pwc

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

2026 Global Digital Trust Insights: C-suite playbook and findings – India edition

Foreword

Siddharth Vishwanath
Partner and Leader, Risk Consulting
PwC India

Today, business leaders find themselves at a crossroads in India's digital transformation story, where ambition must be met by balancing risk. In a time marked by constant change and growing uncertainty, the need for digital trust is more important than ever. The India edition of our 2026 Global Digital Trust Insights survey report goes beyond providing an outlook of the current cybersecurity landscape for Indian enterprises. It highlights the need for a new playbook for resilience which requires leaders to challenge traditional cyber strategies.

Geopolitical concerns, technological advancements, and regulatory changes are impacting businesses and redefining trust in the digital age. Cybersecurity has now evolved from a necessary defence to a strategic driver of growth and fulfilment of national goals. India is not far behind in this race, and our aspirations are evident from bold and transformative initiatives such as 'Viksit Bharat 2047' and 'Make in India'. However, as we rally towards a future driven by technological advancements, we face an unsettling truth: Our digital goals are moving faster than our preparedness.

This year's survey saw 3,887 business and tech executives across 72 countries—including 138 from India—share their views on critical areas such as threat outlook and emerging risks, cyber investments and priorities, the impact of emerging technologies such as AI and quantum computing, and cyber leadership strategies.

Our findings reveal an interesting paradox: While Indian organisations are investing significantly in cybersecurity—with 72% of leaders prioritising cyber risk in their strategic plans—only a small fraction are fully equipped to handle the emerging threats. This gap isn't a sign of weakness but a call for strong leadership. It reminds us that resilience comes from tackling risks head-on, not avoiding them.

Nearly 60% of Indian organisations say they are spending more on proactive cybersecurity measures, and 47% are looking to prioritise agentic AI as one of the top AI security capabilities over the next 12 months. The emergence of AI and quantum computing is changing how we engage with threats. These technologies are here to revolutionise how we defend, detect, and respond to threats. But they also demand new skills. The ongoing shortage of cyber talent, complexity of third-party risks, and changing landscape of the digital age urge us to rethink how we lead, govern, and innovate.

While Indian businesses are making progress, significant challenges remain. For one, quantum threat readiness is lagging. Though quantum computing is one of the top three threats, 40% of organisations in India have not yet considered or not started implementing quantum-resistant security measures. Further, only 5% are prioritising these measures in their budgets. Third-party breaches are another top unaddressed risk, with 18% of India's business leaders ranking them as the threat they are least prepared to handle due to limited visibility into vendor practices and fragmented governance.

This report is both a reflection and a manifesto. It highlights the progress we have made. While cybersecurity has been elevated to the boardroom by investing in proactive measures and embracing managed services to bridge critical gaps, we need to think bigger, act faster, and lead with greater conviction. The future will be shaped not by those who wait for certainty, but by those who are ready to make bold decisions amid uncertainty. For leaders of tomorrow who are shaping India's digital future, incremental changes will no longer be enough. We need to embed cybersecurity into an organisation's core. We must view risk as a chance for innovation and growth, not as an obstacle.

The decisions we make now will have a lasting impact beyond our boardrooms and data centres; they will define the legacy we leave for future generations. Together, we can ensure that our digital future is not only ambitious, but also secure, resilient, and trustworthy.

Table of contents

01

Risk and threat landscape

Geopolitics is reshaping cyber vulnerabilities

72%

of Indian organisations are increasing cyber risk investment in response to geopolitical volatility

42%

are reassessing their cyber insurance policies

Top 2

cyberthreats organisations are least prepared to address: third-party risks and quantum computing

A rapidly shifting world order marked by strained alliances, trade disputes, and weakened international institutions is redefining the cyberthreat landscape and challenging traditional models of global business. In this new era of strategic competition, organisations are proactively re-evaluating their cyber capabilities, operational footprints, and global partnerships to build resilience and seize emerging opportunities.

In response to this geopolitical volatility, 72% of Indian business and technology leaders have made cyber risk investment one of their top three strategic priorities for the year ahead, significantly higher than global leaders (60%). This elevated focus reflects a heightened awareness in India of cybersecurity's role as a strategic enabler of resilience and business continuity.

Organisations in India are also proactively adjusting their operational strategies:

49%

are re-evaluating the **location of critical infrastructure**

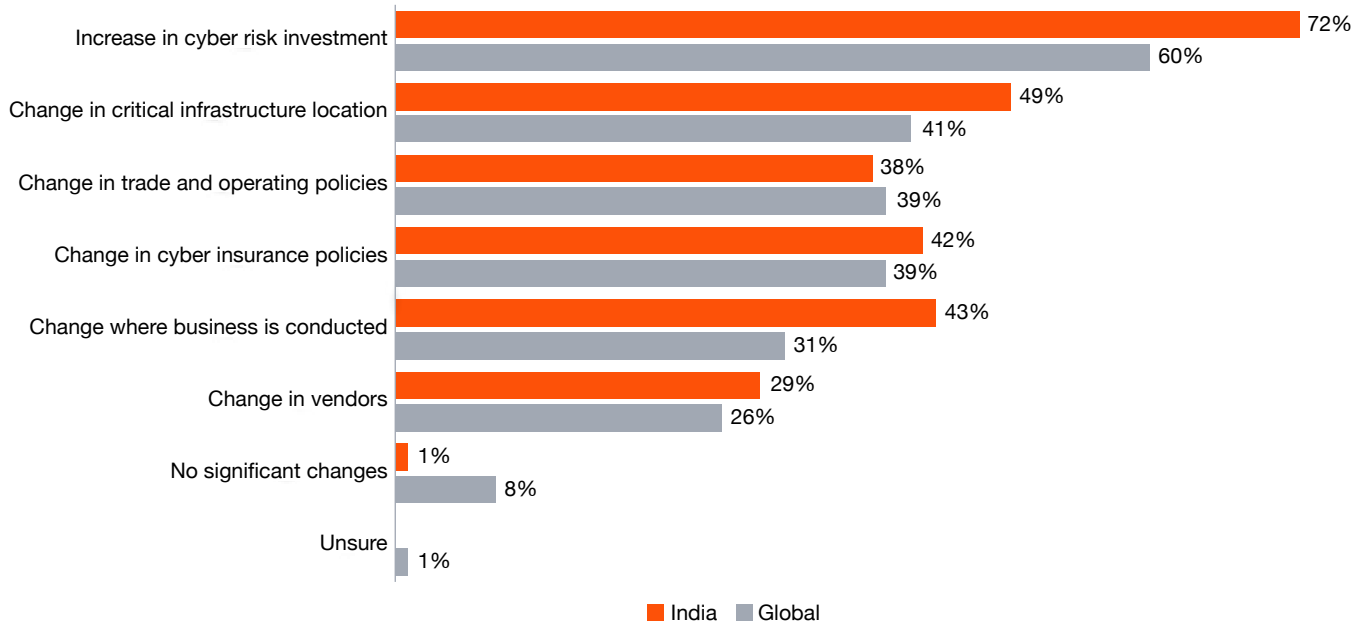
43%

are considering **changes in where business is conducted**

42%

are reassessing their **cyber insurance policies**

Cyber strategy changes in response to current geopolitical landscape



Q. 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?

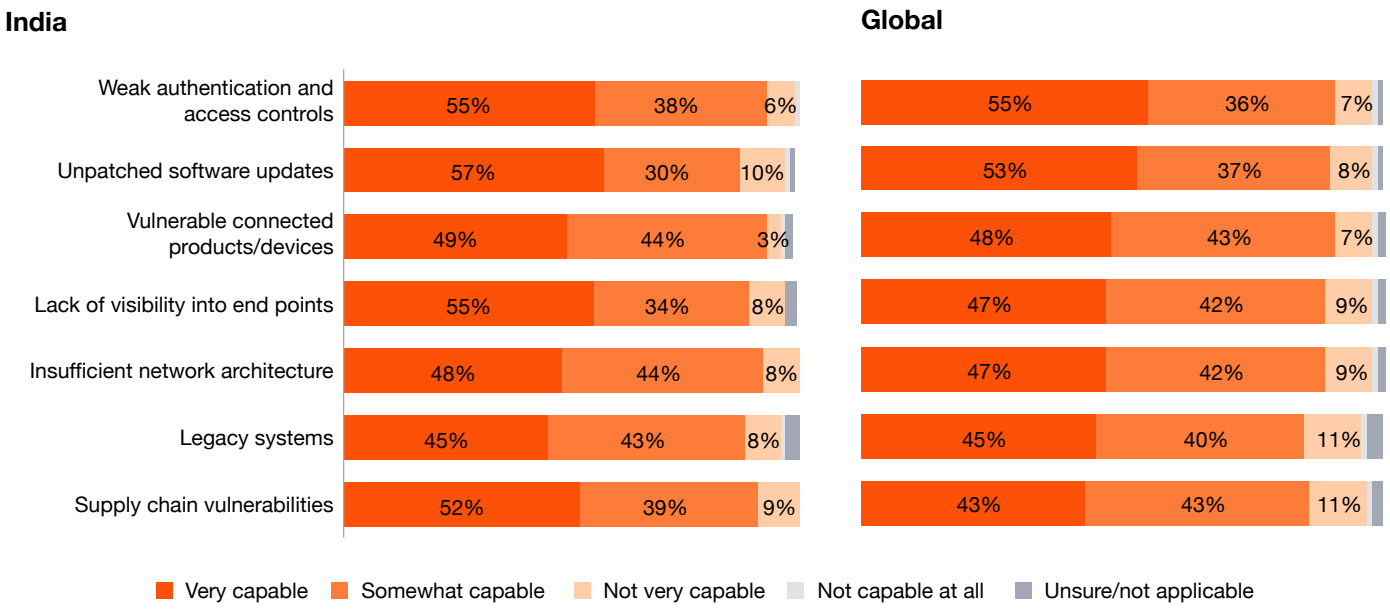
Base: All India respondents=138

Source: PwC 2026 Global Digital Trust Insights

Feeling secure vs being secure

Indian organisations are approaching cyber resilience with caution. While many acknowledge progress in specific areas, a significant number still express limited confidence in their ability to withstand major cyberattacks across critical vulnerabilities. Key areas of concern include **legacy systems, supply-chain dependencies, insufficient network architecture, and lack of visibility into endpoints**, all of which remain frequent targets for sophisticated threat actors. This fragmented readiness reflects the complexity of India's digital transformation journey, where rapid adoption of new technologies often outpaces the maturity of underlying security frameworks.

Level of capability to withstand a major cyberattack



Q. Given the current geopolitical landscape, how capable is your organisation to withstand a major cyberattack targeting the following vulnerabilities?

Base: India security leaders, COOs and operations directors=89

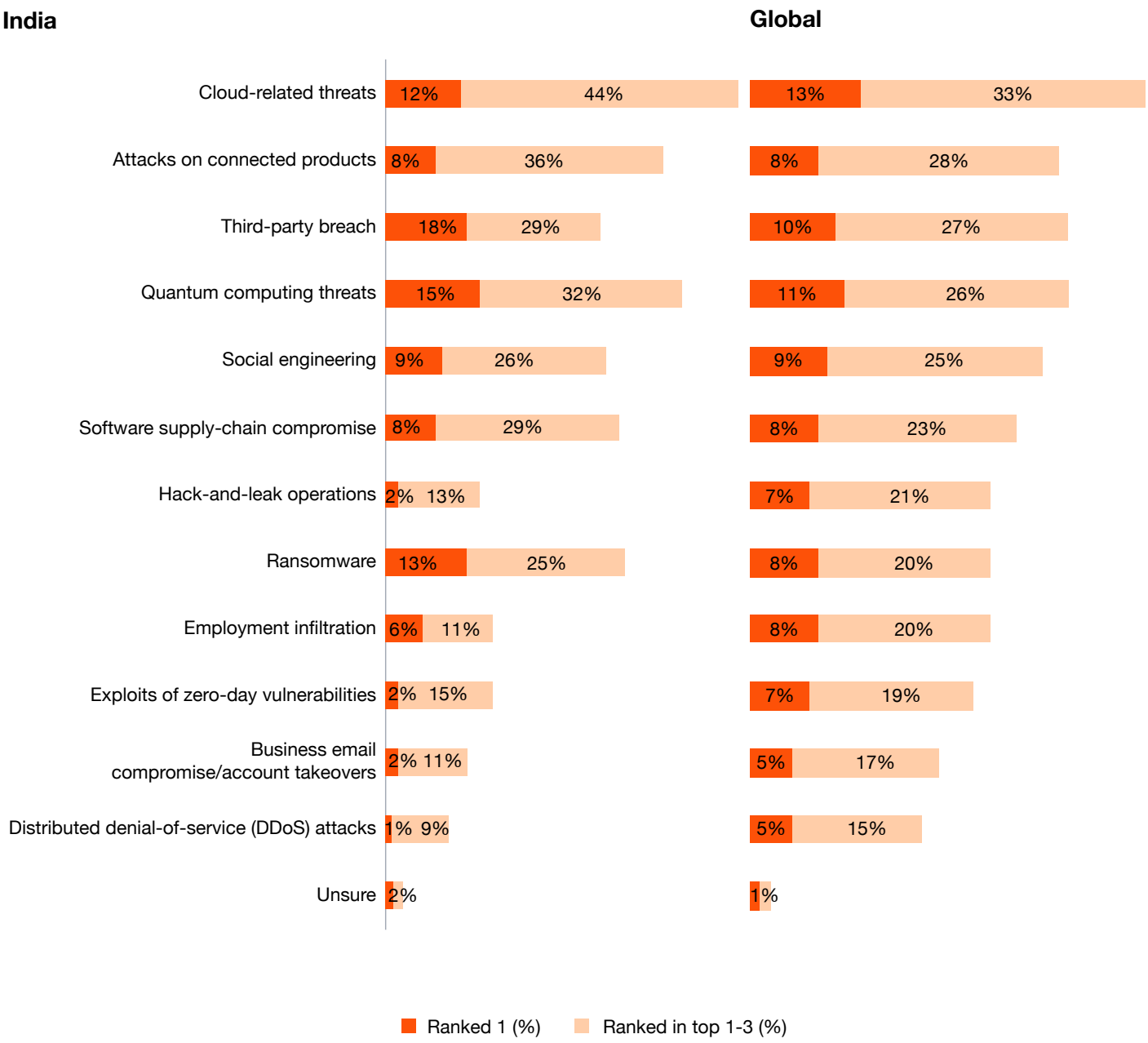
Source: PwC 2026 Global Digital Trust Insights

Persistent risks and emerging threats

Indian organisations have identified **third-party breaches (18%)** as the top threat they are least prepared to address. As digital ecosystems expand, limited visibility into vendor security practices and fragmented governance are exposing businesses to significant risk. Also high on the threat radar are **quantum computing threats (15%)** and **ransomware (13%)**, both reflecting growing concerns over emerging technologies and evolving attack methods. While quantum threats are still nascent, the lack of preparedness signals a need for early action. Ransomware continues to challenge organisations due to its disruptive impact and recovery complexities.

In the past year, **cloud** and **connected products** threats were among the top concerns for Indian organisations, and they continue to be prominent this year. While not the highest-ranked individually this year, both remain consistently cited as areas of low preparedness. Their sustained presence on the threat radar highlights ongoing challenges in securing rapidly expanding digital environments. As Indian enterprises scale cloud adoption and deploy more connected products, such as smart and IoT-enabled devices, the need to close foundational gaps in governance, visibility, and control has become increasingly urgent.

Cybersecurity threats organisations are least prepared to address



Q. Over the next 12 months, which of these cyberthreats is your organisation least prepared to address?

Base: India security leaders=85

Source: PwC 2026 Global Digital Trust Insights

Learning the hard way

Recent data underscores the financial and operational impact of cyber incidents. Nearly **25% of executives** from Indian organisations report that their most severe breach in the past three years resulted in losses exceeding **$1 million**, with exposure highest among enterprises generating **$5 billion or more in revenue (45%).**

Given the challenges of recovery, organisations that have experienced a major attack are turning costly lessons learned into action. These companies are:

- **Increasing cyber budgets (87%)** to strengthen defences and accelerate capability development
- **Leveraging managed services (42%)** to address critical skill gaps and enhance operational resilience
- **Revising cyber insurance policies (42%)** in line with rising premiums and evolving insurer requirements
- **Embedding data minimisation practices (34%)** across processes to reduce risk and improve compliance

These losses are driving a shift from reactive recovery to proactive resilience, positioning these organisations to better withstand future threats and regulatory scrutiny.

Call to action

In an era of geopolitical volatility, cybersecurity has evolved from a defence necessity to a strategic enabler of resilience and growth. This heightened focus reflects a recognition that robust cyber capabilities underpin business continuity and trust in uncertain times.

- **Elevate cyber risk to a board-level priority:** Align cybersecurity investments with risk exposure.
- **Reinforce third-party risk governance:** Strengthen vendor oversight and supply-chain security to address the top threats Indian organisations feel least prepared for.
- **Act early on quantum resilience:** Begin scenario planning and capability development for quantum threats before they mature into mainstream risks.
- **Modernise cyber insurance strategies:** Reassess coverage considering evolving threat vectors, rising premiums, and insurer expectations.
- **Strengthen foundational controls:** Set up controls around endpoints for better security and visibility through reinforced governance to address persistent vulnerabilities and emerging threats.

02

Cyber strategy and operations

Where investment meets impact

Only 30%

are spending significantly more on proactive vs reactive cybersecurity measures

87%

expect their cyber budget to increase over the coming year

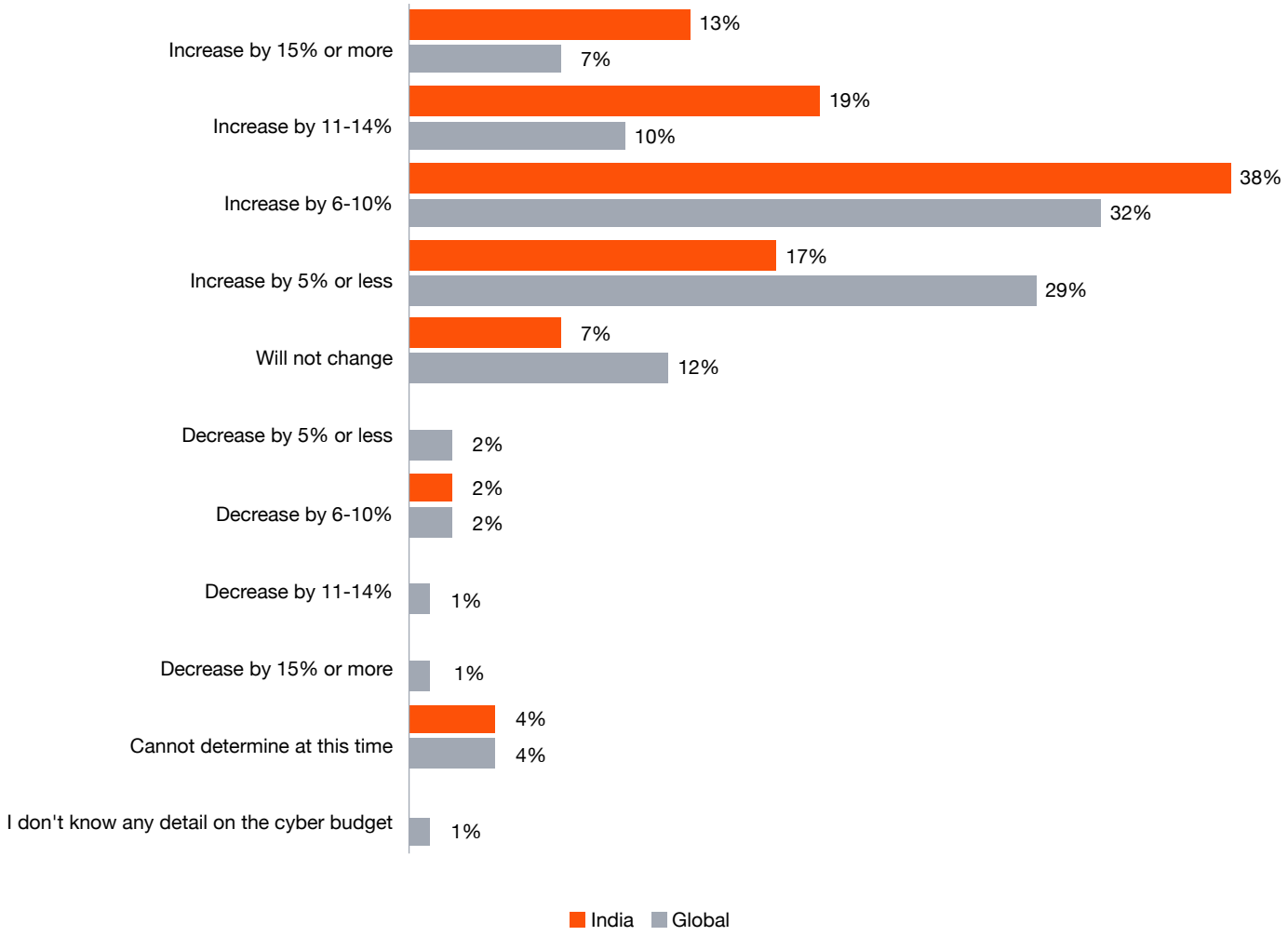
Only 31%

are measuring the financial impact of cyber risks to a large extent

Cyber budgets: Still rising, but with sharper focus

Cyber budgets are still rising, though at a more deliberate pace. This year, **87%** of leaders of Indian organisations expect their cyber budgets to grow in the coming year and nearly one-third of them plan to boost spending by more than **10%**—a slight dip from last year's 93%, yet a strong signal of sustained investment. This moderation may reflect a strategic rebalancing, as organisations respond to geopolitical volatility while reassessing how cyber risk fits within broader business priorities.

Changes in cyber budgets in 2026



Q. How will your organisation's cyber budget change in 2026?

Base: India security leaders, CFOs and finance directors=95

Source: PwC 2026 Global Digital Trust Insights

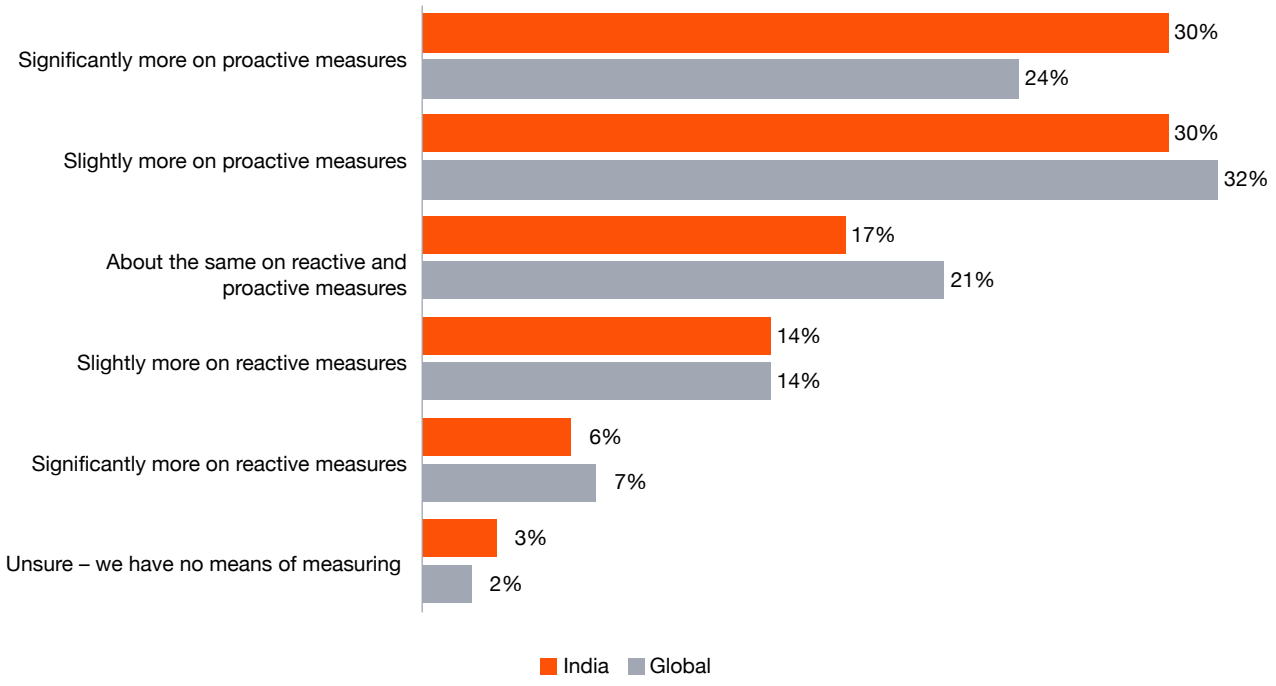
The cost of preparing vs reacting

Cybersecurity is about readiness. It means planning ahead and investing in proactive measures such as monitoring, assessments, testing, controls and training—before a crisis happens. Yet only **30%** of organisations are prioritising proactive spending over reactive measures such as response, customer care, remediation, recovery, litigation, and fines, which are more costly and risky.

Nearly **60%** of organisations in India spend more on proactive cyber measures as compared to **56%** of organisations globally. What's more, those numbers likely underestimate the true cost of reacting. While proactive spending sits in the security leader's budget and is easy to track, reactive costs are dispersed across the business—legal, communications, operations, IT, product, marketing, government relations—and include harder-to-quantify costs such as lost opportunities and reputational damage.

For that matter, spending on proactive measures won't help if the focus is on the wrong risks or the measures aren't nimble enough to adapt to new conditions. True readiness requires a deep understanding of the risk and threat landscape—one that informs the company's cyber strategy, the people it hires and the processes, systems, and tools it adopts.

Spending on reactive vs proactive measures



Q. Is your organisation spending more resources on reactive or proactive cybersecurity measures?

Base: All India respondents=138

Source: PwC 2026 Global Digital Trust Insights

Mapping investment priorities to preparedness

Cyber leaders are sharpening their focus, and budgets are beginning to reflect that shift. **AI and cloud security**—areas where organisations feel least prepared—remain top investment priorities. But the investment picture is far from complete. The threat landscape is broadening, and not all risks are receiving proportional attention. While connected products remain among the top areas of low preparedness, budget allocation continues to be modest, signalling a persistent gap between awareness and action.

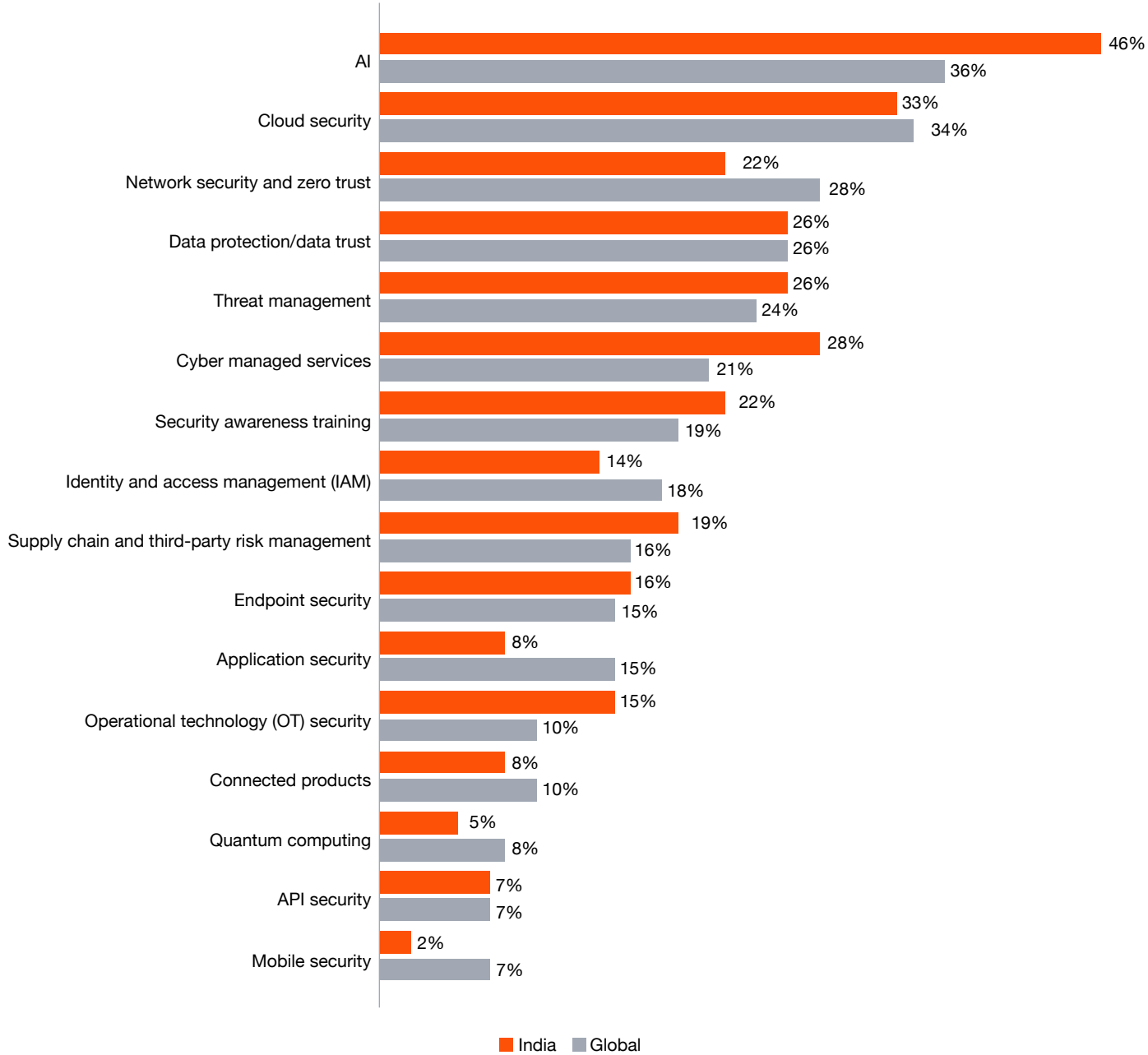
What's more, while quantum computing risks represent emerging and complex threats, third-party breaches remain a persistent and systemic challenge. Yet both rank among the top areas of low preparedness, underscoring the urgency for a more dynamic investment strategy.

Looking ahead, zero trust architecture continues to be a major driver of cybersecurity investments, as Indian organisations look to engineer and re-architect systems to make security frictionless for business operations.

In parallel, data trust has emerged as a critical priority for Indian organisations, influenced by the Digital Personal Data Protection (DPDP) Act. This regulatory development is accelerating investments in data governance, protection and privacy controls, and compliance frameworks, signalling that future cyber spending will increasingly focus on building trust, resilience, and regulatory alignment.

In sum, while organisations are beginning to align budgets with risk, the pace of alignment varies. To truly close the gap, cyber investments must be guided not just by current exposure but also by the evolving threat landscape and operational realities.

Investments organisations are prioritising when allocating cyber budgets (% that ranked in their top 3 priorities)



Q. Which of the following investments are you prioritising when allocating your organisation's cyber budget in the next 12 months?

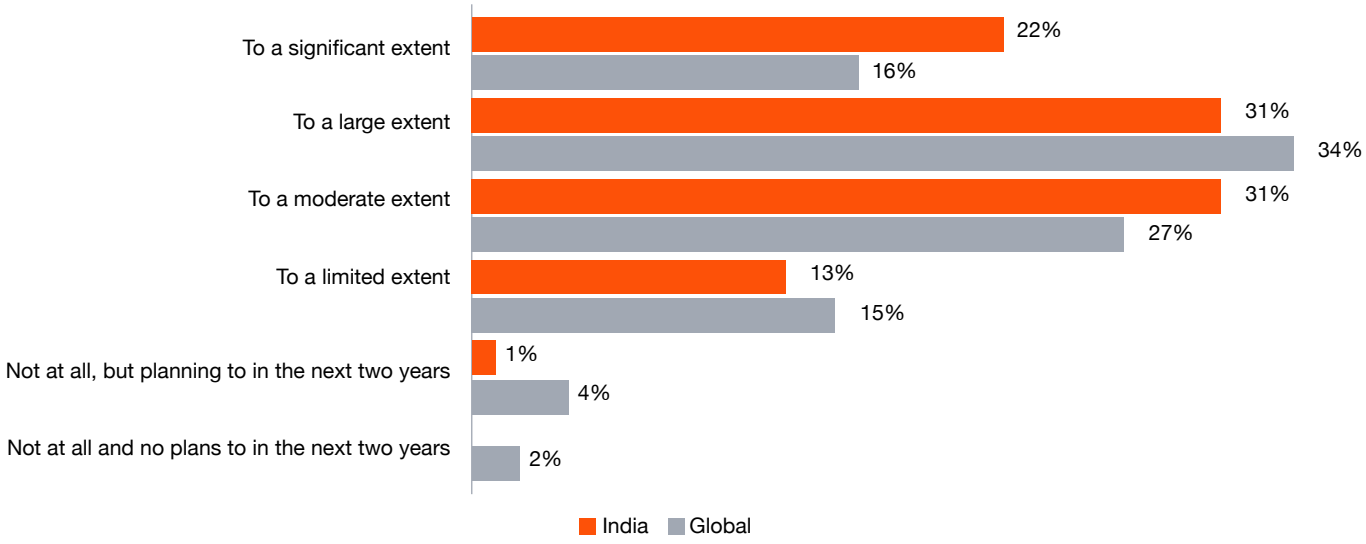
Base: India security leaders=85

Source: PwC 2026 Global Digital Trust Insights

Putting a price on cyber risk

An increasing number of organisations are applying financial metrics to assess cyber risk. Over half report using cyber risk quantification to evaluate potential financial impact to a significant or large extent, aligning closely with global benchmarks. However, a deeper analysis reveals that only 22% are doing so at a truly significant level. Business leaders need credible, actionable cyber risk reporting insights[1] to assess the threats their organisations face and judge how best to respond.

Measuring the financial impact of cyber risks



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

Base: India security leaders, CFOs, CEOs, CROs, and the board =120

Source: PwC 2026 Global Digital Trust Insights

Cyber spend must shift from volume to value

Budgets are rising, but impact depends on proactive allocation and measurable outcomes. Prioritise prevention over response, align investments to evolving risks, and embed financial quantification to turn spend into resilience and growth.

1 https://www.pwc.com/gx/en/issues/cybersecurity/cyber-risk-quantification.html

Call to action

- **Rebalance spending towards prevention:** Shift focus from reactive recovery to proactive readiness. This includes security engineering and architecture, clinical implementation of controls, and enhanced level of situational awareness through monitoring.
- **Align investment to both emerging and persistent risks:** Ensure funding addresses not only new threats such as quantum computing but also long-standing vulnerabilities such as third-party breaches and supply chain exposures.
- **Quantify cyber risk:** Use financial metrics to assess and communicate the business impact of cyberthreats.
- **Integrate cyber into business strategy with adaptive governance:** Embed cybersecurity into core decision-making, operations, and transformation initiatives while enhancing oversight and agility to respond to evolving threats, regulatory shifts, and operational realities.

03

AI in cybersecurity

From promise to priority

Top cyber investment priority for security leaders is AI

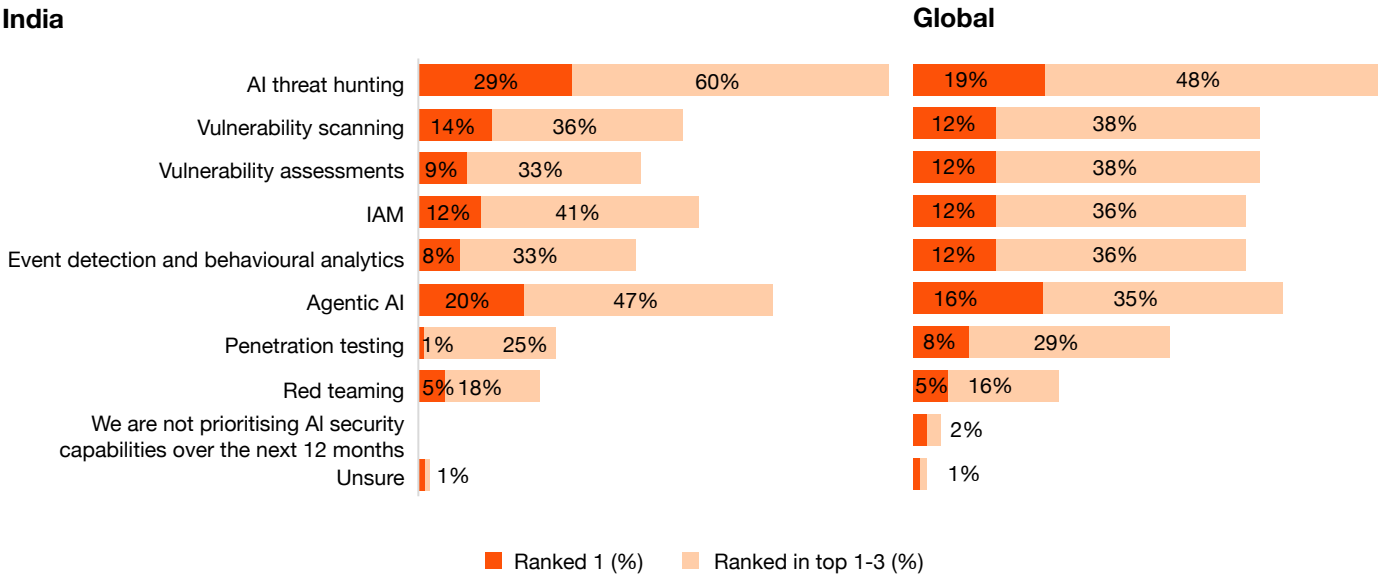
Top AI security capability prioritised by security leaders is threat hunting

Top 3 areas of priority for agentic AI are cloud security, data protection, and cyber defence

AI's potential for transforming cyber capabilities is clear and far-reaching. That's why it ranks highest in several categories we surveyed. AI enablement of key cyber capabilities is the top priority when it comes to allocating cyber budgets, leveraging managed cybersecurity services, and addressing cyber talent gaps.

AI is the top **cyber investment** area and the focal point for closing capability and talent gaps for Indian organisations. Over the next 12 months, leaders place the highest emphasis on **AI-enabled threat hunting**, alongside agentic solutions, IAM, vulnerability scanning, and assessment programmes, signalling a pivot from tooling to **intelligence-led detection and response.**

Agentic AI among the top prioritised AI security capabilities



Q: Which of the following AI security capabilities will your organisation prioritise over the next 12 months?

Base: India security leaders=85

Source: PwC 2026 Global Digital Trust Insights

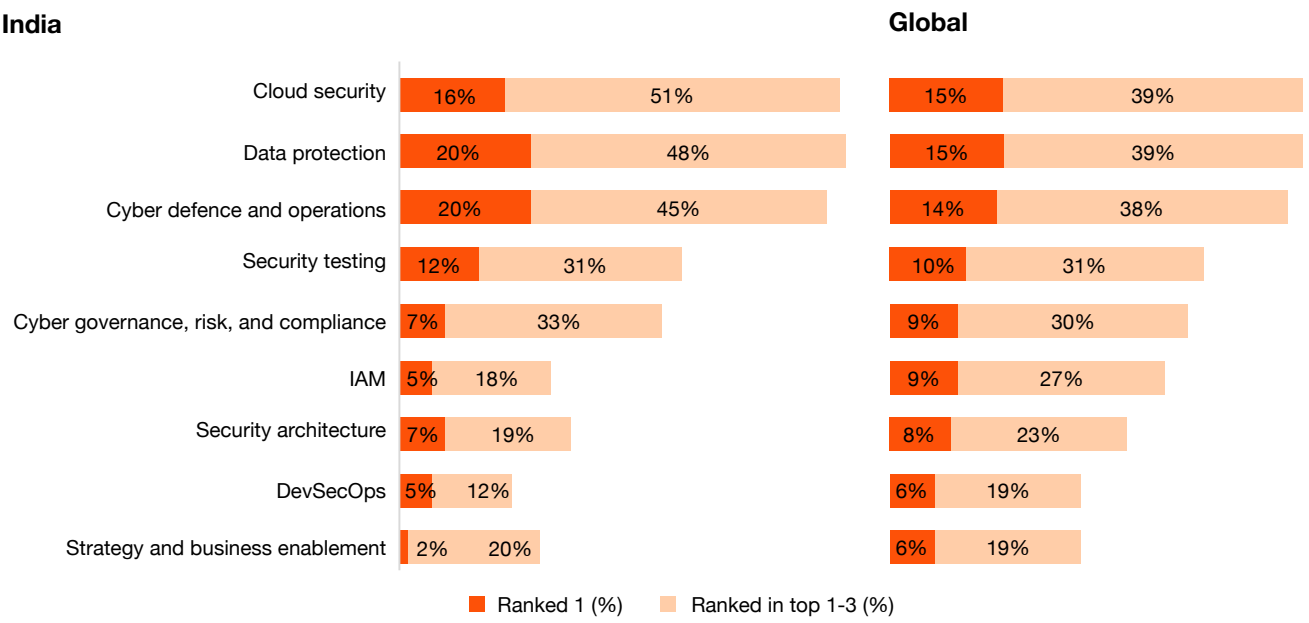
Agents of change in cyber defence

Organisations are graduating from analytical AI to agentic AI—autonomous, goal-directed systems that act with limited human intervention, collaborate with teams, and initiate security responses. That's why security leaders rank AI agents among the top AI security capabilities their organisations are prioritising over the next 12 months.

Where are they planning to deploy these agentic solutions? Cloud security, data protection, cyber defence, and operations rank as the top security priority areas for AI agents in the coming year. Security testing, cyber governance, risk and compliance (GRC), and security architecture are close behind. The near-term payoff is faster triage and reduced mean time to contain; the long-term objective is adaptive resilience at scale.

While agentic AI is gaining momentum in cloud security, data protection, and cyber defence, survey data shows hesitation around its use in DevSecOps and IAM. This scepticism likely stems from the high-stakes nature of patching and vulnerability remediation, where human oversight remains critical. Automated actions in these areas carry risks of misconfigurations or outages, prompting caution among security leaders. Skill gaps further complicate adoption, especially in environments where security tooling must integrate seamlessly with automated development workflows. In the case of IAM, agentic AI could automate access provisioning and anomaly detection. However, organisations remain wary because IAM systems were built for static identities, not autonomous agents that act and delegate dynamically. This caution is also seen in CERT-In's July 2025 guidelines[2] which amplify the need for risk-based audits which require technical evidence of access controls and real-time remediation tracking. These requirements demand transparency and operational accountability—attributes that fully autonomous IAM solutions cannot yet guarantee. This also explains why IAM adoption of agentic AI is slow: The stakes of missteps in identity governance are simply too high.

Agentic AI priorities to increase efficiency and productivity



Q. In which of the following areas will your organisation prioritise agentic AI to increase efficiency and productivity over the next 12 months?

Base: India security leaders=85

Source: PwC 2026 Global Digital Trust Insights

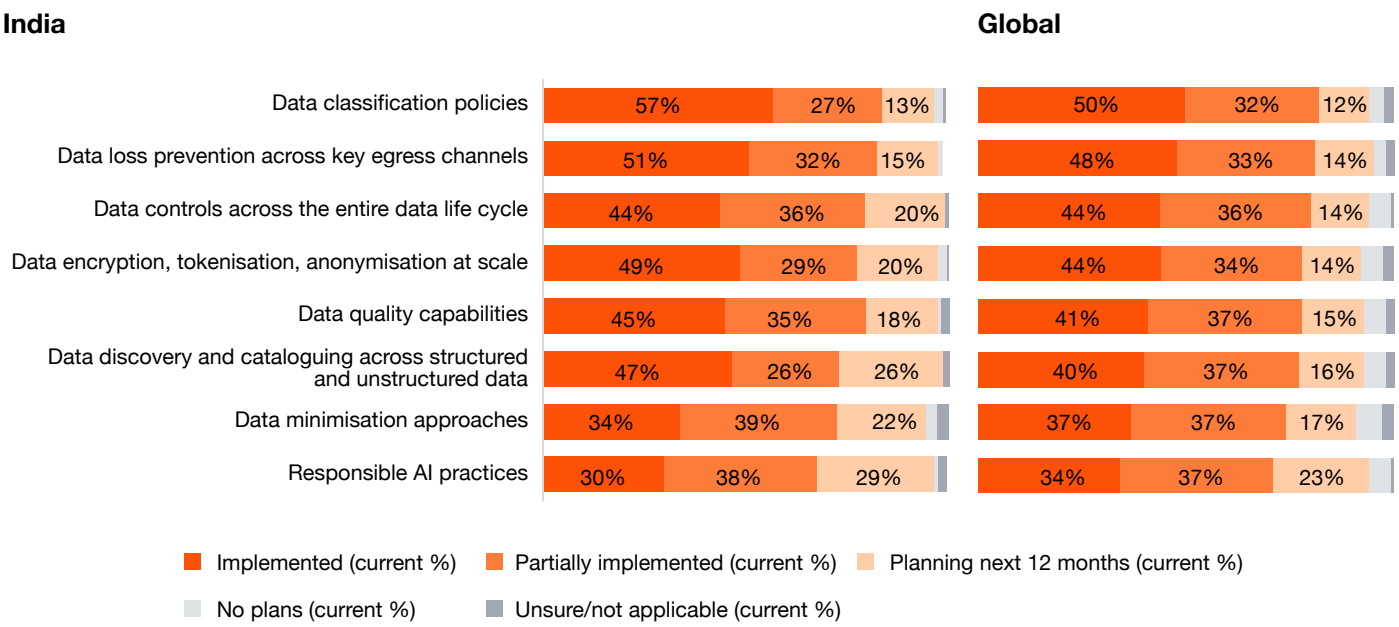
2 https://www.cert-in.org.in/PDF/Comprehensive_Cyber_Security_Audit_Policy_Guidelines.pdf

Data discipline for AI at scale

Effective AI demands curated, high-quality datasets and enterprise-wide governance. Organisations are making steady progress in implementing data risk controls, with classification and loss prevention being the most mature areas. However, advanced practices such as data minimisation and responsible AI remain underdeveloped, highlighting a gap between compliance-driven measures and forward-looking governance.

India's DPDP Act is expected to accelerate data clean-up initiatives across enterprises. By mandating explicit consent, data accuracy, and the right to erasure, the DPDP Act compels organisations to reassess and streamline their data inventories. This regulatory push not only strengthens privacy compliance but also lays the groundwork for scalable, ethical AI adoption. As businesses align with DPDP requirements, they are likely to invest more in data hygiene, minimisation, and governance frameworks, bridging the gap between foundational controls and strategic readiness for AI at scale.

Measures to address data risk



Q. To what extent has your organisation implemented or is planning to implement any of the following measures to address data risk across the enterprise?

Base: India security leaders, CFOs, finance directors, CDOs, chief counsel/GC/CLO, CROs, risk directors, CAEs, and internal audit directors=101

Source: PwC 2026 Global Digital Trust Insights

Call to action

- **Prioritise AI-driven threat detection:** Invest in AI-enabled threat hunting to shift from reactive defence to intelligence-led response.
- **Accelerate agentic AI adoption:** Deploy autonomous AI agents across the enterprise within security architecture, governance frameworks, and operational workflows to drive speed, scalability, and consistent resilience.
- **Embed responsible AI principles:** Evaluate AI deployments through the lens of fairness, transparency, and accountability to ensure ethical and compliant use across security functions.
- **Close the data governance gap:** Strengthen enterprise-wide data discipline and move beyond compliance to enable responsible AI at scale.
- **Build AI-native security talent:** Shift hiring and upskilling strategies towards professionals who are already proficient in AI tools and can apply them to security use cases. Focus on enabling technically skilled professionals to adapt AI capabilities to threat detection, response, and governance rather than retrofitting AI knowledge into traditional security roles.

04

Quantum computing readiness

Preparing for next-level threats

Top 3

threats organisations are least prepared to address now include quantum computing

40%

of organisations haven't considered or started implementing any quantum-resistant security measures

Only 5%

of security leaders include quantum readiness in their top three budget priorities

As India accelerates its digital transformation journey in 2025, the emergence of quantum computing presents both a technological frontier and a strategic challenge. National efforts to build secure digital infrastructure and reinforce technological sovereignty driven by initiatives such as the **IndiaAI Mission** and the **National Quantum Mission** are laying the foundation for next-generation cybersecurity capabilities. The IndiaAI Mission, with its focus on democratising AI access, building indigenous compute infrastructure, and promoting responsible AI development, complements quantum preparedness by enabling scalable, secure, and ethically governed digital systems. Together, these missions signal India's intent to lead in frontier technologies while safeguarding its digital future.

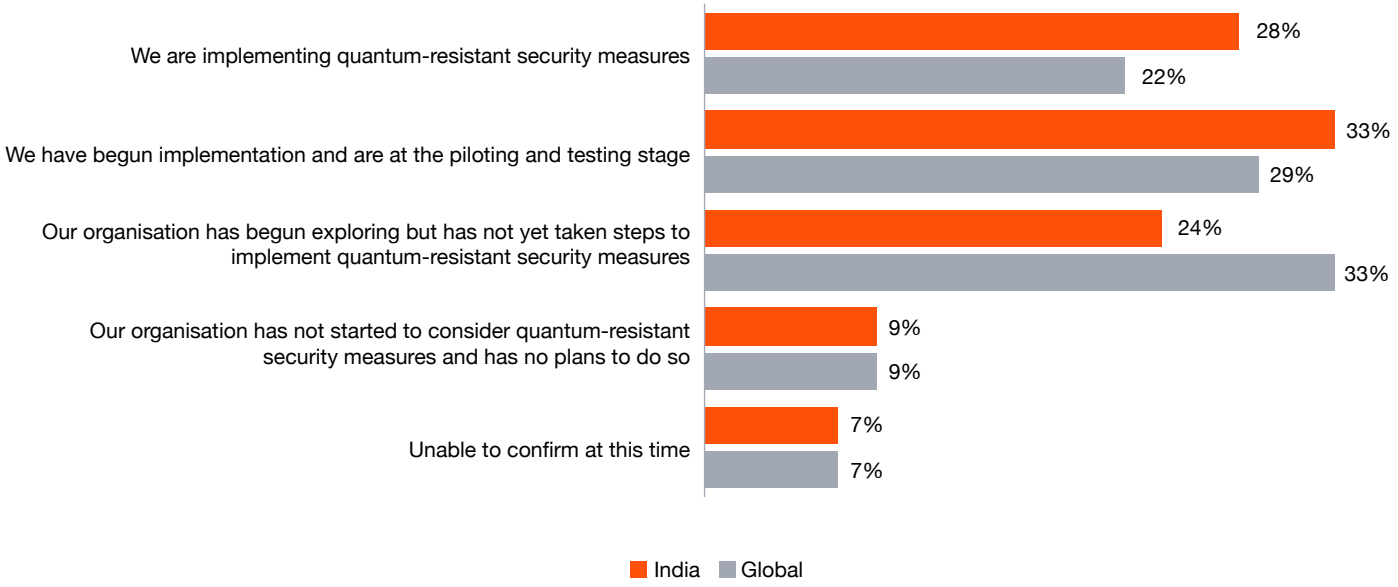
Quantum computing is no longer a distant possibility; it is a rapidly advancing reality poised to redefine the foundations of digital security. As quantum capabilities evolve, so too must the cryptographic systems that underpin global infrastructure. The transition to post-quantum cryptography (PQC) is not merely a technical upgrade; it is a strategic imperative that demands foresight, agility, and sustained commitment.

Recognising this urgency, CERT-In's white paper **'Transitioning to quantum cyber readiness'**[3] has offered a practical roadmap for organisations. It recommends starting with a comprehensive cryptographic inventory (cryptographic bill of materials [CBOM]/ quantum bill of materials [QBOM]), adopting a risk-based approach to migration, and piloting hybrid cryptography solutions. The roadmap emphasises phased rollouts, the development of crypto-agile architectures, and the use of AI-enhanced implementation and continuous monitoring. CERT-In underscores that quantum risk is immediate, not theoretical, and urges organisations to act now to safeguard India's digital future.

3 https://www.cert-in.org.in/

Some organisations in India have made initial progress, with **33%** in the piloting and testing stages. However, only **28%** have moved beyond piloting, and almost **40%** haven't considered or started implementing any quantum-resistant security measures. These gaps highlight the importance of CERT-In's guidance: Overcoming barriers such as limited awareness, resource constraints, and competing demands will require proactive, structured, and continuous action to ensure India's digital infrastructure remains resilient in the quantum era.

Quantum-resistant security progress



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

Base: All India respondents=138

Source: PwC 2026 Global Digital Trust Insights

Quantum concerns grow, but readiness lags

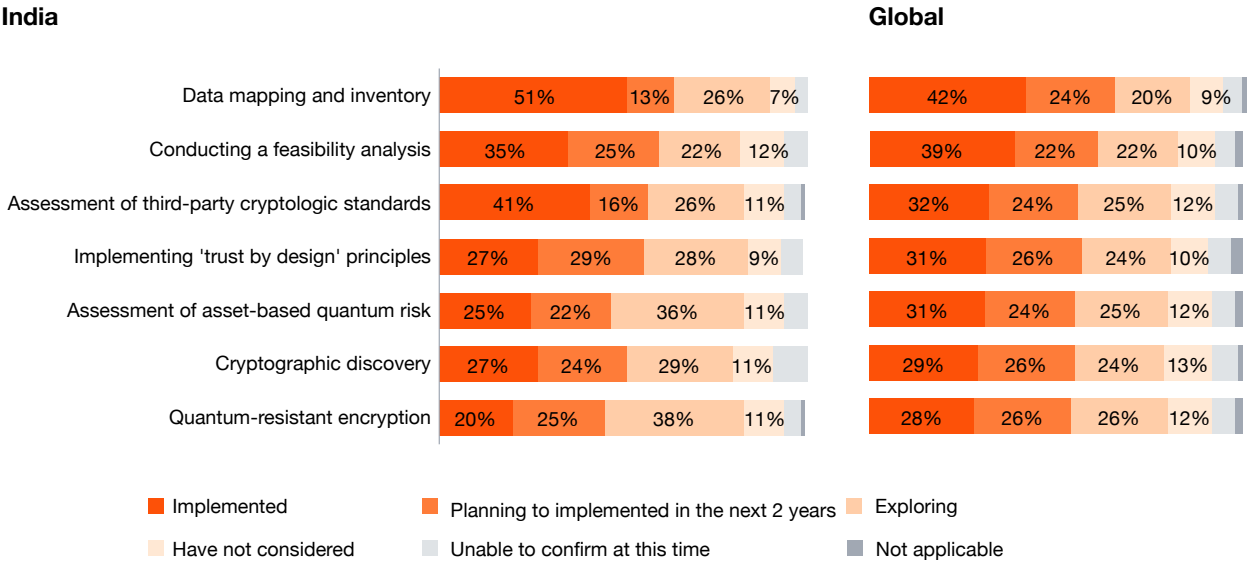
Awareness of quantum threats is growing. Quantum computing now ranks among the top three threats that organisations feel least prepared to address, up several notches from last year. But are these concerns translating into action?

Despite the growing urgency, **40%** of Indian organisations have not considered or started implementing any quantum-resistant security measures. Although these steps aren't exhaustive, they are core practices in a multi-year journey that need immediate attention. Looking ahead, only 5% of security leaders include quantum readiness in their top three budget priorities for the coming year.

Organisations with over $5 billion in revenue are more likely to have implemented these steps, including a data inventory to mitigate the 'harvest now, decrypt later' risk, feasibility analyses, assessment of third-party cryptographic standards, testing, and implementing quantum-resistant encryption. Higher-growth companies, too, are recognising the cyber challenge quantum presents and are positioning themselves accordingly.

But they remain the exception. As the technology advances, the ability to quickly adopt quantum-resistant cryptography is poised to become a defining enterprise capability.

Implementation of quantum-resistant security measures



Q. How far along is your organisation when it comes to the following quantum-resistant security measures?

Base: India security leaders=85

Source: PwC 2026 Global Digital Trust Insights

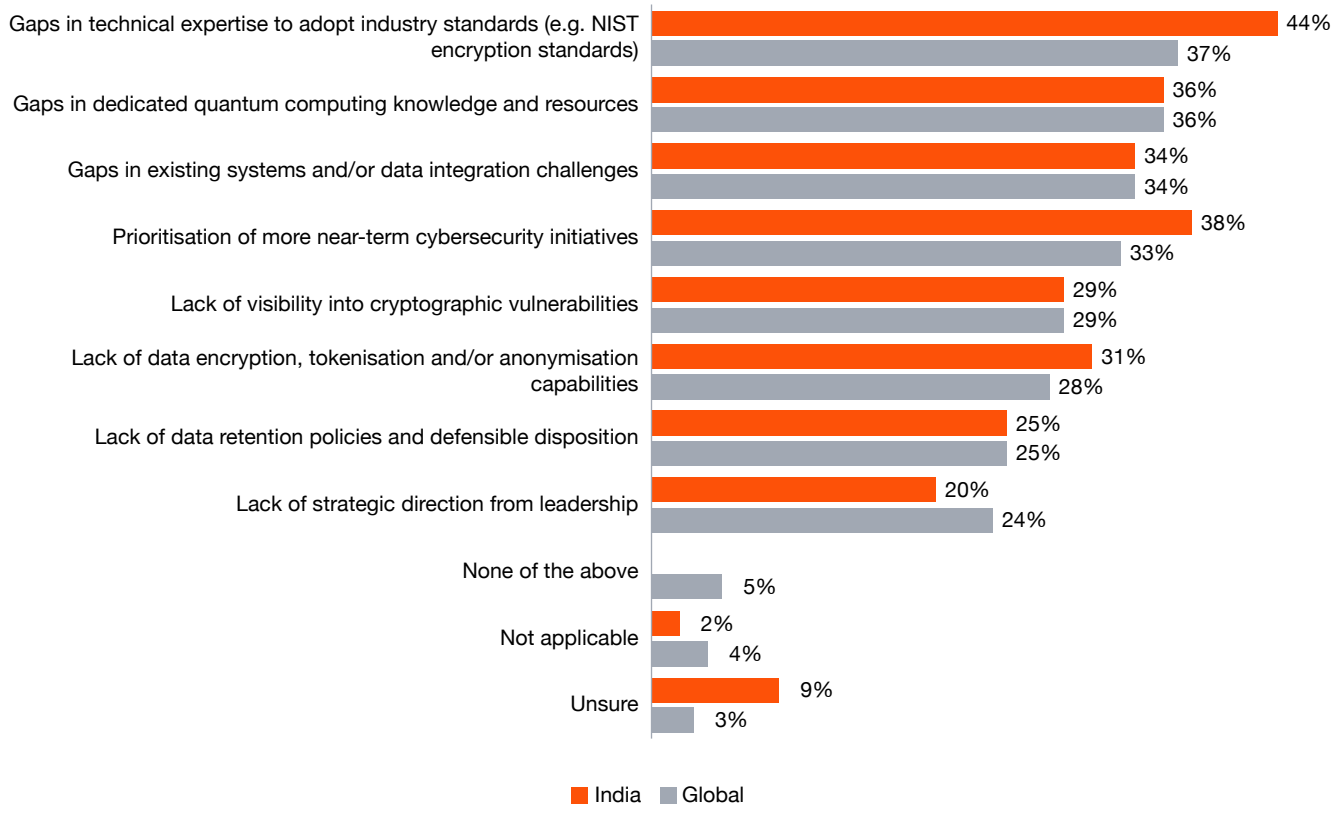
Why post-quantum cryptography is hard

Quantum readiness isn't just a technical upgrade; it's a foundational and strategic shift to future-ready security practices. The top internal barriers? Gaps in technical expertise, limited institutional knowledge, and the prioritisation of more immediate cybersecurity concerns over long-term quantum resilience.

As organisations establish cryptographic inventories to start transitioning to quantum-resistant cryptography, they should identify vulnerable algorithms across their technology stack. While it's widely understood that public key encryption is vulnerable given 'harvest now, decrypt later', security leaders should be aware of technologies they're relying on for authentication and digital signatures using equally vulnerable cryptographic algorithms.

These hurdles make one thing clear: Even when prioritised, starting a cryptographic inventory and implementing quantum-resistant cryptography takes time. And time is in short supply. Leading industry encryption standards—such as those from the US National Institute of Standards and Technology (NIST)—recommend deprecating vulnerable algorithms before threat actors gain quantum computing capabilities. That's why it's critical for companies to close knowledge gaps, assess their cryptographic dependencies, and build a roadmap for readiness.

Internal challenges to achieving post-quantum cryptography over the next 12 months



Q. What are your organisation's biggest internal challenges to achieving post-quantum cryptography over the next 12 months?

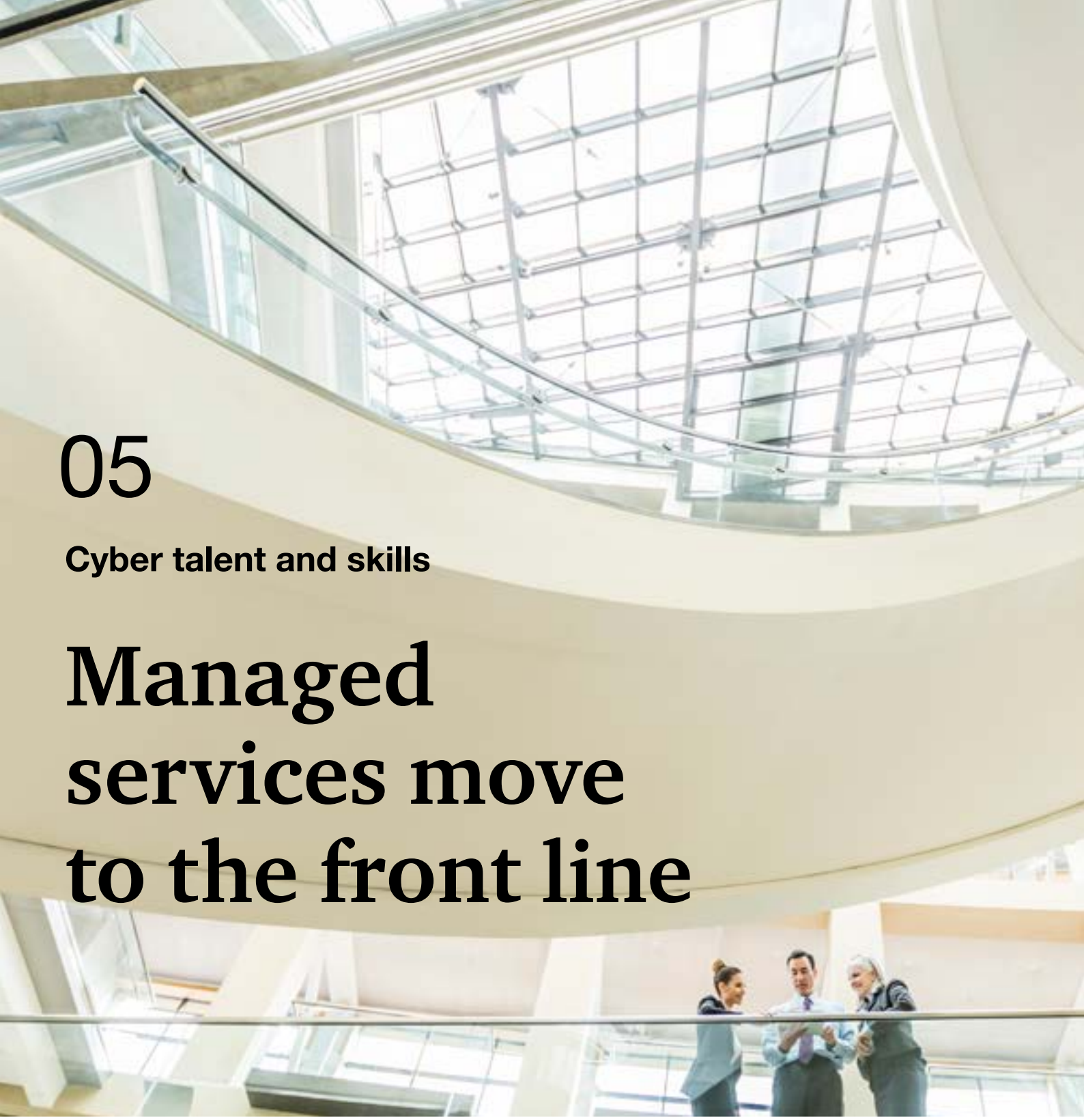
Base: India security leaders=85

Source: PwC 2026 Global Digital Trust Insights

Call to action

As India races ahead in its digital transformation, quantum computing is emerging not just as a technological marvel but as a looming cybersecurity frontier. The shift to quantum resilient security isn't optional—it's a strategic necessity. In a landscape where data sovereignty and security of national digital infrastructure are paramount, organisations must move beyond awareness to action. The future of cybersecurity will be defined by those who prepare today for the quantum realities of tomorrow.

- **Make quantum readiness a strategic priority:** Elevate post-quantum cryptography from a technical concern to a board-level agenda.
- **Close knowledge gaps:** Build internal awareness and expertise around quantum threats and cryptographic transitions.
- **Build a multi-year roadmap:** Treat quantum readiness as a phased journey. Start now to stay ahead of disruption.



05

Cyber talent and skills

Managed services move to the front line

Top 2

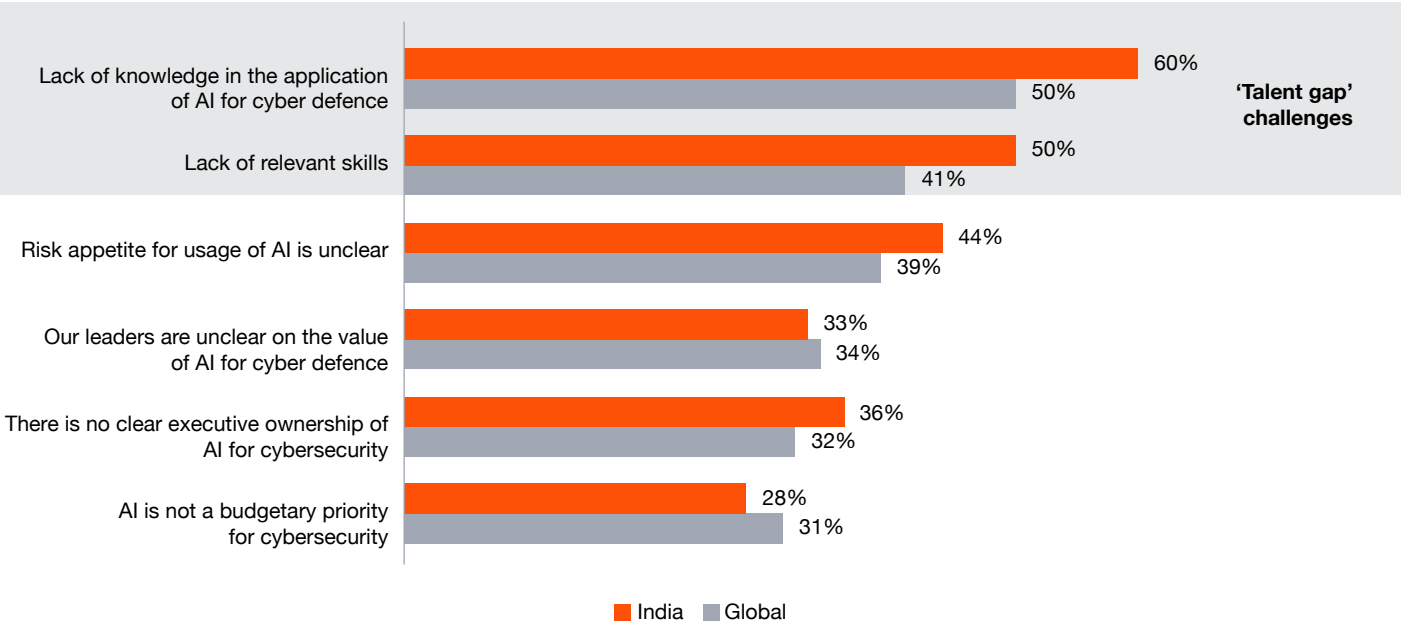
challenges in implementing AI for cyber defence are knowledge and skills gaps

61%

rank AI and machine learning tools among their top three priorities to address cyber talent gaps over the next 12 months

A persistent cybersecurity talent shortfall is slowing progress just as organisations aim to operationalise AI, secure complex environments, and prepare for next-generation threats. Over the past year, **knowledge and skills gaps** were the two most cited barriers to implementing AI for cyber defence—prompting a shift from hiring alone to **scaling capability** through multiple levers. Many Indian organisations are exploring new ways to gain proficiency, including AI tools (61%), cybersecurity tool consolidation (51%), security automation tools (49%), and upskilling or reskilling (49%).

AI implementation challenges for cyber defence



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

Base: India security leaders, CEOs, CFOs, finance directors, COOs, and operations directors=123

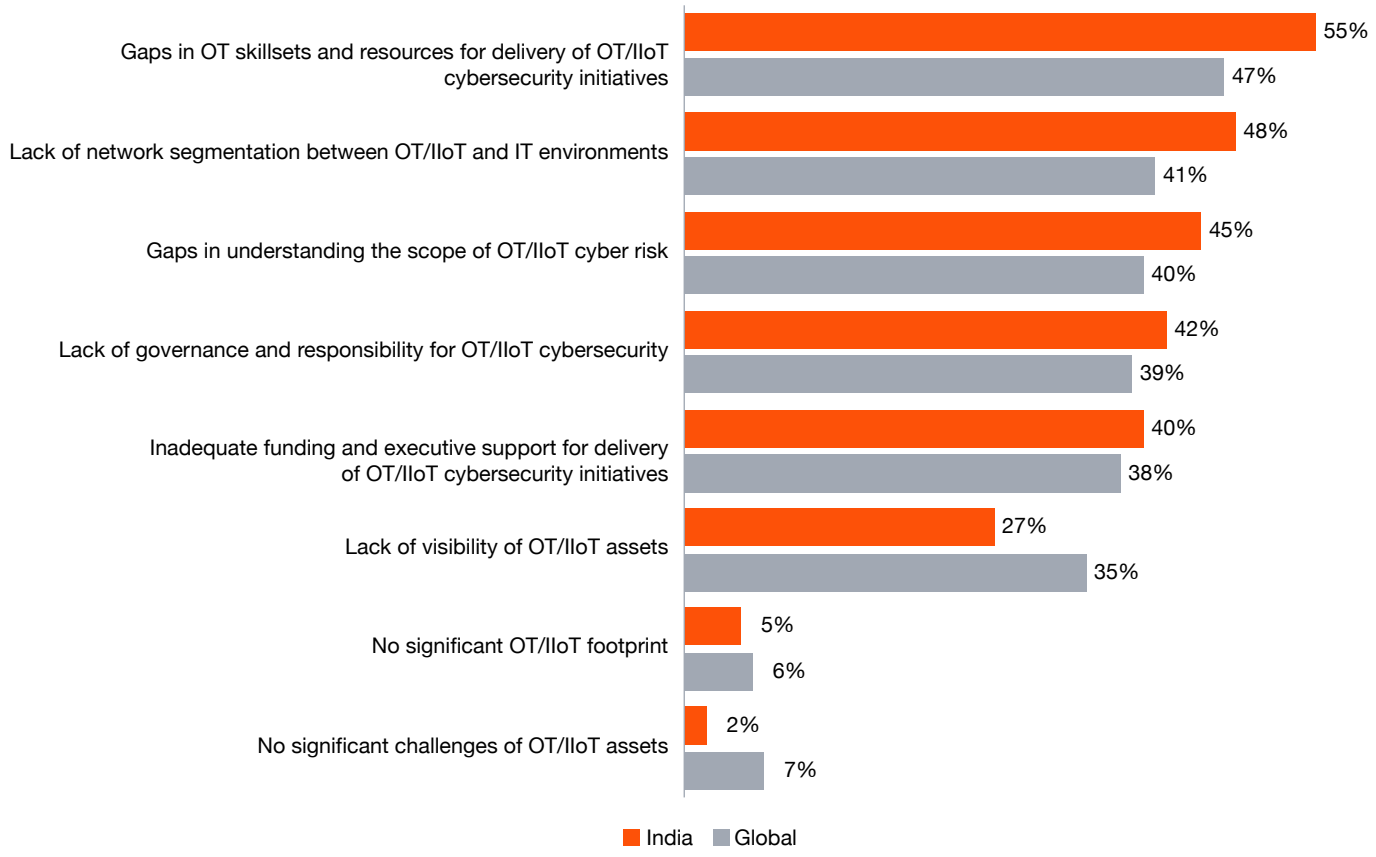
Source: PwC 2026 Global Digital Trust Insights

Wanted: OT skills

OT and industrial internet of things (IIoT) have become pressure points in today's security landscape. As organisations digitise their physical infrastructure, the complexity and exposure of these environments are increasing while the capabilities to secure them struggle to keep pace.

More than half (55%) the leaders of Indian organisations we surveyed cite a lack of qualified personnel among their top three challenges, while 42% point to unclear governance and ownership. Together, these discrepancies expose a deeper issue—that many organisations still lack the structure and expertise to manage increasingly connected operational systems with confidence.

Obstacles for securing OT and IIoT systems



Q. What are the top 3 challenges your organisation faces in securing OT/IIoT systems?

Base: India security leaders=85

Source: PwC 2026 Global Digital Trust Insights

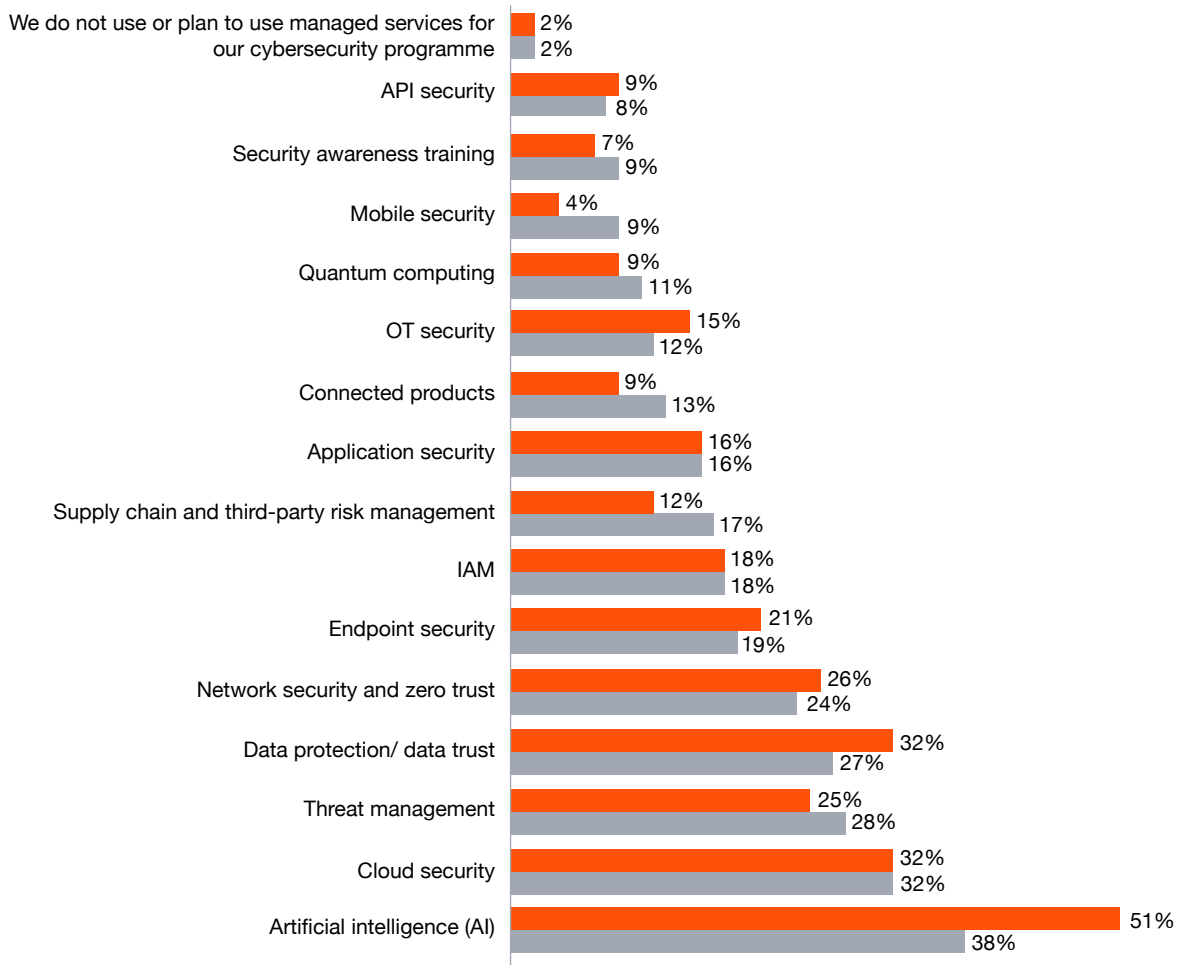
Managed services as a strategic accelerator

In India's fast-evolving digital ecosystem, managed security services are no longer just operational support; they are becoming a core delivery model for cybersecurity. Organisations face acute skill gaps in hiring, training, and retaining talent that is both technically proficient and deeply aware of business ecosystems and value chains—which are constantly evolving. To address this, enterprises are turning to providers who can share risks and rewards, making managed services central to their cyber strategy.

This shift is also evident in recent survey findings: As organisations accelerate cloud adoption and embed AI across business functions, these technologies have emerged as both top cybersecurity investment areas and primary use cases for specialised managed services.

Managed service providers bring proven experience in engineering, implementation, and operations, combined with sharp business context gained from working across industries and scales. This expertise helps organisations modernise defences while enabling innovation and growth.

Cybersecurity priorities for the use of managed services



Q. Which, if any, of the following areas of your cybersecurity programmes is your organisation prioritising to utilise managed services over the next 12 months?

Base: India security leaders=85

Source: PwC 2026 Global Digital Trust Insights

Call to action

As AI becomes central to defence strategies, organisations must rethink how they build capabilities, not just through hiring but also by scaling skills with automation, managed services, and continuous learning. In this new era, resilience will come from headcount as well as the intelligent empowering of teams to secure what's next.

- **Invest in capabilities, not just headcount:** Shift focus from hiring alone to building scalable, AI-augmented security teams.
- **Continuous learning:** Prioritise upskilling and reskilling programmes to future-proof your workforce.
- **Leverage managed services strategically:** Employ specialised partners to accelerate maturity, bridge talent gaps, and ensure compliance.

C-suite playbook

From uncertainty to action—what leaders can do now

This year's survey shows that the most forward-looking organisations are aligning cybersecurity with business strategy and prioritising readiness over being reactive.

Many have already established foundational cyber risk management practices by reinforcing a governance structure that aligns to leading cyber frameworks, embedding cyber risk controls across the enterprise and prioritising risk assessments and reporting.

To be future-ready, however, you'll need to do more than business as usual. That means confronting uncertainty, making bold but informed decisions, and building agility into your strategy.

Chief information security officer (CISO)/chief security officer (CSO)

Your ability to not only translate complex cyber risks into business risks but also effectively communicate how cybersecurity is a shared responsibility are key to securing C-suite buy-in and collaboration. This shared understanding will help foster foundational governance, resilience, regulatory compliance, and response practices. Moving forward, you should proactively address novel risks by advancing a secure-by-design mindset and use data to measure and show where cyber investments are needed most.

Foundational
Quantify geopolitical risk exposure using metrics tied to critical infrastructure, global operations, and industry-specific disruptions, and share findings with the C-suite.
Implement dynamic threat modelling aligned to current intelligence on high-risk regions, cyberthreat campaigns, and data extortion trends.
Embed responsible AI[4] principles across AI deployments and classify AI systems (including models, agents and their identities, applications, and training data) based on sensitivity, criticality, and exposure.
Secure AI by expanding existing security controls to AI systems and identify gaps where new capabilities are required (e.g. AI guardrails or LLM gateways).
Regularly re-examine and update cyber risk governance models to incorporate evolving technology risks like AI and quantum.
Strengthen governance through actionable KPIs that track performance in managing third-party, supply chain, legacy, and cloud-based risks.
Run tabletop exercises and simulations to stress-test decision-making, determine escalation paths, and validate recovery steps.

Future-ready
Establish cybersecurity as a shared responsibility with the C-suite and board by incorporating governance discussions on top of threat intelligence insights and executive-level summaries of emerging threats and adversary capabilities.
Operationalise AI agent oversight and governance through discovery, classification, exposure mapping, and continuous monitoring, including adversarial simulations.
Shift from point-in-time vendor assessments to continuous third-party risk monitoring.
Assess which systems depend on cryptography and adopt post-quantum cryptographic (PQC) standards where needed.
Determine if your business should leverage managed services by developing an ROI-based managed services plan that maps technology, skills, and resource needs.
Assess your data and determine what should be quantum-ready now, then work with your data governance teams on quantum adoption.

4 https://www.pwc.com/us/en/tech-effect/ai-analytics/responsible-ai-cybersecurity.html

Chief technology officer (CTO)/chief information officer (CIO)

Your foundational focus on securely scaling technology[5] and proactively addressing talent and training gaps provides critical support to the organisation's cyber posture. You should continue collaborating closely with security leadership to embed risk controls and governance throughout technology adoption. Looking forward, you must lead efforts to pilot and integrate emerging technologies such as AI and quantum computing with built-in security while driving innovation that anticipates and mitigates future cyber risks.

Foundational	Future-ready
Scale AI and other emerging technologies securely, budgeting for and embedding critical proactive security measures.	Coordinate with CISOs and data leaders to secure sensitive training data and reinforce AI model input/output governance.
Collaborate closely with the CISO and chief risk officer (CRO) to align technology deployment with risk management and compliance requirements.	Align quantum adoption and pilot initiatives with enterprise-wide quantum-resistant security strategies in partnership with security leadership.
Secure AI by embedding governance and cyber risk controls in AI implementation from the start, aligned with secure-by-design principles.	Advance adoption of automation and AI-driven risk detection and response tools to increase operational efficiency and resilience.
Enforce consistent identity, access, and policy controls across third-party platforms, APIs, and integrations.	Adopt a secure-by-design framework for connected products throughout the operational life cycle.
Apply robust IIoT and OT governance into your architecture strategy to gain end-to-end visibility and controls across distributed environments.	

5 https://www.pwc.com/us/techrisk

Chief risk officer (CRO)

Your focus on identifying enterprise and emerging risks, and their interdependencies with cybersecurity, is critical to safeguard the organisation. You should continue tailoring controls for evolving vulnerabilities while confirming that risk frameworks are still current. Looking ahead, your role will continue to require integrating AI, quantum, and geopolitical exposures into an adaptive, forward-looking risk management strategy that supports the organisation's agility and resilience.

Foundational	Future-ready
Embed threat-led scenarios into risk registers and stress-testing cycles, prioritising threats with known geopolitical vectors.	Expand third-party risk models to consider quantum capability in vendor environments and resilience to adversarial AI misuse.
Evaluate existing controls to address these exposures, tailoring current mitigation strategies where necessary.	Leverage AI to continuously assess cyber risk at scale, from cyber risk quantification through assessments to reporting.
Quantify AI and quantum risks using tailored business impact analyses, prioritising areas with digital workforce automation.	Develop an intelligence-integrated risk framework (IIRF) that incorporates various lenses of strategic threat intelligence into enterprise risk scoring.
Support compliance efforts by mapping cyberthreat management to regulatory requirements.	Pilot predictive threat modelling tools to simulate emerging threats and quantify probable business impacts over the next 12 to 36 months.

Chief financial officer (CFO)

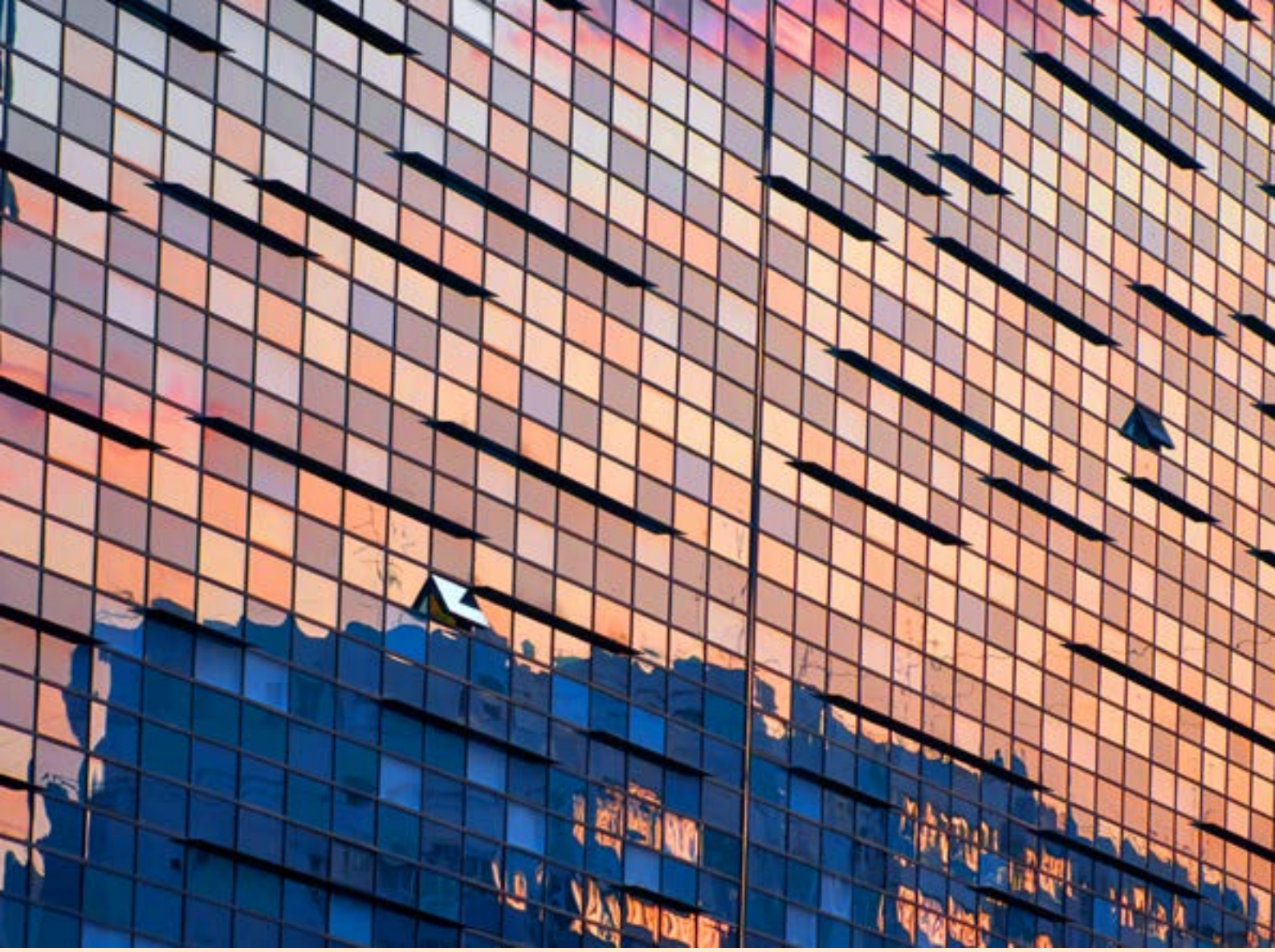
Your foundational role in enforcing appropriate budgeting for proactive cyber measures in strategic initiatives and tech implementations is essential to organisational resilience. You should continue identifying inefficiencies and aligning budgets with high-impact cyber initiatives. Looking ahead, preparing for emerging risks means proactively mapping future budget needs and fostering ROI-driven funding models, so the organisation can invest wisely in security technologies and skills.

Foundational	Future-ready
Support strategic investments that drive long-term resilience, competitive advantage, and regulatory readiness.	Advocate for cybersecurity as a material business function, linking investment levels to board-level performance objectives.
Assess the long-term costs of reacting to security incidents versus investing proactively in cyber defences, managed services, insurance, compliance, etc.	Create a capital allocation reserve for ‘resilience enablers’, including zero-day exploitation response capabilities and post-quantum hardening.
Recalibrate cyber ROI metrics to include savings from incident prevention, regulatory fines avoided, and response time reduction.	Develop ROI-driven business cases for managed security services.
Collaborate with CISOs, CTOs, and CIOs to budget effectively for cybersecurity skill development and technology training.	Identify and reduce inefficiencies such as tool redundancies and consolidate where possible.
Support sustainable funding models that balance operational costs with strategic cyber investments.	

Chief executive officer (CEO)

Your ongoing commitment to making sure cybersecurity is a business priority remains essential. You should continue aligning business initiatives with the cyber risk management strategy while fostering collaboration across the board and C-suite. Looking ahead, your role involves building influential partnerships and championing investments that enable your organisation to navigate emerging cyber challenges.

Foundational	Future-ready
Mandate cyber scenario participation at executive offsites, simulating sector-specific disruptions and hybrid threat operations.	Lead multi-industry alliances for post-quantum standardisation, joint defence postures, and threat intelligence exchange.
Tie cyber resilience to revenue enablement, such as securing digital platforms, customer data trust, and cross-border growth.	Champion investment in emerging technologies (AI, quantum) with security designed from the start.
Advocate responsible innovation, confirming that AI and quantum projects embed ethical and security guardrails from inception.	Institutionalise quantum and geopolitical foresight reviews into strategic planning cycles and board risk charters.
Understand where cyber budget trade-offs are made and if those trade-offs meet risk appetite.	Actively participate in stress tests to prepare for geopolitical and technological disruptions.
Make cybersecurity a shared responsibility at every level, from the boardroom to the back office.	
Keep the board informed on strategic cyber programme priorities and engage directors to discuss programme needs.	



About this survey

The 2026 Global Digital Trust Insights is a survey of 3,887 business and technology executives conducted in the period from May to July 2025. The India edition of the global survey report focuses on the responses of the executives of 138 Indian businesses.

33% of the respondents are executives in large Indian companies with $1 billion or more in revenue; 34% are in companies with $10 billion or more in revenues.

64% of the respondents from India who participated in our survey are tech executives and 36%, business executives.

PwC Research, PwC's global Centre of Excellence for market research and insight, conducted this survey.

About PwC

We help you build trust so you can boldly reinvent

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.com.

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.

Contact us

Sundareshwar Krishnamurthy
Partner and India Cyber Leader
PwC India
sundareshwar.krishnamurthy@pwc.com

Anirban Sengupta
Partner and Co-Leader - Cyber and Digital Risk
PwC India
anirban.sengupta@pwc.com

pwc.in

Data Classification: DC0 (Public)

SG/Oct 2025 - M&C 49319