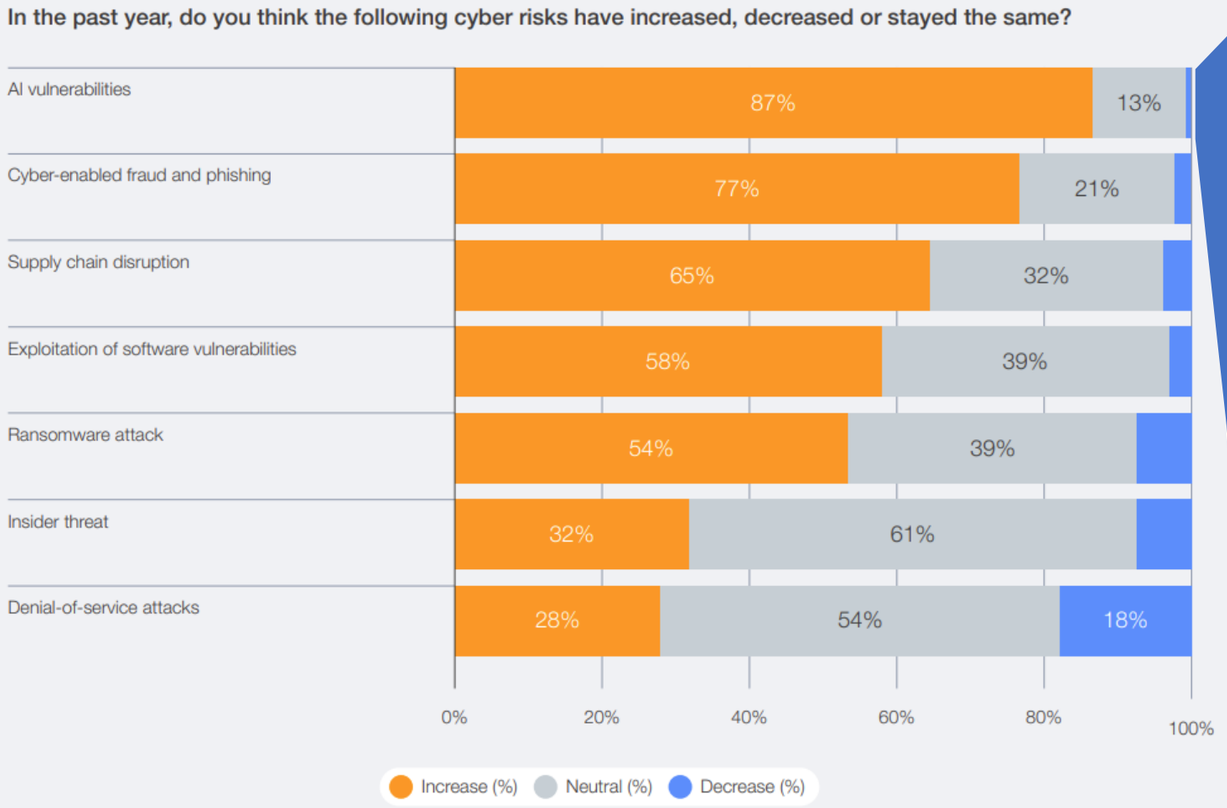
Cybersecurity Trends: The 2026 Risk Landscape

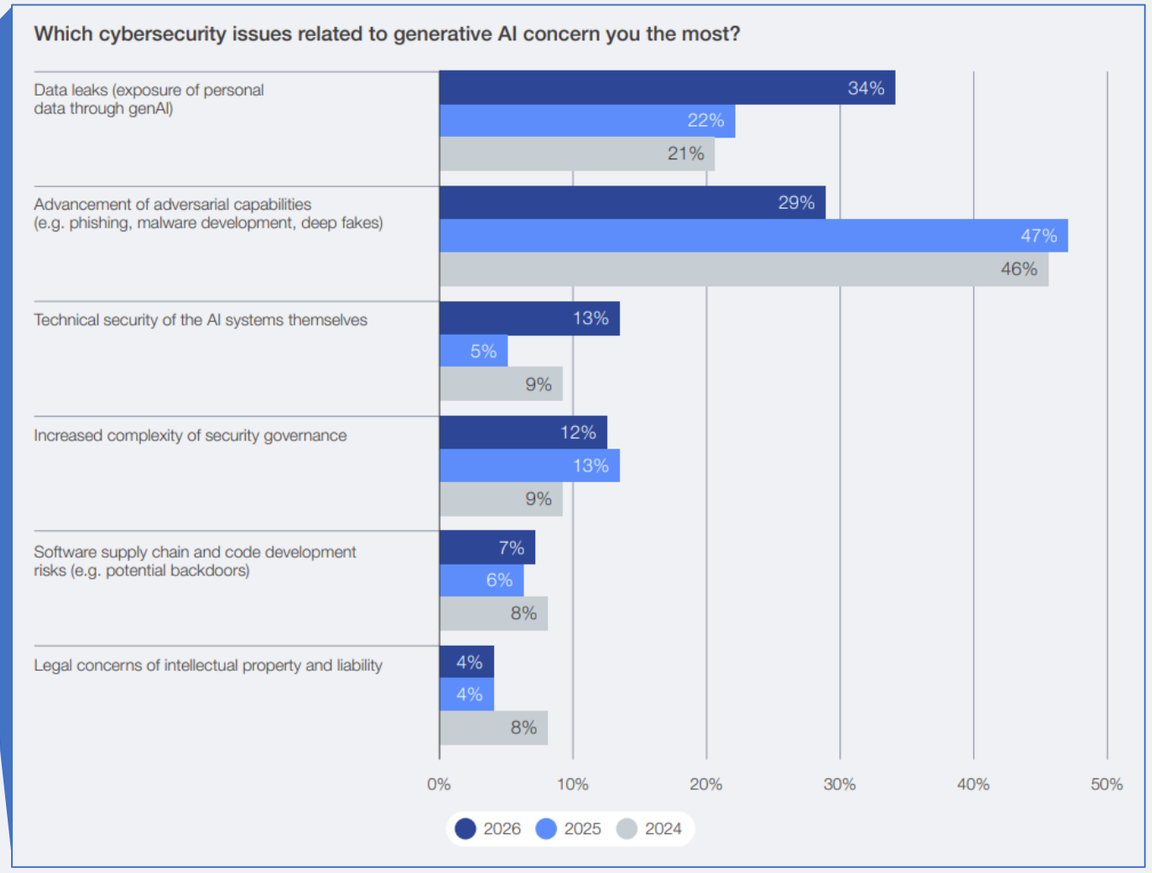
Global Risks Changing by AI

The Highlighted Cybersecurity Risk:

- Ranked as the fastest-growing risk, highlighting how quickly AI is changing the threat landscape.

The Big Reversal: In a major shift from last year, CEOs are now more worried about **internal data leaks** than hackers' AI capabilities.



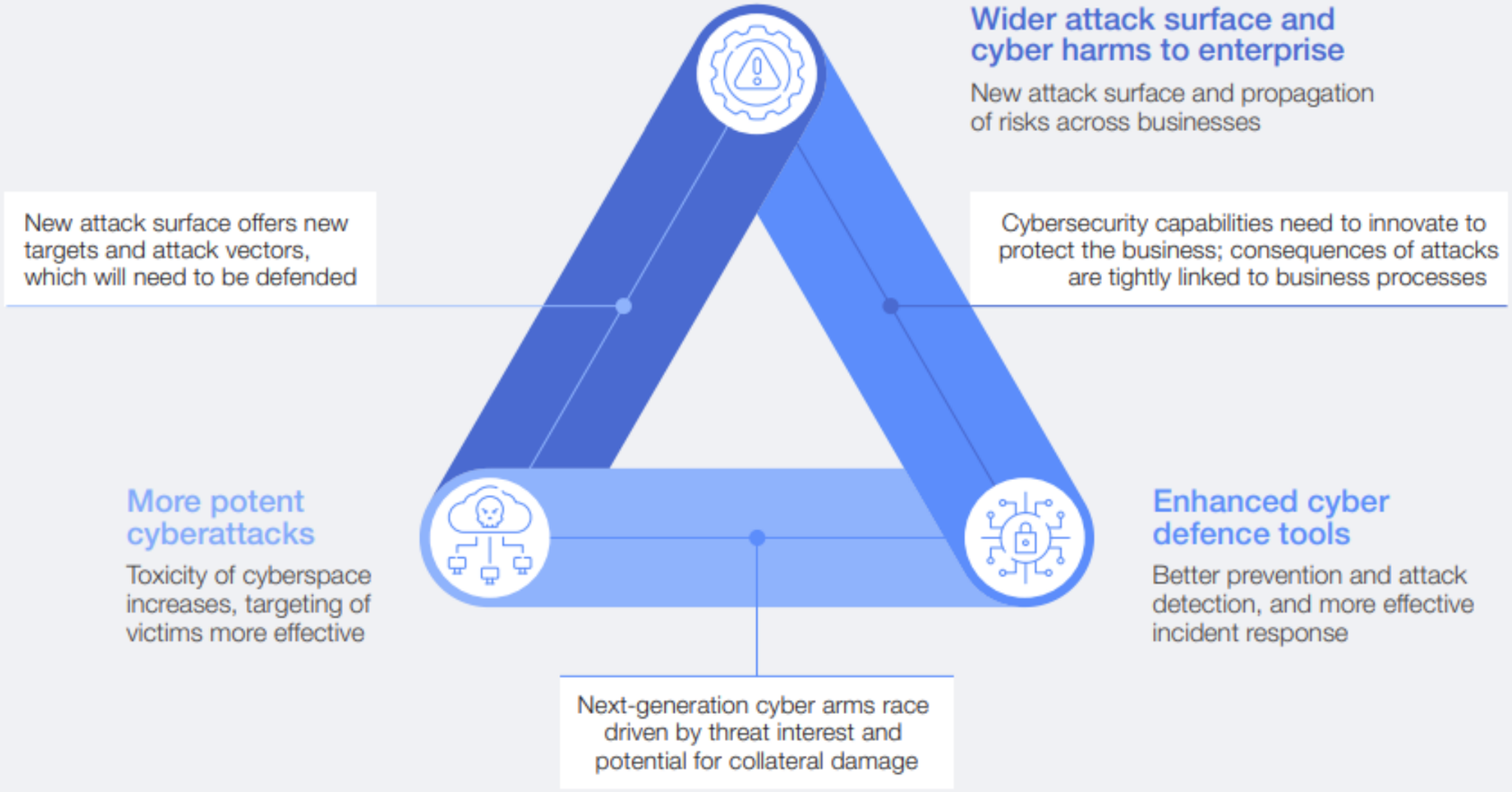


Cybersecurity Trends: The 2026 Risk Landscape

Global Risks Changing by AI

Impact	Description
New Weak Spots	Using AI creates new vulnerabilities that traditional security isn't built to fix.
Supercharged Defense	AI helps security teams find threats faster and automate repetitive work.
Smarter Attacks	Hackers use AI to make scams more precise and attacks more automated.

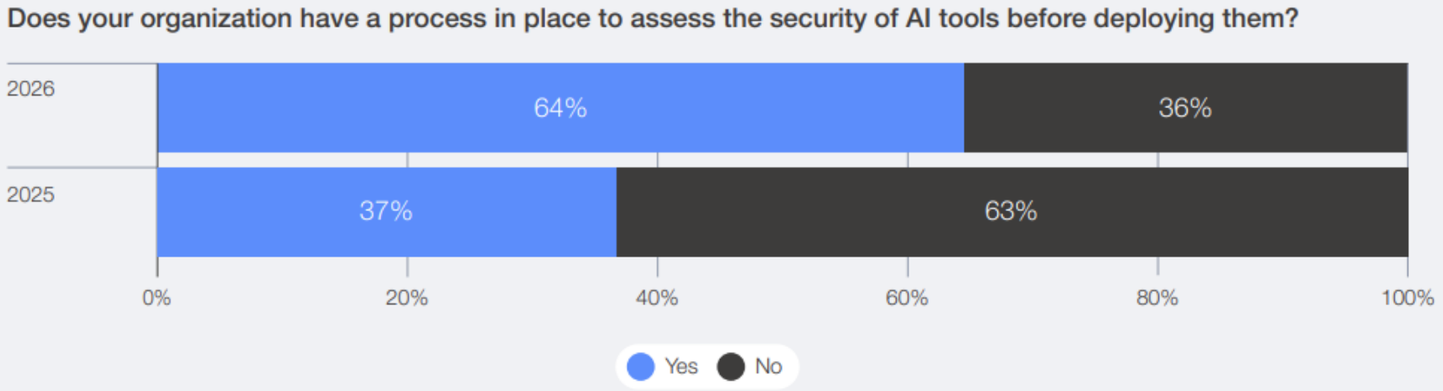
Impacts of AI on cybersecurity



Source: Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards. (2025). World Economic Forum[2]

Cybersecurity Trends: The 2026 Risk Landscape

Global Risks Changing by AI



Organizations assessing AI security nearly doubled, rising from 37% in 2025 to 64% in 2026.

Shift to Continuous Assurance:

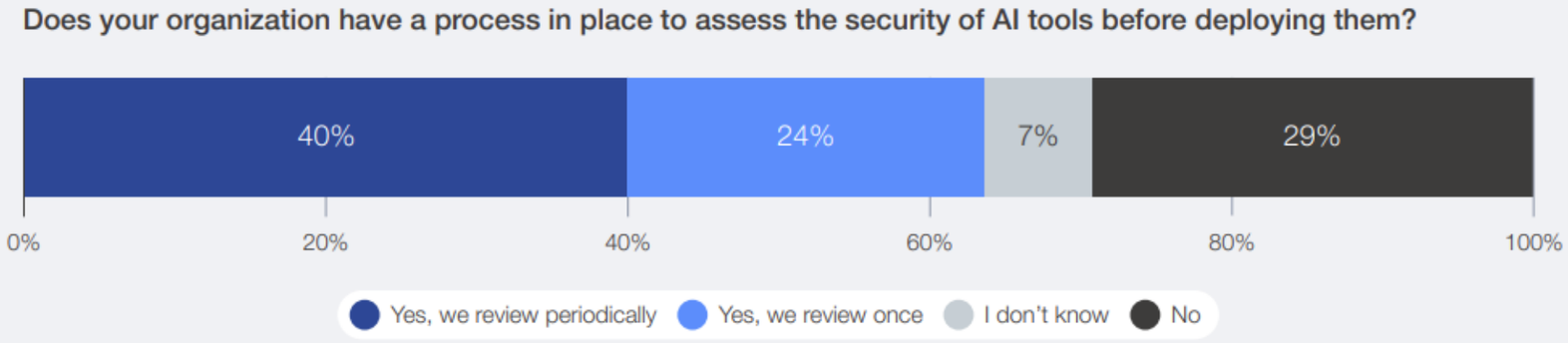
- 40% of organizations now conduct periodic reviews of AI tools before deployment, moving away from "one-time" checks (24%).

Significant Security Gap:

- Roughly one-third (~33%) of organizations still have no process to validate AI security before use.

Systemic Exposure:

- This lack of validation creates serious risks, even as the race to use AI for cyber defense speeds up.



AI is not a "plug-and-play" solution. To win in 2026, you must wrap AI in **strong governance** and keep **human judgment** at the heart of your security.

Cybersecurity Trends: The 2026 Risk Landscape

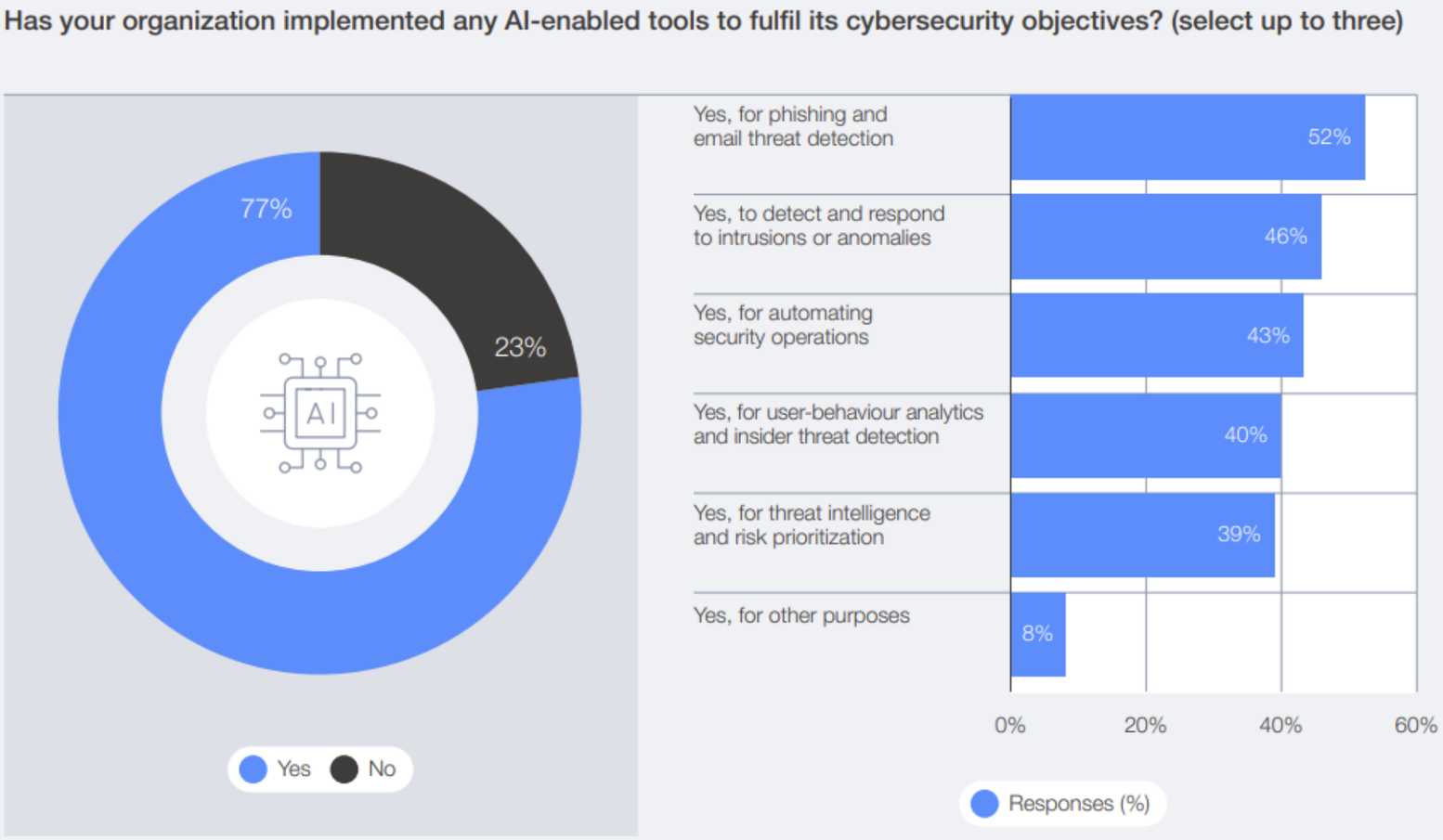
Global Risks Changing by AI

AI Agents Challenges

- **Security & Governance Challenges:** Their integration challenges traditional security frameworks and raises questions about automated decision-making and alert prioritization.
- **Identity & Access Complexity:** Managing agent credentials and permissions is now as critical—and potentially more complex—than managing human users.
- **Need for Zero-Trust:** Without strong governance, agents risk accumulating excessive privileges or being manipulated via prompt injections, requiring continuous verification and "zero-trust" principles.

Widespread Adoption:

- 77% of organizations have already adopted AI for cybersecurity to stay ahead of increasingly sophisticated threats.



Cybersecurity Trends: The 2026 Risk Landscape

Global Risks Changing by AI

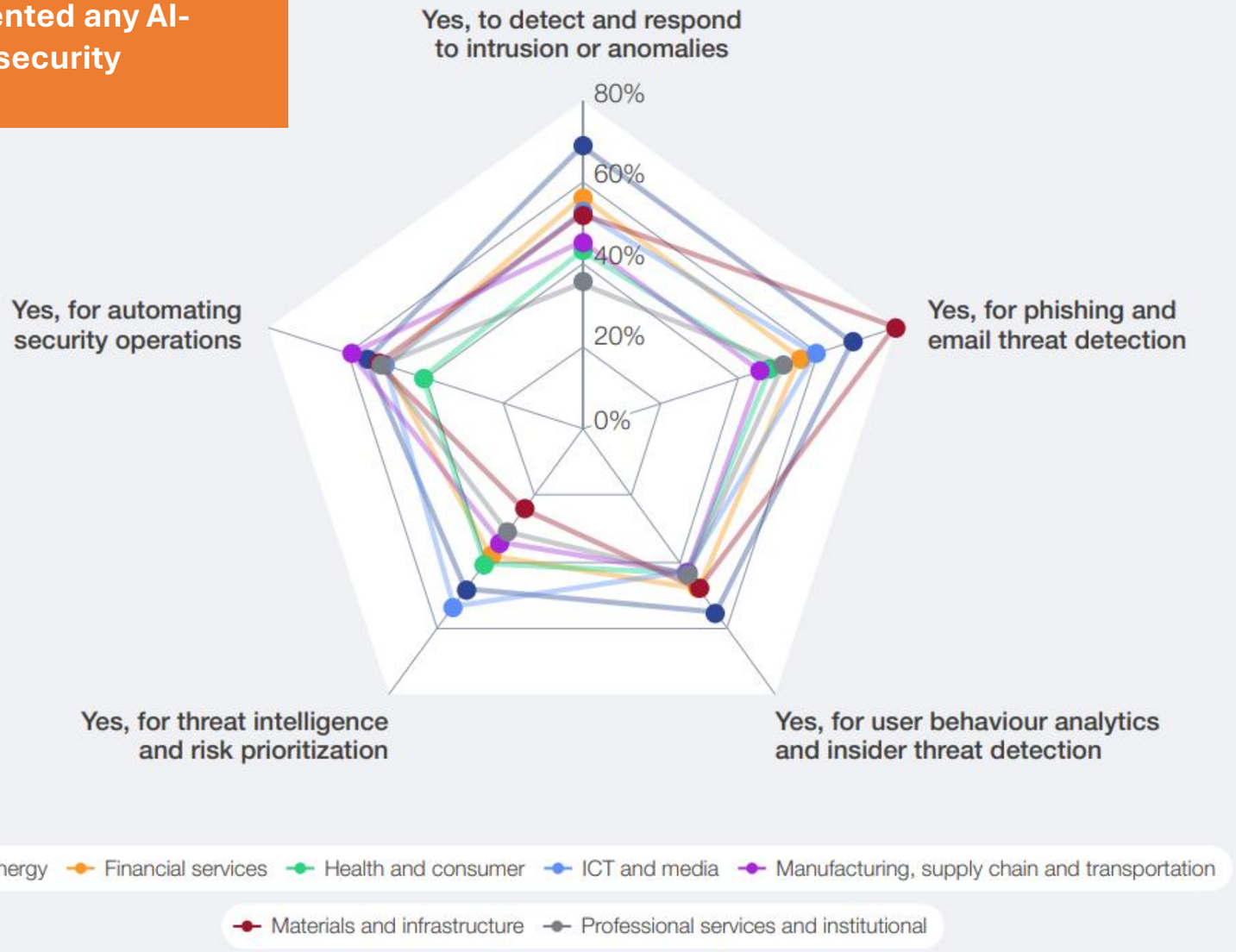
Skills and Strategic Priorities

- **Fast-Growing Demand:** "Networks and cybersecurity" are projected to be among the top three fastest-growing skills by 2030, alongside AI and big data.
- **The New Skill Set:** Modern security professionals must blend technical proficiency with strategic and ethical literacy.
- **Organizational Path Forward:** The recommended strategy is a collaborative model anchored in **security-by-design** principles, focusing on AI literacy and continuous validation.

Cybersecurity Trends: The 2026 Risk Landscape

Global Risks Changing by AI

Has your organization implemented any AI-enabled tools to fulfil its cybersecurity objectives?



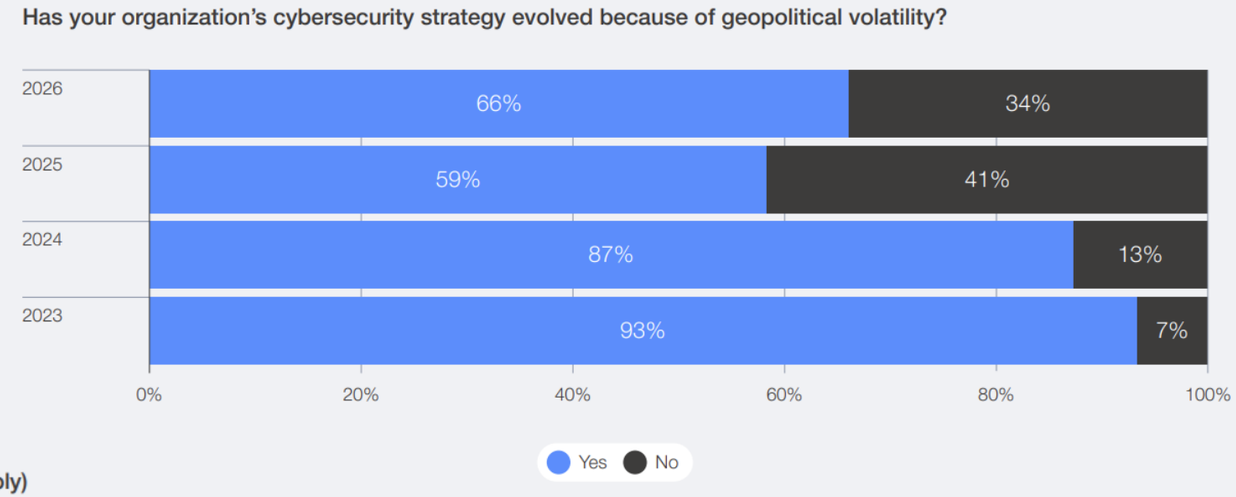
Geopolitics as a Security Driver

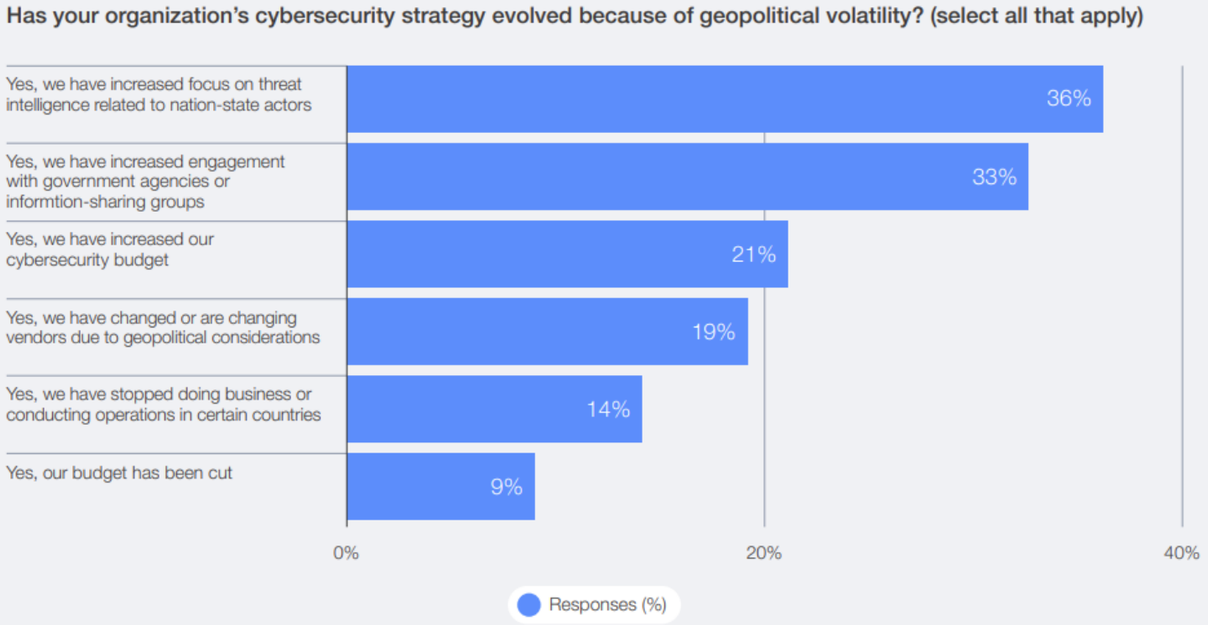
Cybersecurity Trends: The 2026 Risk Landscape

Geopolitics as a Security Driver

Geopolitical Impact on Cybersecurity Strategy

- Strategy is now defined by a "fragmented" world characterized by trade wars, sanctions, and intense technological competition.
- While the percentage of organizations shifting their strategy due to geopolitics dropped from 93% in 2023 to 66% in 2026, this indicates that geopolitical risk is no longer a "shock" but a permanent, integrated feature of modern cyber defense.





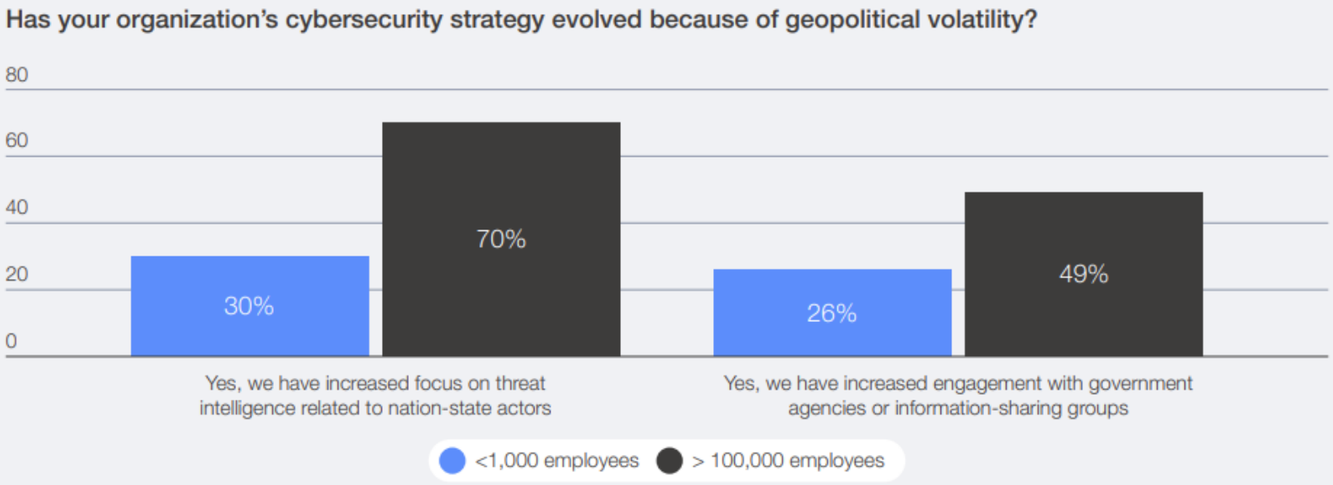
Geopolitical Resilience: The Shift to Collaboration

- **End of Isolated Defense:** Organizations are moving away from protecting themselves in silos and are instead shifting toward **intelligence-driven collaboration**.
- **Top Strategic Shifts:** To handle geopolitical volatility, leaders are prioritizing **threat intelligence** and **government engagement** as the two biggest changes to their security plans.
- **Shared Awareness:** There is a growing consensus that surviving global uncertainty requires **shared situational awareness**—knowing what is happening globally by working together.

Cybersecurity Trends: The 2026 Risk Landscape

Geopolitics as a Security Driver

The Scale of Collaboration: Large vs. Small Employers



Global Exposure Drives Action:

- Large global organizations lead the shift toward intelligence-driven collaboration because their widespread operations make them more vulnerable to geopolitical volatility.
- Smaller organizations often lack the staff and global footprint to participate in collective security, leading them to "accept" geopolitical risks rather than actively mitigating them

The Intelligence Gap:

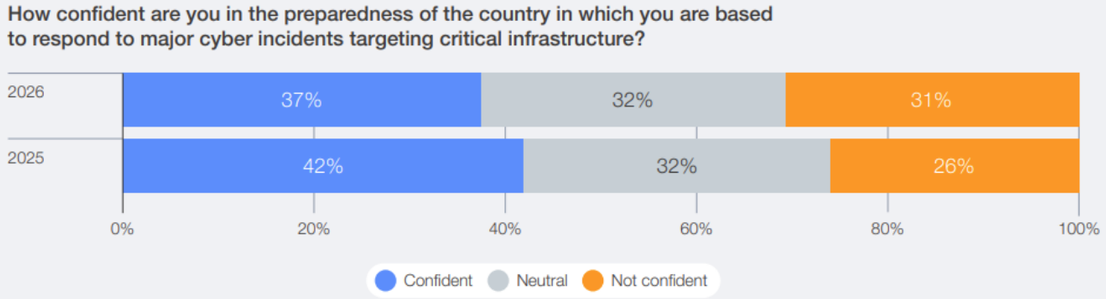
- 70% of the largest employers (over 100,000 employees) have ramped up their focus on threat intelligence, while only 30% of small employers (under 1,000 employees) have done the same.

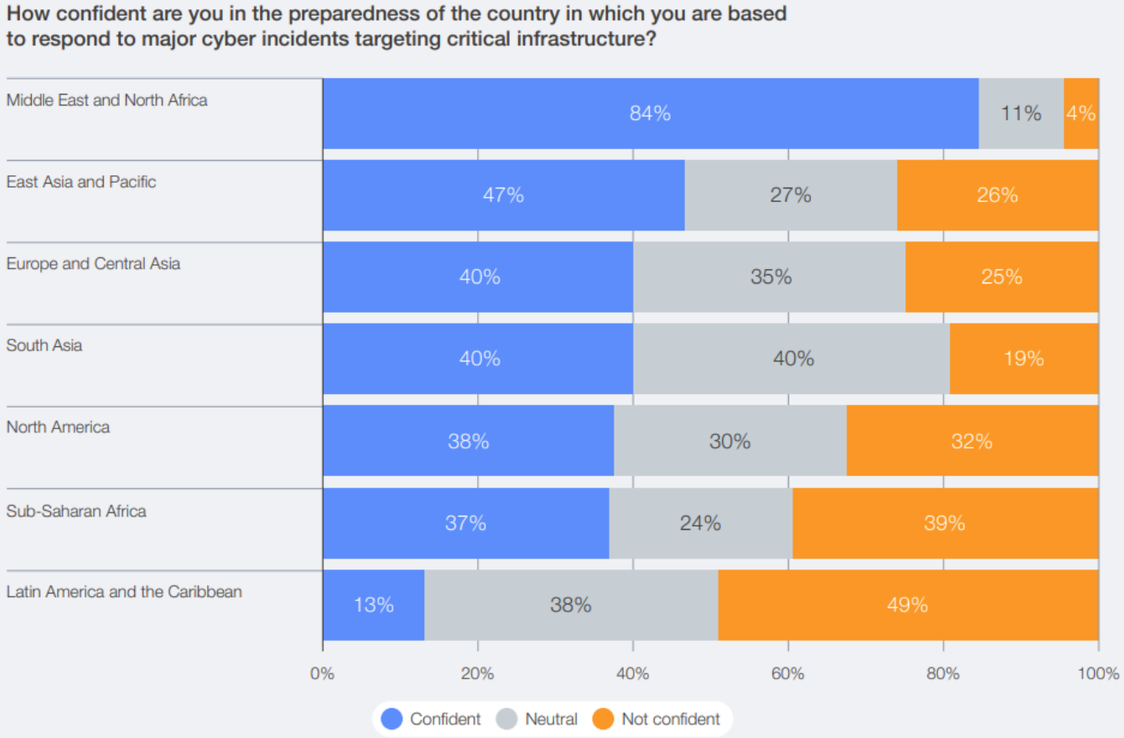
Government Partnerships:

- 49% of large organizations are deepening ties with government agencies and sharing groups, nearly double the 26% rate of smaller firms.

Cybersecurity Trends: The 2026 Risk Landscape

Geopolitics as a Security Driver





The Global Confidence Gap

- **National Readiness Concerns:** 31% of leaders now lack confidence in their country's ability to respond to a major cyber incident, up from 26% last year.

Highest Confidence:

- Respondents in the **Middle East and North Africa (MENA)** report the highest degree of confidence at **84%**.

Lowest Confidence:

- Conversely, those in **Latin America and the Caribbean** express significantly less faith, with confidence levels dropping to only **13%**.

Significant Variance:

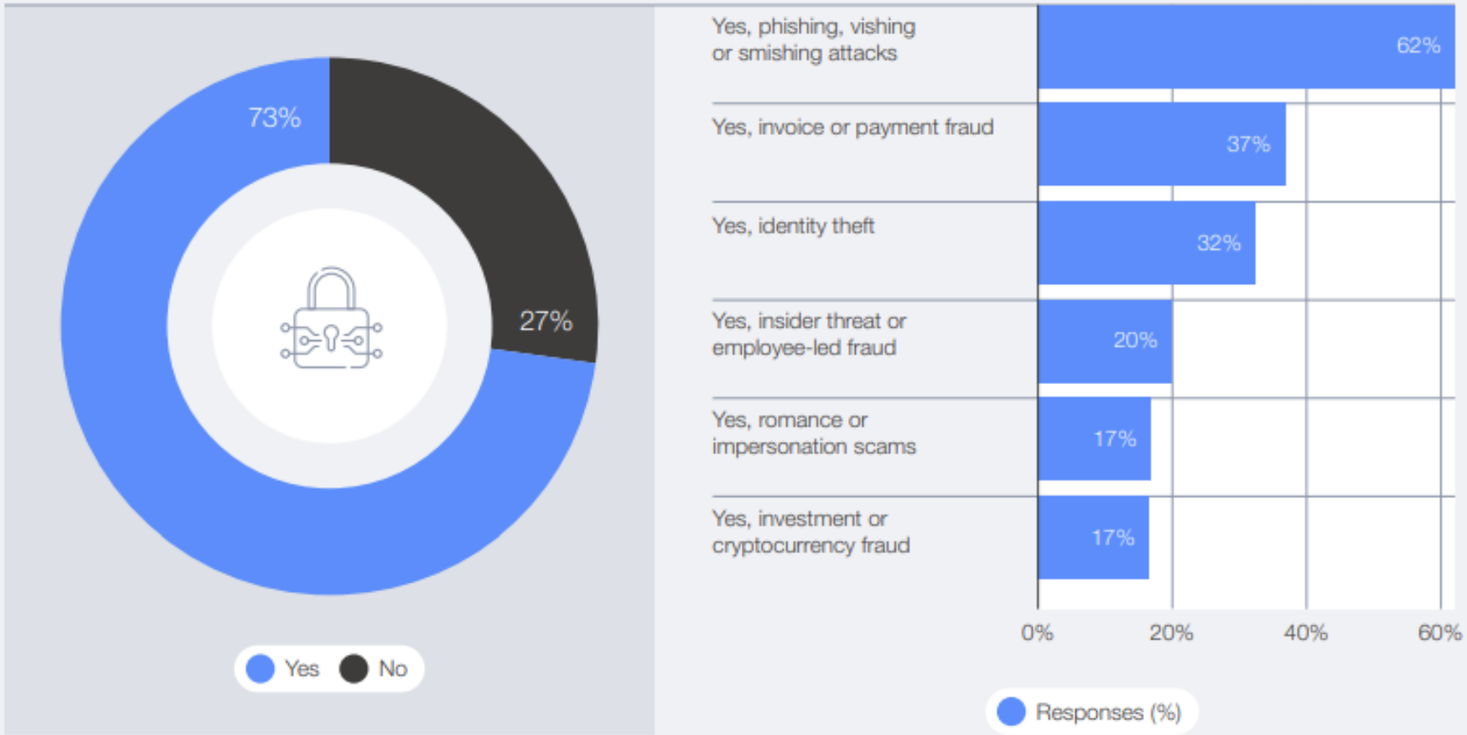
- This highlights a massive global gap in perceived national security readiness across different geographical zones.

The Evolution of Cybercrime, AI, Fraud

Cybersecurity Trends: The 2026 Risk Landscape

The Evolution of Cybercrime, AI, Fraud

Have you or anyone in your professional/personal network been affected by cyber-enabled fraud in the past 12 months? (select all that apply)



Growth Trend:

- 77% of leaders reported an overall increase in cyber-enabled fraud and phishing.

Personal Impact:

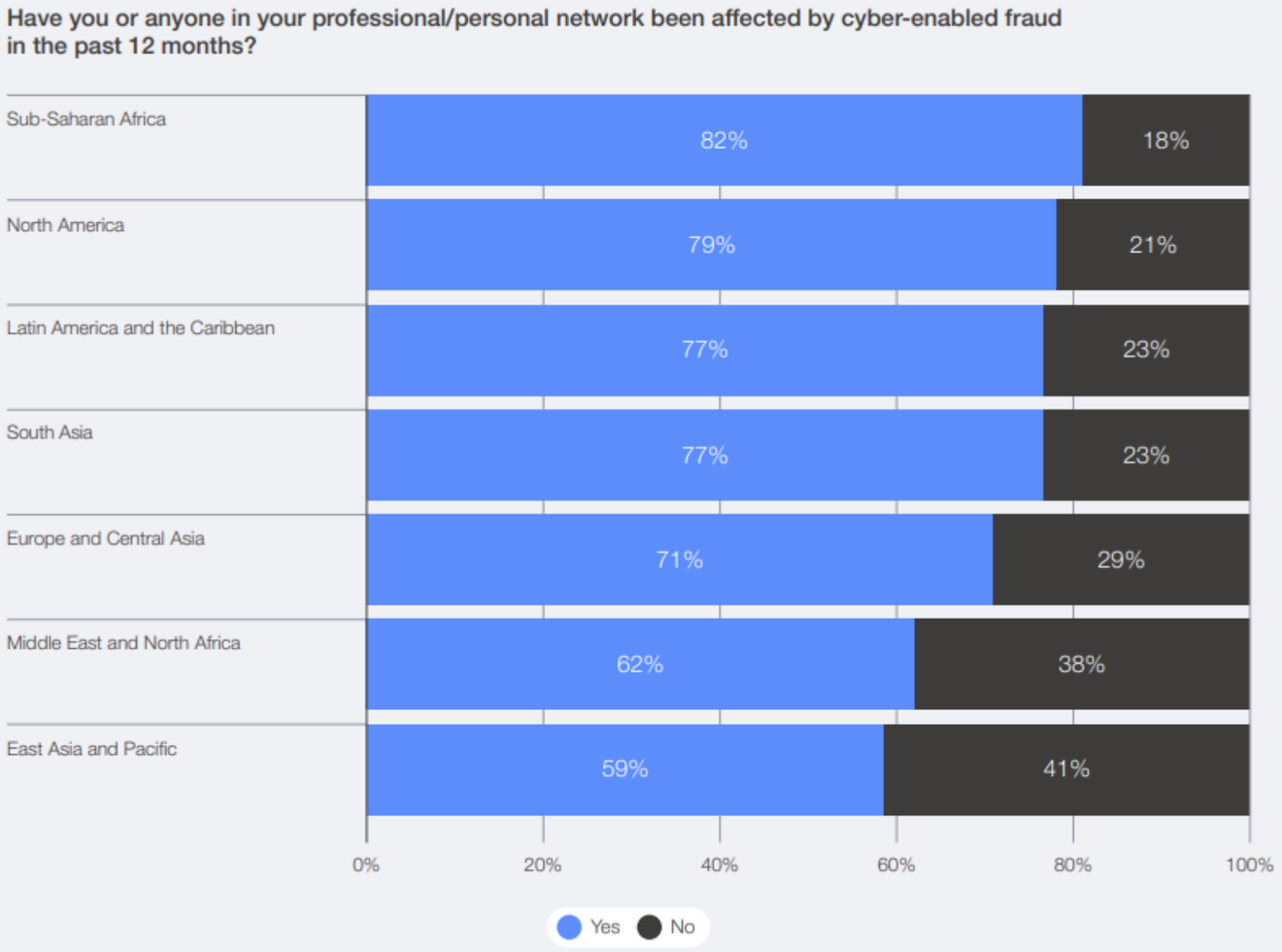
- 73% of respondents stated that they or someone in their professional network has been personally affected by fraud.

Top 3 Attack Vectors:

- **Phishing:** Including vishing (voice) and smishing (SMS).
- **Payment Fraud:** Direct financial targeting.
- **Identity Theft:** Stealing credentials or personal data.

Cybersecurity Trends: The 2026 Risk Landscape

The Evolution of Cybercrime, AI, Fraud



While the global data shows a high impact of fraud, the regional breakdown reveals a unique position for the East Asia and Pacific region, including Thailand.

Regional Impact (59%):

- At 59%, the East Asia and Pacific region reports the lowest percentage of people affected by cyber-enabled fraud compared to areas like Sub-Saharan Africa (82%) or North America (79%).

Strategic Context:

- Despite being the lowest statistically, nearly **6 in 10** professionals in this region are still impacted. In Thailand specifically, this pressure is often felt through high-stakes mobile banking security and strict regulatory compliance requirements from the **Bank of Thailand (BOT)**, **SEC**, and **OIC**.

Cybersecurity Trends: The 2026 Risk Landscape

The Evolution of Cybercrime, AI, Fraud

AI-Powered Deception & Automation

Scaling Social Engineering: GenAI automates the creation of high-fidelity phishing, deepfake audio/video, and localized content that evades traditional human and system scrutiny.

Weaponized Datasets: Attackers use models trained on breached data to replicate authentic communication styles and enhance targeting precision.

The Agentic Turning Point: Shift from simple reconnaissance to **autonomous AI agents** capable of executing the entire attack life cycle—from exploitation to data exfiltration—independently.

To counter these "silent" and automated threats, a **Systemic Defense Framework** is required:

Prevention:

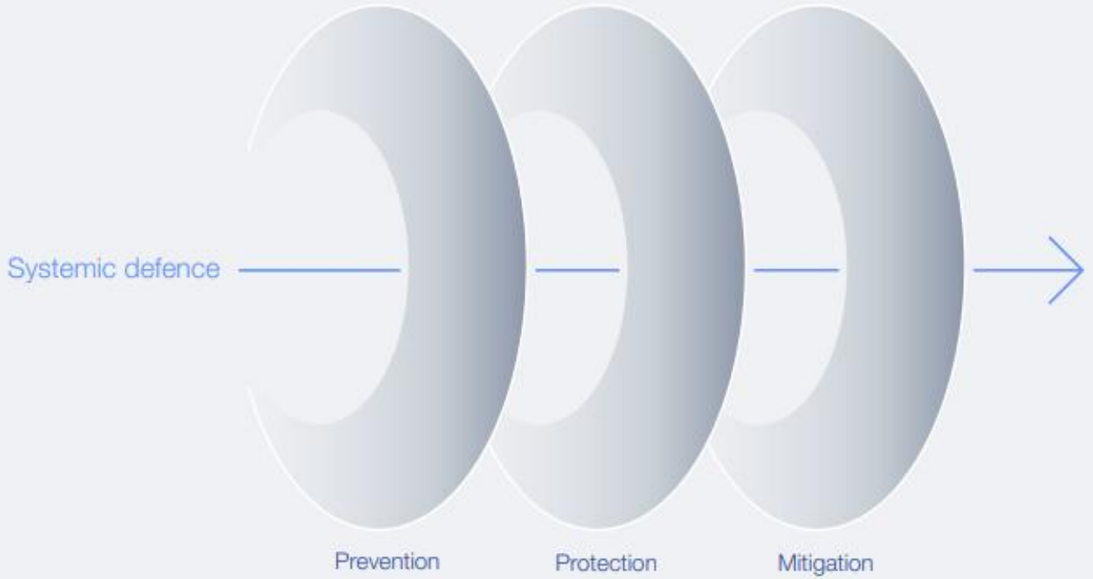
- Stronger verification and AI literacy.

Protection:

- Guarding training data and using security-by-design.

Mitigation:

- Cross-platform coordination and adaptive response to deepfake events.



Source: Fighting Cyber-Enabled Fraud: A Systemic Defence Approach. (2025). World Economic Forum

Resilience as Economic Value

Cybersecurity Trends: The 2026 Risk Landscape

Resilience as Economic Value

Cyber Resilience: Trends and Progress in 2026

- **Significant Growth:** Despite the low overall percentage, there has been a double-digit increase in organizations exceeding requirements, rising from 9% in 2025 to 19% in 2026.
- **Growing Confidence:** Overall survey data reflects a rising trend in organizational confidence regarding their ability to withstand and recover from cyberattacks.

Top 3 Barriers to Resilience

Organizations report three primary obstacles preventing them from achieving higher levels of cyber resilience.

Rapidly Evolving Threats (61%)

- : The speed of new technology adoption and the changing nature of attacks.

Supply Chain Vulnerabilities (46%):

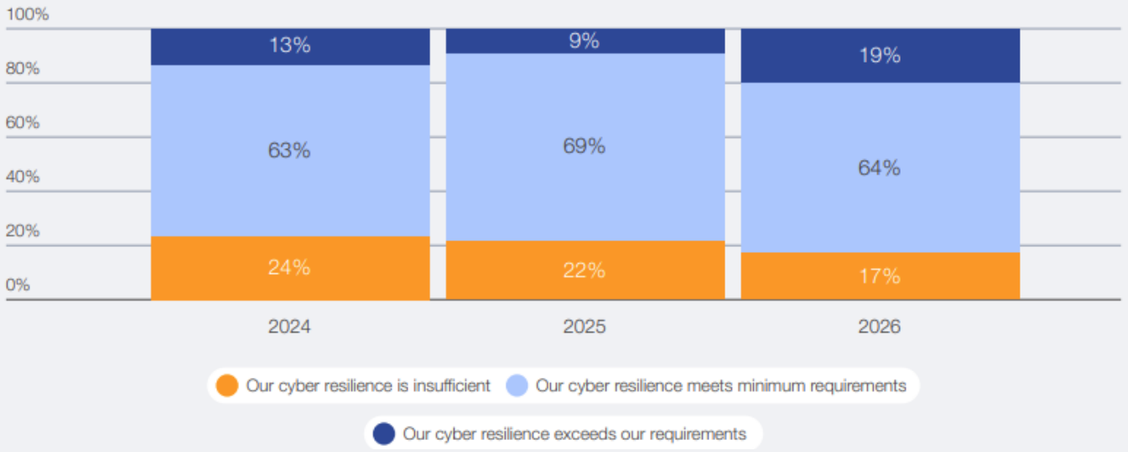
- Risks introduced through third-party partners and complex vendor networks.

Skills Shortage (45%):

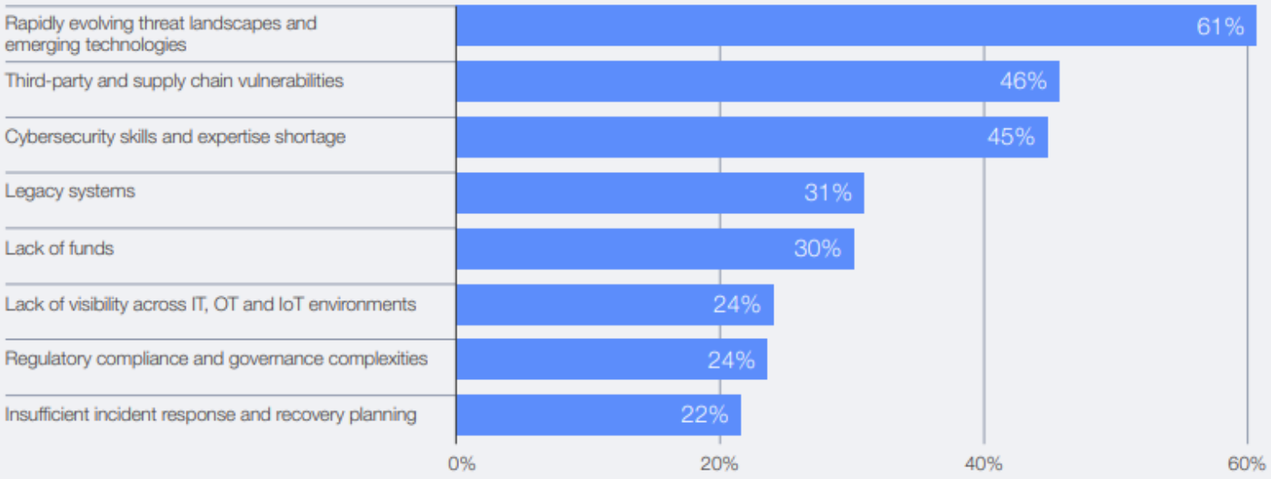
- A critical lack of internal expertise and cybersecurity personnel.

With AI is the technologies with the greatest cybersecurity impacts in next 12 months

How would you rate your organization's cyber resilience?

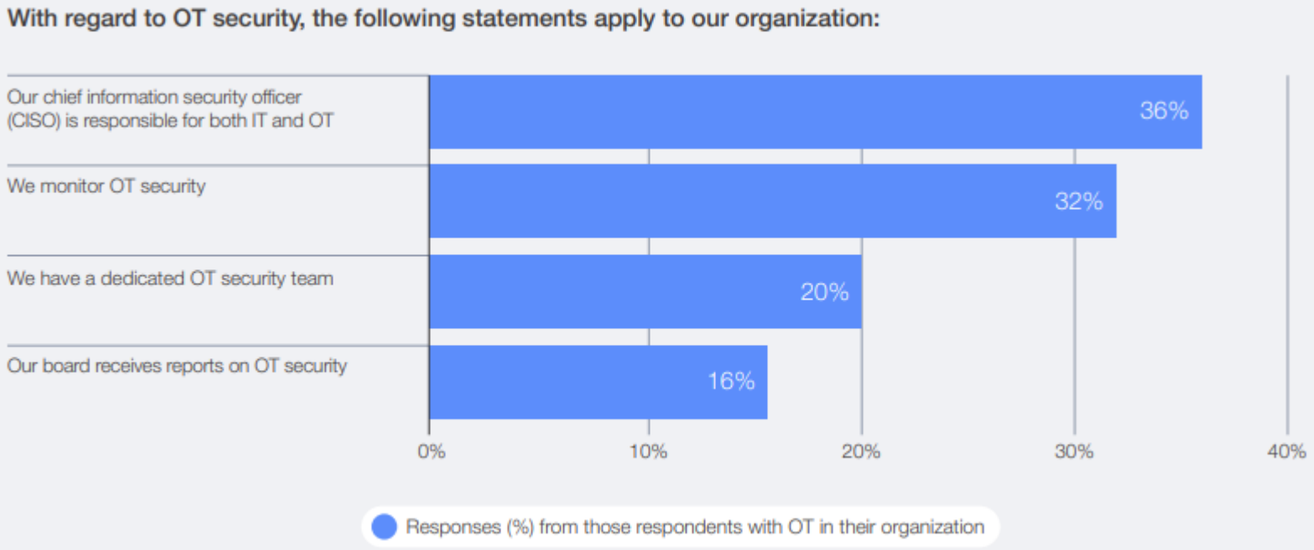


What is your organization's greatest challenge to becoming cyber resilient? (select up to three)



Cybersecurity Trends: The 2026 Risk Landscape

Resilience as Economic Value



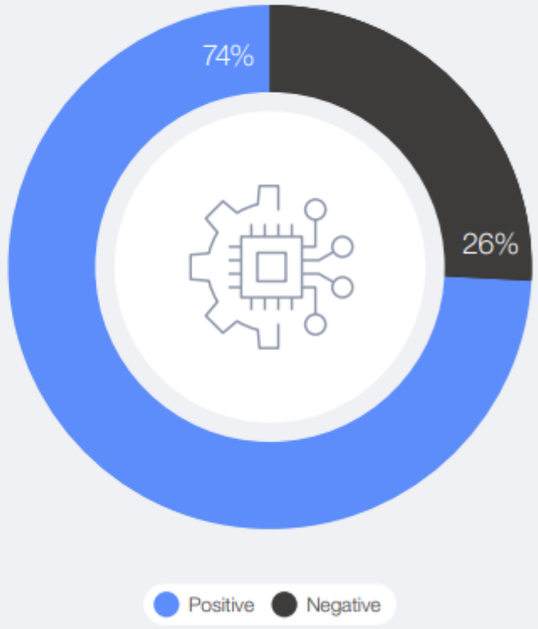
The Convergence Crisis: IT/OT Security

- **The Death of the Air-Gap:**
  - Strict segregation between Information Technology (IT) and Operational Technology (OT) is no longer tenable due to modern connectivity demands.
- **High-Stakes Sectors:**
  - This shift primarily affects manufacturing, energy, transportation, and critical infrastructure.
- **Modernization Barriers:**
  - OT environments are slow to adapt because they are deeply integrated into core functions and have long investment cycles.
- **Need for Segmentation:**
  - To manage risk in a connected environment, organizations must shift focus to advanced network segmentation.

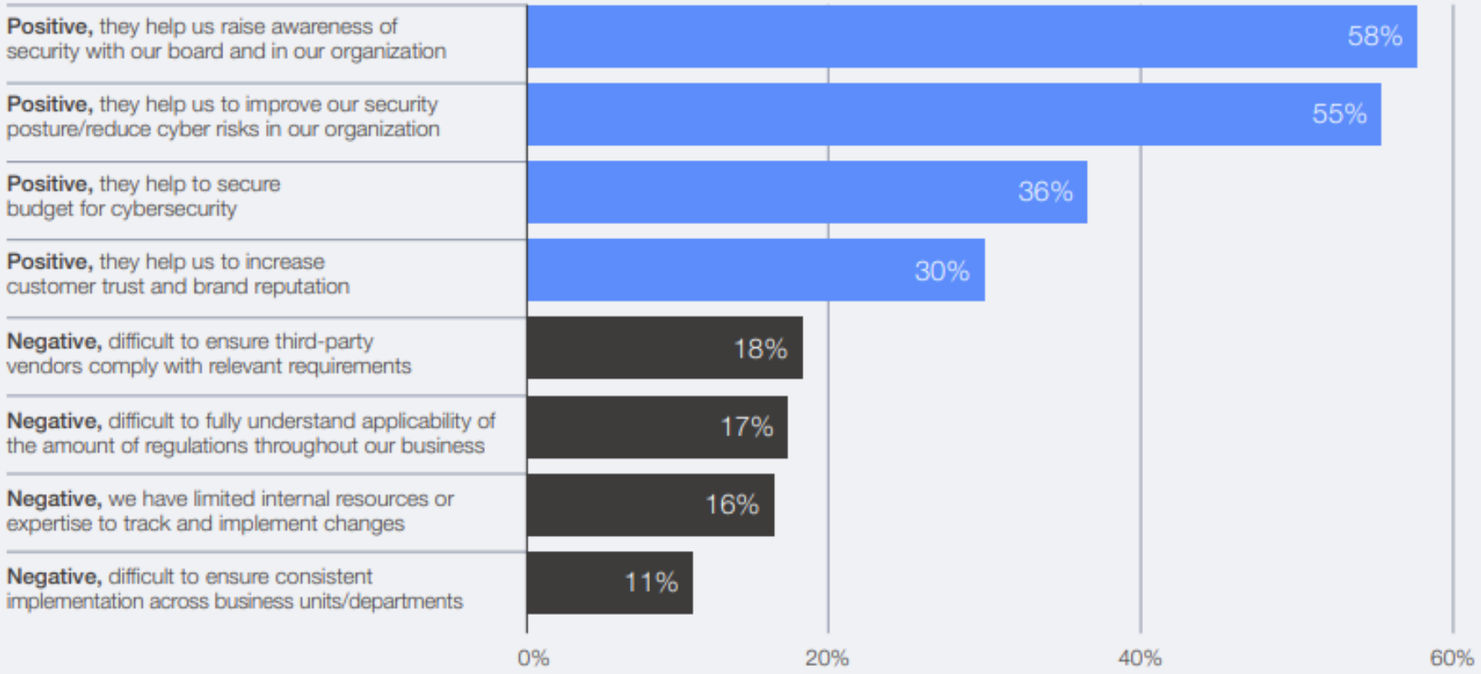
Cybersecurity Trends: The 2026 Risk Landscape

Resilience as Economic Value

What is your view about the effectiveness of cyber-related regulations?



What is your view about the effectiveness of cyber-related regulations? (select up to three)



The State of Global Cyber Regulation

The Strategic Benefits

- **Boardroom Leverage: 58% of practitioners** find that regulations are the most effective tool for raising cybersecurity awareness among board members and executives.
- **Operational Gains: 55%** report that these rules drive **tangible improvements** in the organization's overall security posture, moving security from a "theoretical" concern to a practical reality.

The Practical Challenges

- **Supply Chain Friction: 18%** of respondents struggle with the logistical nightmare of ensuring **third-party vendors** comply with a diverse set of global requirements.
- **Internal Roadblocks: 16%** cite a lack of internal resources and specialized expertise as a major barrier to compliance.
- **Clarity Issues:** Organizations are also finding it difficult to determine exactly how and where certain regulations apply across different **business units**.

Cybersecurity Trends: The 2026 Risk Landscape

Resilience as Economic Value

The Cyber Resilience Compass

Objective: A collaborative framework that shares proven, frontline practices to strengthen organizational resilience.

Source: The Cyber Resilience Compass: Journeys Towards Resilience. (2025). World Economic Forum

Compass category	Hallmark	High resilience	Insufficient resilience
Leadership	Board members hold personal liability in the event of cyber breaches	30%	9%
Governance, risk and compliance	Hold a positive view on effectiveness of cyber-related regulations	79%	62%
People and culture	Have the skills needed to achieve current cybersecurity objectives	78%	15%
Business processes	Involve security function in the procurement process	76%	53%
Technical systems	Assess the security of AI tools before deploying them	83%	39%
Crisis management	Simulate cyber incidents and/or plan recovery exercises with ecosystem partners	44%	16%
Ecosystem engagement	Assess the security maturity of suppliers	74%	48%

Cybersecurity Trends: The 2026 Risk Landscape

Resilience as Economic Value

1. Leadership

- **Board Engagement:** 99% of resilient organizations have boards involved in cyber.
- **Strategic Role:** 45% have clearly defined oversight roles, ensuring CISOs can translate technical risks into business actions.

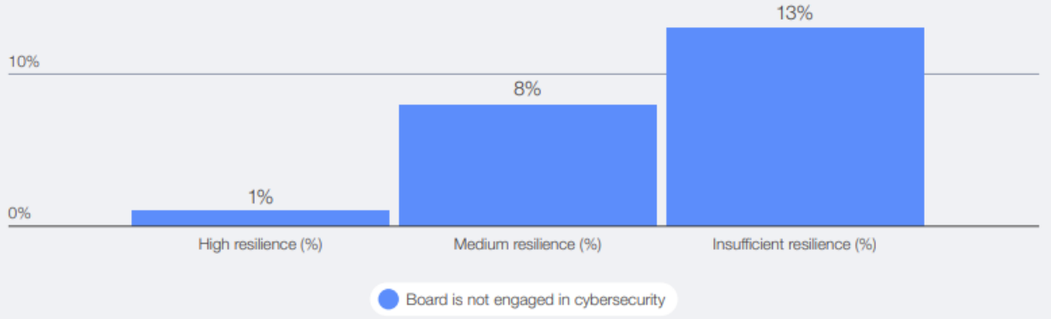
2. Governance, Risk, and Compliance (GRC)

- **Reputation Asset:** 44% of resilient firms use regulations to build **customer trust and brand value**, whereas struggling firms see them primarily as a resource drain (34%).

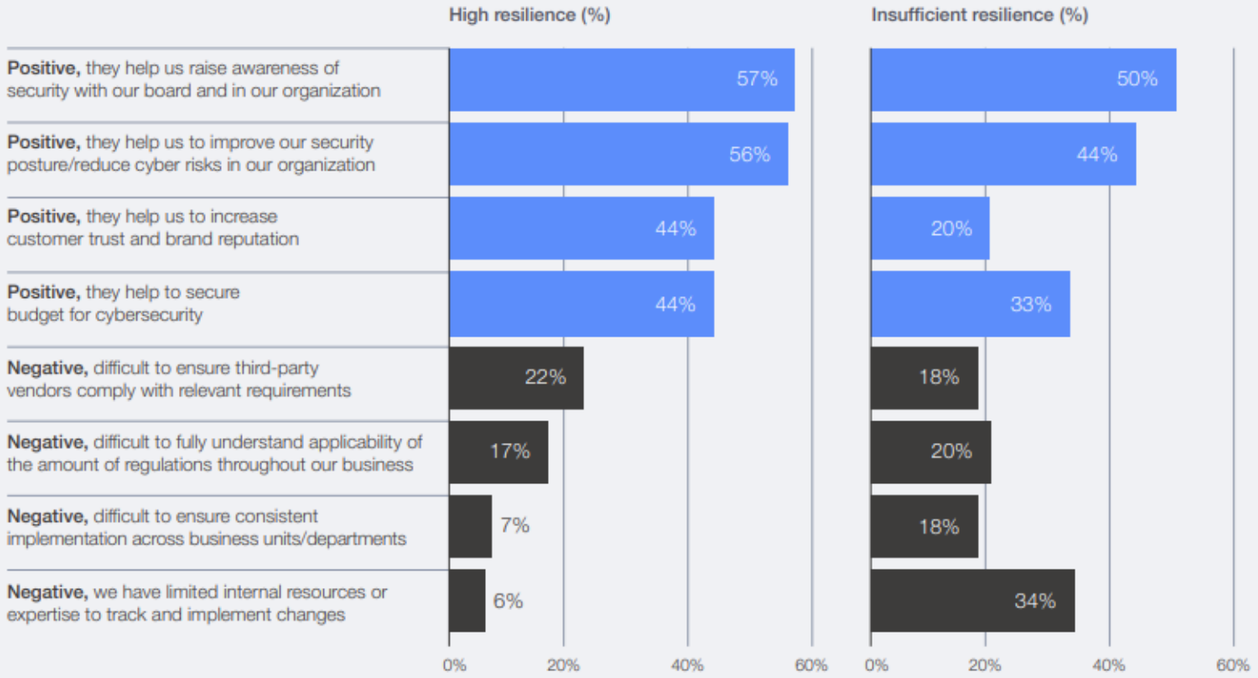
3. People and Culture

- **The Talent Gap:** A staggering **85% of insufficiently resilient organizations** lack the necessary workforce, compared to just 22% of resilient ones.

Board engagement gaps, across organizational resilience levels



What is your view about the effectiveness of cyber-related regulations?



Cybersecurity Trends: The 2026 Risk Landscape

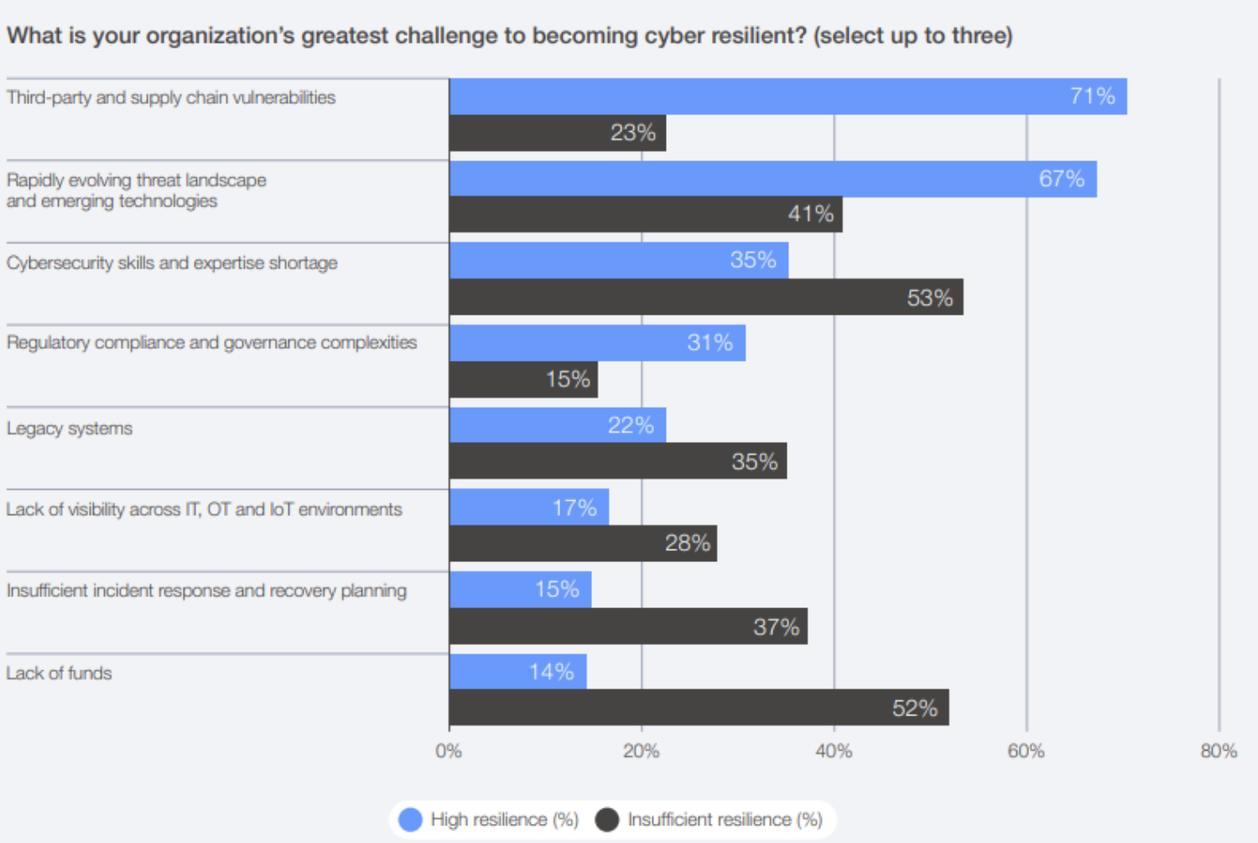
Resilience as Economic Value

4. Crisis Management

- **Ecosystem Simulations:** Rather than practicing in a vacuum, 44% of top-tier organizations run **joint cyber incident simulations** with their ecosystem partners.

5. Ecosystem Engagement

- **Supply Chain Priority:** Highly resilient firms rank **supply chain exposure** as their #1 risk. They are more likely to assess suppliers (74%) and proactively share threat intelligence (53%).



Cybersecurity Trends: The 2026 Risk Landscape

Resilience as Economic Value

6. Business Processes

- **Security by Design:** 76% of resilient organizations integrate their security function directly into the **procurement process**, ensuring third-party risk is managed before a contract is signed.

7. Technical Systems

- **Future-Proofing:** Resilient firms are significantly more likely to monitor **OT security** (44% vs. 9%) and regularly review the security of **AI tools** (71% vs. 20%).

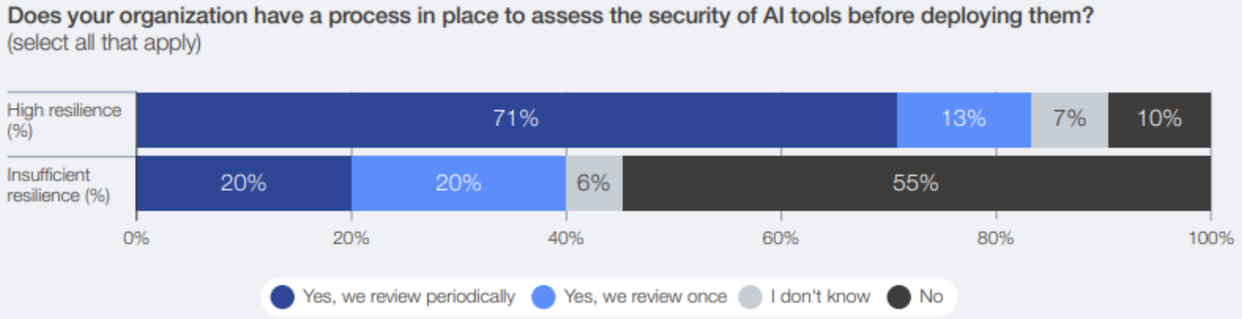


TABLE 5 **Ranking of cyber risk concerns, by organizational resilience level**

Rank	Insufficient resilience	Medium resilience	High resilience
1	Ransomware attack	Ransomware attack	**Supply chain disruption**
2	Cyber-enabled fraud and phishing	Cyber-enabled fraud and phishing	Exploitation of software vulnerabilities
3	Exploitation of software vulnerabilities	Exploitation of software vulnerabilities	Cyber-enabled fraud and phishing
4	AI vulnerabilities	AI vulnerabilities	Ransomware attack
5	**Supply chain disruption**	**Supply chain disruption**	AI vulnerabilities

The Supply Chain Transparency Crisis

Cybersecurity Trends: The 2026 Risk Landscape

The Supply Chain Transparency Crisis

The Cascading Impact of Supply Chain Risks

The "Butterfly Effect":

- Highly interconnected dependencies mean a single breach in one supplier can trigger a **global cascade**, crippling production and operations across multiple industries.

Mapping Blind Spots:

- Most organizations struggle to manage risk effectively because these complex interdependencies are **rarely clearly mapped**.

Real-World Precedent:

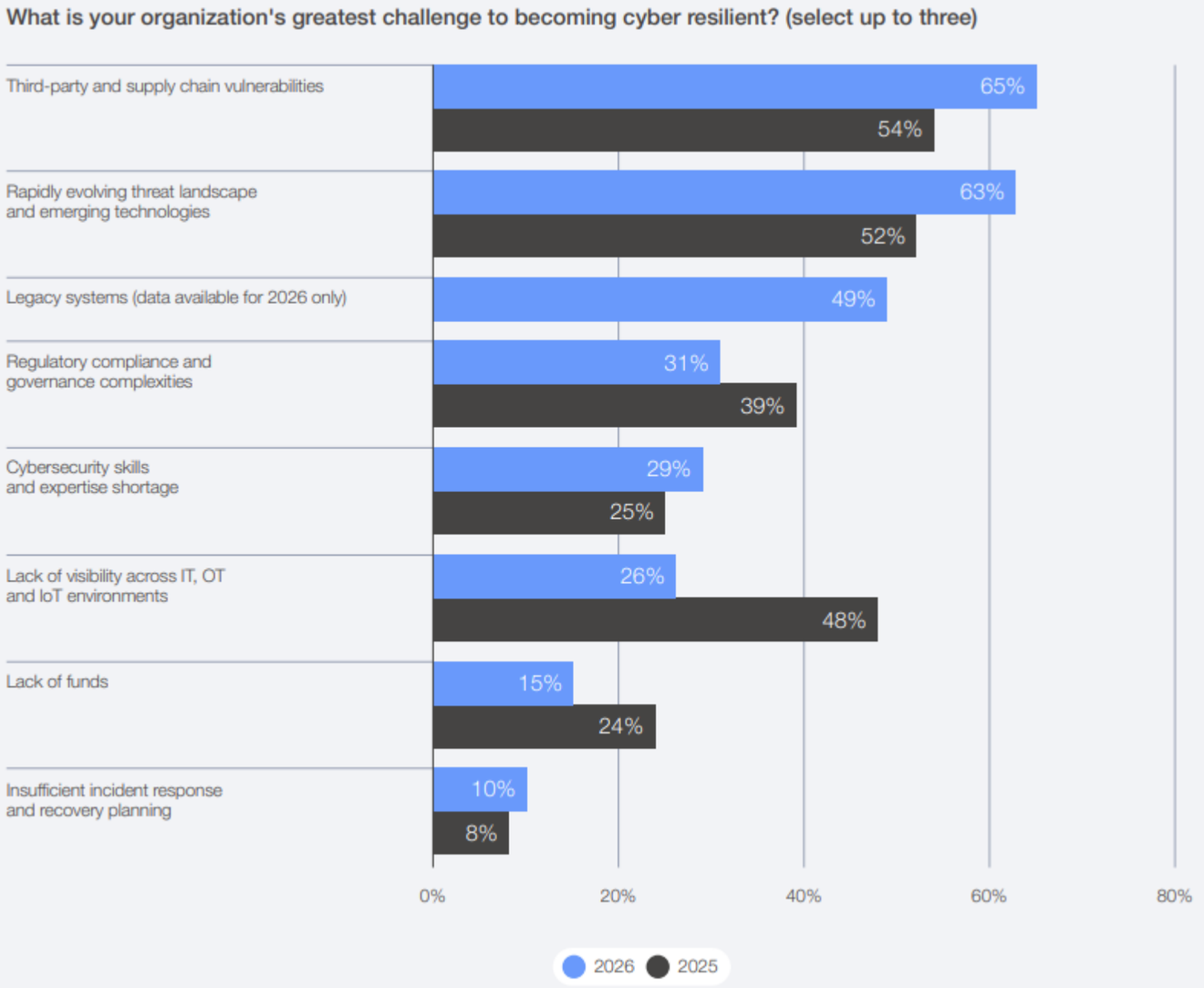
- The **September 2025 European airport attacks** illustrated this fragility; a minor breach in a shared boarding system caused widespread flight cancellations.

Critical Infrastructure Fear:

- There is growing alarm that if a similar "minor" breach hit **hospitals or essential utilities**, the results would be devastating.

Surging Executive Anxiety:

- **65% of large companies** now rank supply chain vulnerability as their #1 challenge, up significantly from **54% in 2025**.



Cybersecurity Trends: The 2026 Risk Landscape

The Supply Chain Transparency Crisis

Top Supply Chain Risks (2026)

TABLE 6 **Ranking of top supply chain cyber risk**

Rank	What do you see as the main supply chain cyber risk for your organization?
1	**Inheritance risk:** Unable to assure integrity of third-party software, hardware and services
2	**Visibility:** Lack of visibility into extended supply chain
3	**Concentration risk:** Too great dependence on critical third-party suppliers
4	**Procurement risk:** Unable to apply security controls to third-party suppliers
5	**External factors:** Uncertainty of impact of external factors

Inheritance Risk:

- The **#1 global risk**; the inability to verify the integrity of third-party software, hardware, and services.

Visibility Gaps:

- The **#2 risk** overall; it is the primary concern for the **Energy, Finance, and Manufacturing** sectors.

The "Weakest Link":

- Small suppliers represent the highest vulnerability due to lower security maturity and fewer resources.

Control Deficit:

- Organizations struggle with a lack of direct authority over the security practices of their external partners.

Cybersecurity Trends: The 2026 Risk Landscape

WORLD ECONOMIC FORUM

The Supply Chain Transparency Crisis

TABLE 7 **Top supply chain risk, by industry**

Industry	Top supply chain risk	Second supply chain risk
Energy	**Visibility:** Lack of visibility into extended supply chain	**Inheritance risk:** Unable to assure integrity of third-party software, hardware and services
Financial services	**Visibility:** Lack of visibility into extended supply chain	**Concentration risk:** Too great dependence on critical third-party suppliers
Health and consumer	**Inheritance risk:** Unable to assure integrity of third-party software, hardware and services	**Visibility:** Lack of visibility into extended supply chain
ICT and media	**Inheritance risk:** Unable to assure integrity of third-party software, hardware and services	**Visibility:** Lack of visibility into extended supply chain
Manufacturing, supply chain and transportation	**Visibility:** Lack of visibility into extended supply chain	**Concentration risk:** Too great dependence on critical third-party suppliers
Materials and infrastructure	**Visibility:** Lack of visibility into extended supply chain	**Concentration risk:** Too great dependence on critical third-party suppliers
Professional services and institutional	**Inheritance risk:** Unable to assure integrity of third-party software, hardware and services	**Visibility:** Lack of visibility into extended supply chain

Cybersecurity Trends: The 2026 Risk Landscape

The Supply Chain Transparency Crisis

1. Security Maturity Assessments (66%):

- The most common action is evaluating the security posture of suppliers.

2. Procurement Integration (65%):

- Nearly two-thirds of organizations involve their security function during the initial procurement process.

3. Threat Information Sharing (38%):

- A minority of organizations actively share threat intelligence with their broader ecosystem of partners and customers.

4. Ecosystem Mapping (33%):

- Only one-third of organizations have detailed maps of their ecosystem to identify specific cyberthreat exposures.

5. Strategy Alignment (33%):

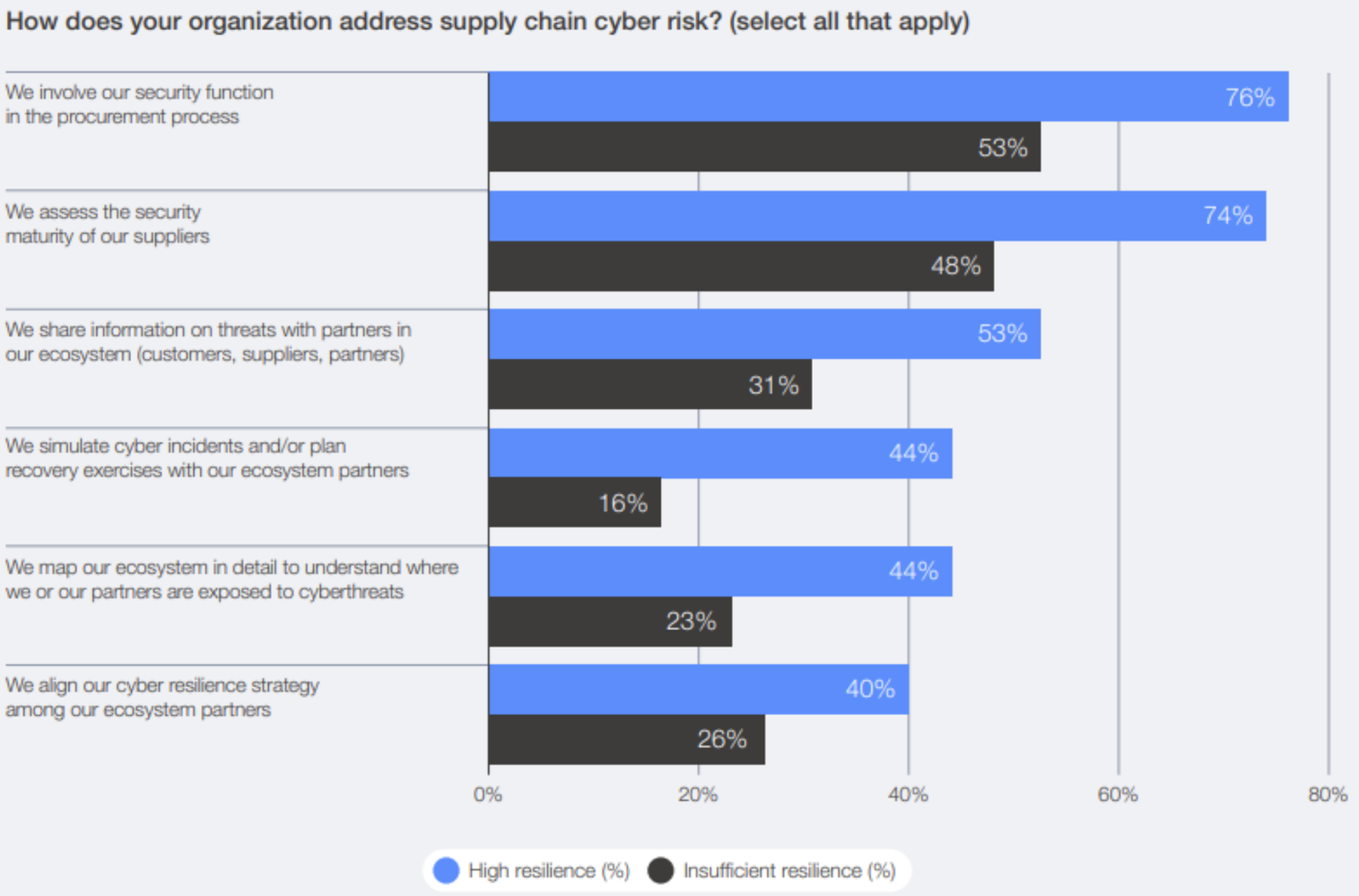
- Tying with mapping, only 33% of respondents align their cyber resilience strategies across their partners.

6. Joint Incident Simulations (27%):

- The least common strategy is running active recovery exercises or cyber simulations with ecosystem partners.

Cybersecurity Trends: The 2026 Risk Landscape

The Supply Chain Transparency Crisis



The Widening Cyber Inequity

Cybersecurity Trends: The 2026 Risk Landscape

The Widening Cyber Inequity

The Three Dimensions of Cyber Inequity

Organizational Size:

- Small organizations are **twice as likely** to suffer from insufficient resilience compared to large enterprises.

Regional Divide:

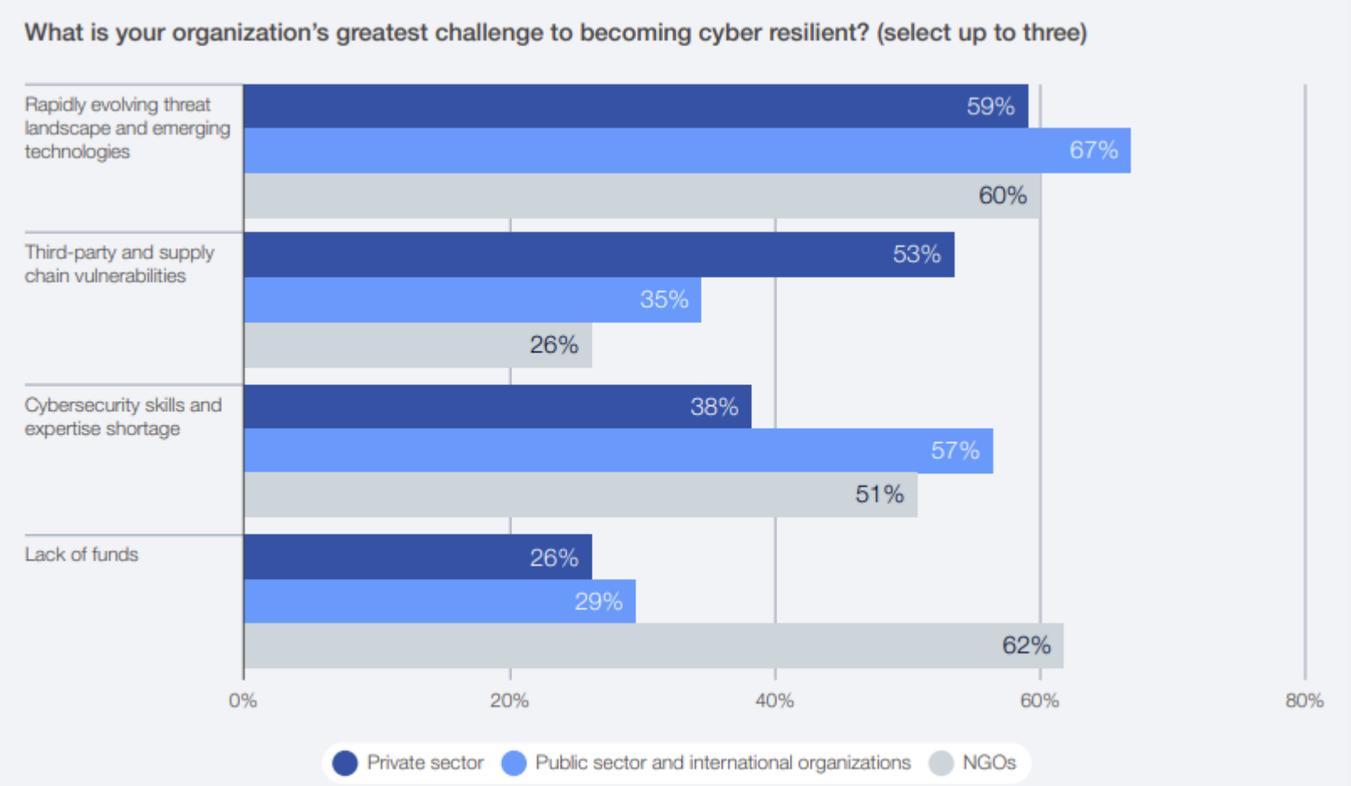
- Confidence in resilience is highest in **MENA**, but remains critically low across **Latin America, the Caribbean, and Sub-Saharan Africa**.

Sector Gap: Resilience varies wildly by industry:

- **NGOs:** 37% report insufficient resilience.
- **Public Sector:** 23% report insufficient resilience.
- **Private Sector:** Only 11% report insufficient resilience.

Cybersecurity Trends: The 2026 Risk Landscape

The Widening Cyber Inequity



The Skills Shortage (The Main Driver)
The lack of cybersecurity expertise is ranked as the **second-most significant challenge** globally, trailing only the threat landscape itself.

Public/NGO Vulnerability:

- The skills gap hits **Public Sector (57%)** and **NGOs (51%)** the hardest.

Talent Drain in Small Firms:

- 46% of small organizations lack necessary expertise, compared to 29% of large organizations.

Systemic Risk:

- This imbalance creates weak links in global supply chains, where the failure of one "insufficient" entity can compromise the entire network.

Cybersecurity Trends: The 2026 Risk Landscape

The Widening Cyber Inequity

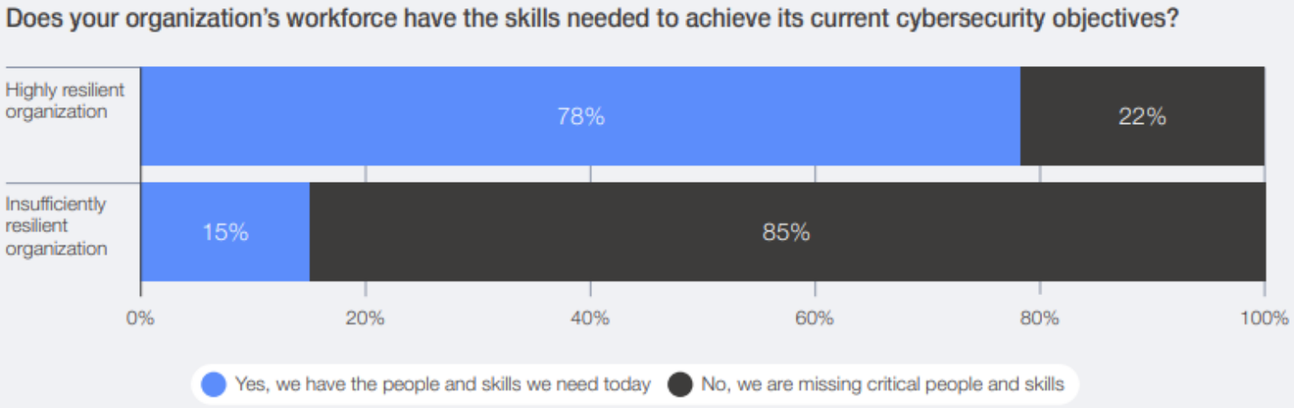
The Resilience Gap

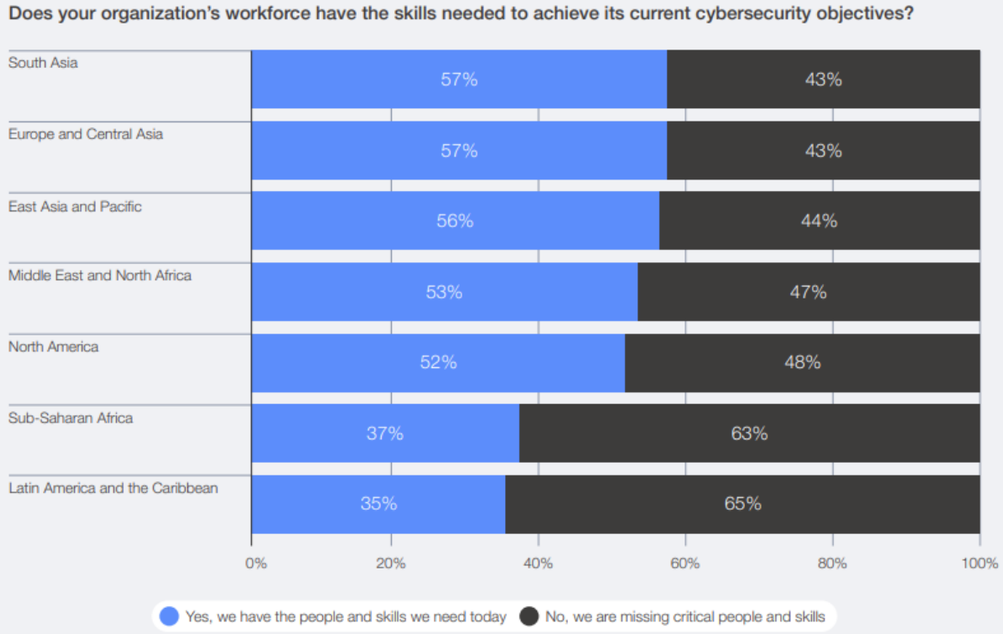
The Talent Barrier:

- **85%** of organizations with "insufficient resilience" struggle with missing critical skills and personnel.

The Competitive Edge:

- Only **22%** of highly resilient organizations report significant skills gaps, showing that talent acquisition is a primary driver of success.





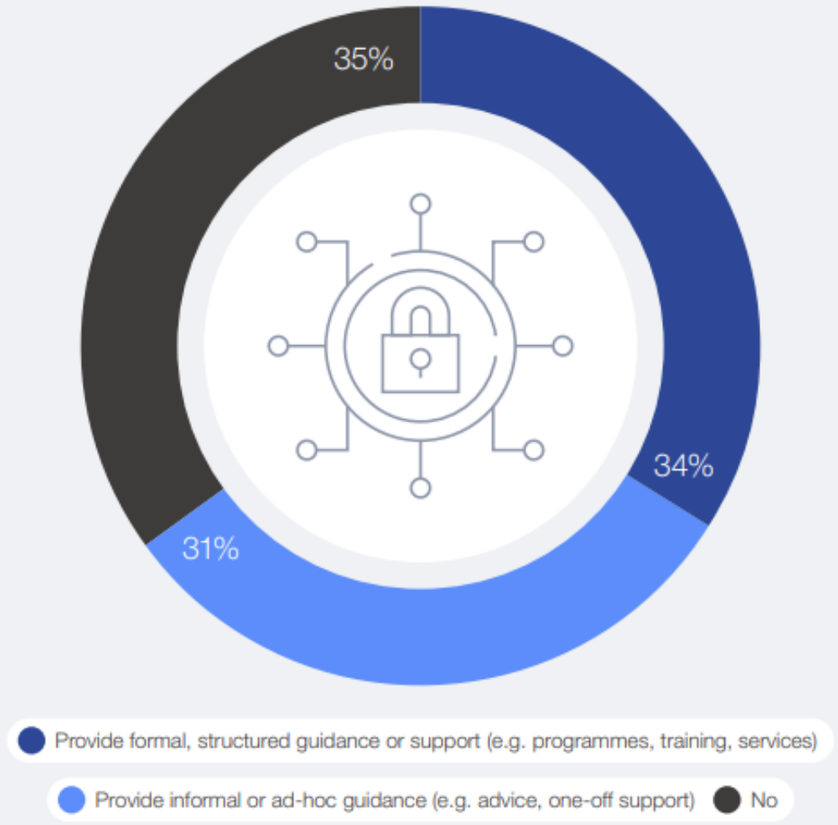
- **Most Acute Shortages:**
  - **Latin America and the Caribbean: 65%** of organizations lack the critical staff and skills needed to meet security goals.
  - **Sub-Saharan Africa: 63%** of organizations report similar critical shortages.

- **The "Global" Impact:** These regions represent the highest levels of talent scarcity, making them the most vulnerable links in the global digital ecosystem.

Cybersecurity Trends: The 2026 Risk Landscape

The Widening Cyber Inequity

Does your organization currently provide cybersecurity guidance or support to smaller or less resourced organizations?

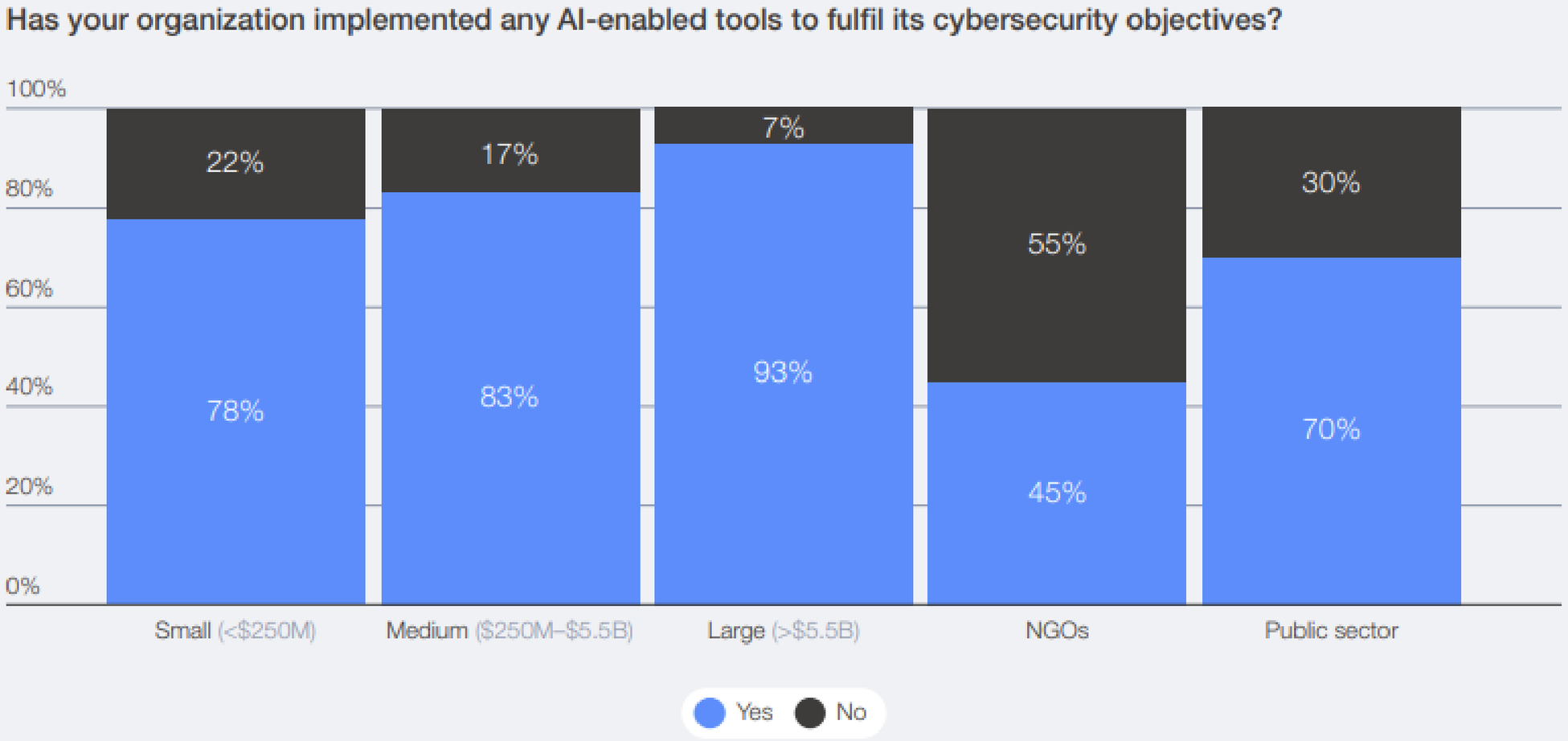


Bridging the Cyber Inequity Gap

- **Public-Interest Actors:** Groups like **CyberPeace Builders** provide mission-driven support (e.g., skilled volunteers) to help NGOs maintain vital services.
- **Accessible Expertise:** Demonstrated success shows that providing tailored guidance to resource-constrained groups meaningfully improves their resilience.
- **The "Sustainable Ecosystem":** Scalable resilience requires a coordinated network of researchers, trainers, incident responders, and volunteer communities.
- **Sustainable Funding:** A new **coordinated funding mechanism** (via initiatives like **Common Good Cyber**) moves away from fragmented support to ensure long-term stability for public-interest services.
- **Global Equity:** The ultimate goal is to make cyber resilience a **public utility** accessible to all, not just those with high financial resources.

Cybersecurity Trends: The 2026 Risk Landscape

The Widening Cyber Inequity




The Rise of "Silent" Threats

Cybersecurity Trends: The 2026 Risk Landscape

The Rise of "Silent" Threats

Autonomous Systems & Robotics: As AI shifts from analysis to physical action in logistics and healthcare, machine-executed decisions will compress detection windows and create new physical safety risks.

Digital Currencies: Rapidly becoming foundational infrastructure; a breach in settlement networks could trigger systemic liquidity shocks or erode confidence in national assets.

Space & Undersea Infrastructure: Despite carrying 99% of global data, these "unseen lifelines" remain critically overlooked in most organizational risk planning.

Climate Change: Extreme weather acts as a risk amplifier, disrupting physical power/data networks while creating new attack surfaces through decentralized renewable energy sensors.

Quantum Computing: Transitioning from a theoretical threat to a material risk to legacy encryption; 37% of leaders expect impacts to begin as early as 2026.