Accenture Research Report

Reinventing the cyber workforce

Three moves to address the cybersecurity talent gap

Authors

Harpreet Sidhu

Global Lead - Cybersecurity

Harpreet Sidhu advises C-suites and boards on cyber strategy, resilience and transformation. He guides end-to-end security solutions that drive business growth for some of the world's most complex organizations.

LinkedIn

Vikram Desai

Senior Managing Director - Cybersecurity, Cyber Strategy Risk and Architecture

Vikram Desai is a three-time Tech CEO who partners with boards and C-suites to build and execute cybersecurity strategies that support, protect and accelerate growth.

LinkedIn

Christian Weiss

Strategy Principal Director - Talent & Organization

Christian Weiss leads transformation projects spanning organizational design, workforce planning and effectiveness, and HR and digital transformation. He delivers integrated, pragmatic solutions to help organizations thrive, with a specialty in cybersecurity.

LinkedIn

Mariana Perez

Associate Director - HR Partner, Cybersecurity

Mariana Perez partners with senior leaders to build future-ready, inclusive workforces by advancing leadership development, talent strategy and cultural transformation, enabling sustained diversity, resilience and high performance.

LinkedIn

Yusof Seedat

Global Research Lead, Cybersecurity

Yusof Seedat creates data-driven insights and thought leadership to guide strategy, business development and market positioning for organizations across the world.

LinkedIn

Executive summary

Cybersecurity is a critical enabler of enterprise resilience, regulatory accountability and digital growth. Yet the cybersecurity workforce designed to protect the business is misaligned with the demands it faces. Fifty-nine percent of open roles now require a hybrid blend of technical depth, business acumen and strategic leadership, which includes soft skills like problem-solving, communication and cross-functional collaboration. Only 40% of professionals, however, currently hold such roles. This highlights a capability imbalance that hiring alone will not correct. Cyber and talent leaders must address this gap holistically to make cybersecurity a sustaining force that helps the business thrive through change.

Almost half of cybersecurity roles globally remain unfilled today. While some surveys suggest overall headcount pressures may be easing in certain markets, the underlying challenge is shifting rather than resolving. Accenture's analysis of more than 550,000 cybersecurity job postings and professional profiles reveals the true constraint is not just the number of cybersecurity professionals available, but also if they have the right mix of technical and soft skills to operate effectively at the enterprise level. It's a gap between what modern cybersecurity requires and what labor markets have to offer.

18%

of organizations today have aligned talent, technology and business strategy to reflect how work is changing

Recent Accenture talent research shows that only 18% of organizations today have aligned talent, technology and business strategy to reflect how work is changing, leaving most labor markets mismatched with current business needs.[1] Modern cybersecurity sits at the intersection of digital platforms, AI deployment, regulatory accountability, operational resilience and customer trust. This requires talent that can work with the business and across functions. Yet the labor market has a disproportionate divide between two capability profiles: **Conductors,** who combine technical depth and business acumen, and **Operators,** who remain primarily execution focused with technical skills sets. Organizations increasingly need Conductors, or professionals who can translate business strategy into secure architecture, quantify and communicate risk, guide cross-functional decisions and embed security into digital transformation. However, the cybersecurity labor market continues to offer mostly Operators. The result is a workforce optimized to operate tools, but not to guide enterprise resilience.

Several forces create this imbalance. First, skills demand is growing more complex, reflecting a need for multidimensional skills and AI-related capabilities. Second, organizational underinvestment and high attrition prevent experience from deepening, eroding internal capability just as demand intensifies.

87%
of leaders cite AI-related vulnerabilities as the fastest-growing cyber risk

Our analysis shows that average cybersecurity tenure fell to 1.8 years for the period between 2015 and 2025, down from 3.3 years between 2005 and 2015. And fewer than three in ten organizations fund structured upskilling programs.[2] Third, external pressures such as AI-enabled threats and rising regulatory accountability are raising the bar faster than workforce skills can adapt. The World Economic Forum's 2026 Cybersecurity Outlook reinforces this point, with 87% of leaders citing AI-related vulnerabilities as the fastest-growing cyber risk.[3] CrowdStrike's 2026 Global Threat Report documents an 89% year-over-year increase in AI-enabled attacks.[4] At the same time, critical cybersecurity knowledge is increasingly distributed across ecosystems, making effective defense impossible for any single company acting on its own.

Post-incident response patterns highlight the consequences of this gap. Following major incidents, companies typically restructure security teams, expand budgets, appoint new leaders and accelerate investments in tools and controls. While these actions stabilize operations in the short term, they rarely address the underlying workforce model.

Fixing the capability imbalance requires reinventing cybersecurity around the people doing the work, specifically how they learn, collaborate and apply multidimensional skill sets in real-world conditions.

Three moves define the path forward:

01 **Build internal capability and the culture to sustain it.**

Companies must nurture hybrid talent through multi-year development pipelines, cross-domain exposure and retention-focused operating models. Talent mobility and personalized learning pathways are also essential to ensure expertise matures rather than churns.

02 **Redesign roles and career paths to cultivate Conductor-level skills.**

Cybersecurity roles must evolve from a narrow vertical ladder into a distributed enterprise capability. Companies must embed cyber talent across all functions to manage risk and enable professionals to grow into business-aligned leaders rather than exiting their roles.

03 **Augment human capabilities with AI, connected architecture and long-term partnerships.**

Design technologies to elevate human judgment, with people always in the lead. When AI is designed with natural workflows in mind, it can absorb a high volume of repetitive tasks while enabling human talent to exercise greater strategic oversight. Architectures must reduce fragmentation and amplify both human and machine capability. Enduring ecosystem partnerships can extend institutional memory and accelerate foresight.

Together, these three moves shift cybersecurity from a reactive cost center to a capability that strengthens with each disruption.

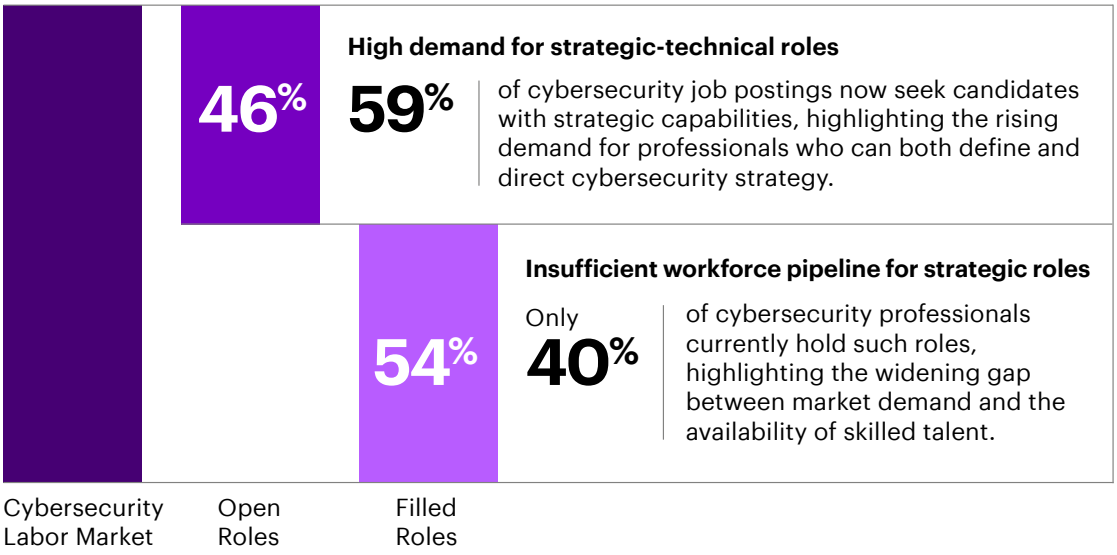
Organizations that address the cyber talent imbalance through deliberate talent strategies across skills, operating models and enablement will gain more than staffing stability. They will build faster recovery cycles, stronger regulatory posture, greater digital agility and deeper customer trust.

Cybersecurity talent is under structural strain

Cybersecurity has shifted from a specialist IT function to a core enabler of enterprise resilience and innovation. Yet workforce models have not evolved at the same pace. The shift is qualitative: Modern cybersecurity requires professionals who can translate strategy into architecture, guide cross-functional teams, quantify business risk and embed security into digital initiatives.

Forty-six percent of cybersecurity roles remain unfilled today. Among those, 59% require combined strategic and technical skills. However, only 40% of the current workforce is employed in roles that fit that profile (Figure 1).

Figure 1: The cybersecurity talent gap is driven by an undersupply of strategic skills in the market



Source: Lightcast Database

Throughout this research, Accenture distinguishes between two cybersecurity capability profiles. Conductors combine deep technical cybersecurity expertise with business acumen, strategic leadership skills and soft skills, enabling them to translate risk into enterprise decisions and embed security into transformation initiatives. Operators, by contrast, primarily execute technical security tasks and controls, with limited exposure to business, governance or cross-functional leadership responsibilities.

Today, cybersecurity sits at the intersection of business strategy, digital platforms, regulation and trust. This shift requires a new balance between Conductor and Operator capabilities in the workforce. Organizations increasingly seek professionals who can orchestrate across domains rather than just operate within silos.

The talent supply chain, however, remains anchored in an outdated model. Most universities focus on technical theory and code rather than enterprise context.[5] Employers train based on legacy job descriptions that fail to reflect modern business needs. And cybersecurity continues to be positioned as an IT career path instead of a strategic business capability.

The result is an imbalance that cannot be rectified by simply hiring more people. At issue is a structural mismatch between the skills produced and the skills required. As threats grow more sophisticated, regulatory expectations intensify and enterprises accelerate digital adoption, organizations face a workforce that is structurally misaligned with modern demands.

At the same time, the knowledge required to defend against modern threats is increasingly distributed across external ecosystems—threat intelligence communities, sector bodies, vendors and government agencies—creating a broader operating model challenge that extends beyond talent imbalances.

This structural gap forms the core of the challenge facing CISOs, CIOs and CHROs. Cybersecurity has become indispensable to business success, yet the talent system built to support it is struggling to adapt. Addressing the talent imbalance requires rethinking how organizations find, develop and retain the people who protect them.

Forces widening the cybersecurity talent gap

Several interlocking forces have created a structural capability gap that widens faster than organizations can respond. Complex demand, organizational underinvestment and external pressures are continuously raising the bar for cybersecurity capability. Each force on its own creates strain; collectively, they form a self-reinforcing cycle that can erode the cybercapability, putting organizations at risk.

Complex demand

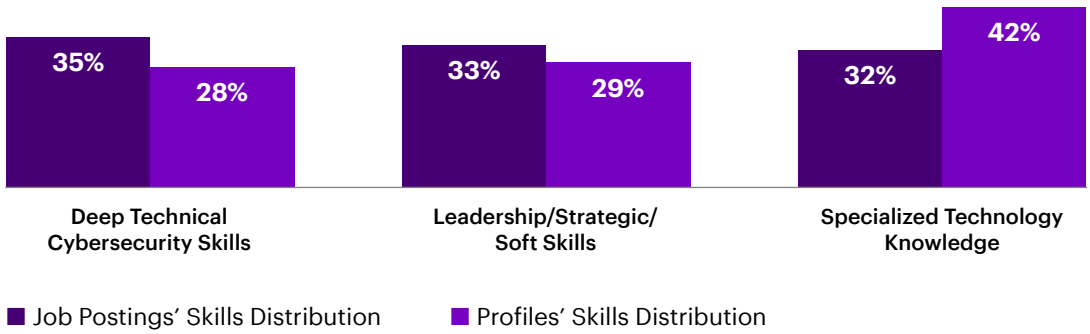
Cybersecurity roles have transformed dramatically, reshaping the competencies required to succeed. The modern practitioner must be as fluent in business processes and transformation as they are in architecture diagrams or threat models. The demands placed on the role have expanded in three distinct dimensions:

- Deep technical cybersecurity expertise across areas such as cloud security, identity management, data protection and secure engineering.
- Specialized technology skills tied to emerging domains, from operational technology to AI and cloud computing.
- Leadership, strategic and soft skills required to operate at the enterprise level, including problem-solving, communication, cross-functional collaboration, risk translation, policy design, vendor management and change leadership.

Labor market data shows that employers are no longer hiring only for isolated technical expertise. For example, skills demanded for cybersecurity engineers are distributed across three dimensions: 35% relate to core cybersecurity expertise, 33% to leadership and strategic capabilities and 32% to specialized technology knowledge (Figure 2). Employers are clearly seeking professionals who can operate across domains rather than within a single technical lane. For cybersecurity product managers, the balance shifts even further. Nearly 59% of required skills fall within the leadership and strategic dimension.

Figure 2: Strategic cybersecurity roles demand more than technical security skills, exposing significant workforce misalignment

Cybersecurity Engineer: Distribution of Skills



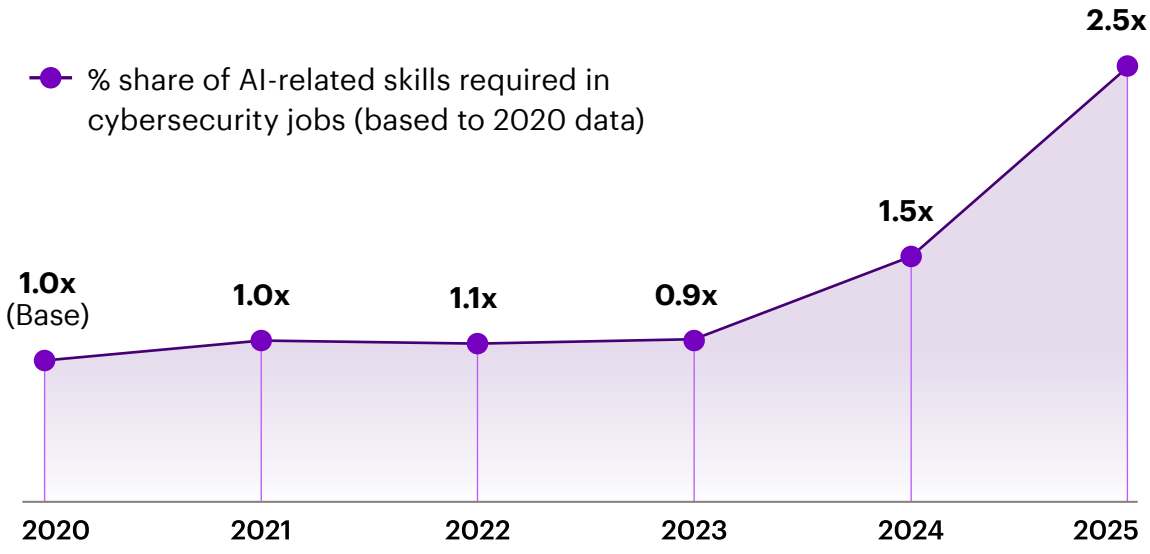
Note: Calculated as a percentage of total skills across the three categories: deep technical cybersecurity, leadership/strategic/soft skills and specialized technological skills, for cybersecurity engineer

Source: Lightcast Database

However, the workforce profile does not mirror this demand pattern. Cybersecurity engineers' profiles show lower concentrations of core cybersecurity expertise (28%) and enterprise leadership capabilities (29%) than job postings require. Capabilities such as automation, security information and event management (SIEM) expertise, and strong computer science foundations appear more frequently in postings than in professional profiles.

AI-related cybersecurity skills further complicate the challenge ahead. Demand for these skills has more than doubled (2.5x) since 2020 (Figure 3), reflecting how rapidly AI is reshaping both attack and defense dynamics. Yet workforce capability is not scaling at the same pace. The gap is particularly pronounced in areas such as AI governance, model security and AI-enabled threat detection. These are advanced capabilities that require a combination of technical depth, domain understanding and strategic judgment. As AI becomes embedded across enterprise systems, this capability gap can widen if organizations do not proactively build these skills internally.

Figure 3: AI-related cybersecurity skills now account for a growing share of job postings



Source: Lightcast Database

Compounding the issue is a visibility problem. Cybersecurity roles make up only 3.5% of all IT job postings, far overshadowed by fields such as software development (35%) and network and systems engineering (16%). The profession does not receive the promotion, branding or public narrative that might attract high-potential candidates from other domains. As a result, cybersecurity competes for a disproportionately small share of the technology talent entering the workforce each year.

Overall, the outcome is predictable: The labor market continues to produce technically capable operators, but far fewer professionals with the hybrid technical, business and leadership capabilities required to integrate and guide cybersecurity at the enterprise level.

> **Cybersecurity competes for a disproportionately small share of technology talent, accounting for just 3.5% of IT jobs posts.**

Organizational underinvestment

Even where talent exists, organizations struggle to develop, retain and empower cybersecurity professionals. Many report sustained operational pressure, with more than half citing frequent work-related stress and one in five considering leaving the profession.[6] The operational tempo is unrelenting, threats are continuous and teams often feel understaffed and under-resourced.

Attrition pressures have been significant in recent years, with work-related stress cited as a leading reason cybersecurity professionals leave their jobs. While retention trends vary by region, average tenure remains low, falling from 3.3 years (2005-2015) to 1.8 years (2015-2025). Despite this, many organizations still underinvest in structural measures such as workload balancing, career mobility and leadership support that could address the root causes of burnout.

Furthermore, even amid widely reported talent shortages, some organizations, particularly larger enterprises, continue to reduce cybersecurity headcount during broad restructuring cycles. Such workforce volatility, whether caused by layoffs or burnout-driven departures, undermines long-term capability development and erodes institutional knowledge.

> **The average tenure of cyber professionals fell to just 1.8 years for the period between 2015 and 2025, down from 3.3 years (2005-2015).**

Fewer than

30%

of organizations fund structured upskilling programs

Despite this, most organizations continue to rely primarily on external recruitment. Fewer than 30% fund structured upskilling programs,[7] and 57% cite insufficient internal investment as a direct cause of talent shortages.[8] According to Accenture's 2025 State of Cyber Resilience research, almost half of respondents (49%) believe talent shortages impact the cybersecurity function significantly.[9] Internal development pathways remain fragmented and compliance-driven or focused narrowly on specific technologies. As a result, mid-career professionals often encounter limited growth opportunities, while early-career talent is confined to narrow, repetitive operational work that does little to expand their skills. Organizations create their own bottlenecks by failing to develop hybrid leaders, even as demand for such talent intensifies.

Higher education systems have also struggled to keep pace. A review of 100 university cybersecurity programs across 24 countries shows persistent gaps in areas such as cyber law, risk management, enterprise architecture and executive communication, capabilities now central to employer demand. Students graduate knowing how to configure a firewall, but not how to assess business risk, communicate with executives or design cross-enterprise security controls.[10,11]

Countries such as Singapore, Germany, China and the US have made significant strides, establishing structured national cybersecurity education pathways. But elsewhere—in parts of Africa, Southeast Asia and Latin America, for example—programs rely heavily on donor funding and often focus on foundational digital literacy rather than specialized cyber capabilities. Even within advanced markets like the European Union (EU), education remains fragmented, producing inconsistent skill readiness.[12]

External pressures

External forces amplify internal capability gaps. Threat actors increasingly leverage automation, AI-generated phishing, deepfakes and adaptive malware, evolving tactics in weeks rather than years. According to the World Economic Forum's 2026 Cybersecurity Outlook report, 94% of leaders expect AI to be the most significant driver of change in cybersecurity in the year ahead, while 87% identify AI-related vulnerabilities as the fastest-growing cyber risk.[13] The rapid advancement of frontier AI models' cyber capabilities reveals that exploits are becoming cheaper, faster and more scalable, outpacing most organizations' remediation capabilities. Workforce skills, by contrast, are shaped by talent pipelines that evolve more slowly than the threat environment. This pace disparity means the bar for competency rises continually. A professional who trained five years ago must now master AI governance, identity-based micro-segmentation, cloud-native detection and software supply-chain risk, all while performing their day-to-day responsibilities.

Meanwhile, cybersecurity and technology leaders are assuming accountability for the cyber-savvy of not just their own people, but the entire workforce. Human risk remains under-managed: Today, only 18% of organizations deliver role-specific cyber awareness programs, according to Accenture's 2025 State of Cyber Resilience research.[14] As attacks grow more targeted, behavioral vulnerabilities remain exposed. Most rely on generic annual training that does little to prepare employees for sophisticated threats like deepfake voice scams. This underinvestment in human risk creates a systemic vulnerability.

The exposure is not limited to frontline staff. Board members and senior executives often lack the cybersecurity fluency required to assess risk, challenge assumptions and make informed strategic decisions, increasing the likelihood of misjudgment at the top. Every employee becomes a potential vulnerability, especially when adversaries are using AI to amplify scale and precision.

At the same time, regulatory regimes are shifting accountability toward individuals. In several major economies, senior technology and security leaders face direct penalties for governance failures, including fines, career-impacting sanctions and even criminal liability. This raises the demand for leaders fluent in law, risk, crisis management and technology, precisely where talent shortages are most acute. Many prospective leaders hesitate to step into senior cyber roles precisely because the personal stakes are so high.

Taken together, complex demand, organizational underinvestment and external pressures have created a structural imbalance that threatens enterprise resilience. Left unchecked, these forces will widen the capability gap each year, leaving enterprises more exposed to disruptions, regulatory consequences and breakdowns in customer trust.

Cybersecurity can no longer rely on incremental hiring or ad-hoc skill development. The function must undergo structural reinvention, and business leaders must play a central role in shaping it.

A widening cyber capability gap could leave enterprises exposed to disruption, regulatory impact and declining customer trust.

Why the current workforce model no longer works

For years, organizations have responded to rising cyber threats by adding new tools, new controls and new specialists. What began as pragmatic defense has hardened into a fragmented workforce model built for a simpler era, one where threats were slower-moving, systems were more contained and cybersecurity could be treated as a specialized technical function.

This model assumes that the external labor market can supply whatever skills organizations lack. It cannot. As cybersecurity becomes embedded in enterprise decision-making, the talent required must combine deep technical fluency with architectural understanding, business acumen and softer skills.

A closer look at post-incident response patterns reveals a critical blind spot. Major cyber incidents often serve as inflection points for organizational change, but the changes that follow are remarkably consistent. Organizations restructure security teams, expand budgets, appoint new leaders and accelerate investments in tools and controls (Figure 4). These actions are effective at stabilizing operations, satisfying regulators and restoring confidence in the short term. What they rarely do is fundamentally redesign how cybersecurity talent is recruited, onboarded, developed, deployed and embedded across the business.

Figure 4: What organizations do after a major cyber incident

Post-incident response patterns

Trigger: Major cyber incident	Response actions	Frequency
Operational disruption Regulatory scrutiny Loss of customer & stakeholder trust	Operational disruption	●●●○○○
	Security budget expansion	●●●●○○
	New security leadership roles	●●○○○○
	Expanded security functions	●●●○○○
	Advanced tool investments	●●●●●●
	Talent realignment (role redesign, reskilling, career path changes)	○○○○○○

Source: Based on an analysis of major cyber incidents reported in the public domain between Jan. 2025 – Jan. 2026

Responses to cyber incidents rarely fail because of missing tools. They fail because people, processes and decisions could not keep pace with how the attack unfolded.

The 2023 cyberattack on MGM Resorts illustrates this pattern. Initiated through social engineering and identity compromise, the attack caused widespread disruption across hotel operations, casinos, reservations and payment systems for several days.[15] In response, MGM strengthened identity controls, elevated incident-response capabilities and increased executive oversight of cybersecurity operations. These actions reduced immediate risk and helped restore services, but they did not address the deeper issue. The breach did not succeed because tools were missing, but because human-centric threats (such as attackers impersonating employees to trigger help-desk credential resets) outpaced existing skills, roles and operating models.[16] Like many organizations, MGM's response focused on remediation rather than redesigning how Conductor-level cybersecurity capabilities are built, distributed and sustained across the enterprise.

In contrast, Cloudflare's ability to consistently mitigate the world's largest distributed denial of service (DDOS) attacks to date, blocking them in real time without service disruption, reflects a fundamentally different approach.[17] These outcomes were the result of years of deliberate capability building, combining automation, scalable infrastructure and specialized human expertise designed to absorb extreme events without crisis-driven intervention. Cloudflare's global infrastructure network and workforce model were built to anticipate, rather than react to, scale and complexity. This reflects a workforce model deliberately designed to cultivate and retain Conductor-level capability before disruption occurs.

Building the capabilities that labor markets cannot currently supply requires stronger collaboration between cybersecurity and people functions.

These contrasting outcomes highlight a central flaw in the prevailing approach to cybersecurity investment. While technology and architecture are often upgraded after incidents, talent systems lag behind. Talent pipelines remain largely unchanged, upskilling is limited and future capability needs are rarely addressed systematically. As a result, organizations resolve today's incidents while leaving tomorrow's skills gaps intact. This also applies to cybersecurity skills in the overall workforce.

This reactive cycle reinforces the very talent imbalance organizations are trying to escape. Without redesigning roles, skills and operating models, post-incident responses optimize technology instead of people. Cybersecurity teams are left perpetually chasing new threats with a workforce that was never designed to keep pace.

The next phase of cybersecurity must therefore be built from the inside out. This involves rethinking how talent is developed, how work is structured and how human expertise is amplified. Today's objective is to create the capabilities labor markets cannot currently supply. Success requires stronger collaboration between cybersecurity and people functions, an alignment that remains underdeveloped in many organizations. Too often, cybersecurity teams attempt to address human capability challenges independently, rather than leveraging specialist expertise in workforce design, learning and organizational development.

Three moves to close the cyber talent gap

Closing the cybersecurity talent gap requires a structural reset in how capability is built, how work is organized and how human expertise is scaled over time. We recommend three moves that, together, enable organizations to build sustainable cyber capability despite persistent market shortages. Each move addresses a distinct gap in today's workforce model and is reinforced by targeted sub-actions that translate intent into execution.

Move 1: Build internal capability and the culture to sustain it

Today's cybersecurity talent challenge cannot be solved through external hiring alone. The hybrid professionals that organizations increasingly require—technically fluent, architecturally aware, business-aligned and equipped with the right soft skills—are emerging too slowly to meet demand. The first move is therefore to partner with HR to deliberately develop capability from within, supported by a culture that allows expertise to mature rather than churn.

Large financial institutions like JPMorganChase invest heavily in internal cybersecurity career pathways, developing talent from within rather than relying solely on external hiring. JPMorgan also partners with workforce organizations such as Per Scholas to expand access to cybersecurity education and early-career pathways.[18]

Some governments are also beginning to intervene at the system level to address structural gaps. The UK Cyber Security Council, established in 2021, aims to professionalize cybersecurity through defined career pathways, competency frameworks and chartered certifications aligned to the Cybersecurity Body of Knowledge (CyBOK), creating clearer entry routes and progression for hybrid cyber professionals.[19]

Develop multi-year internal pipelines that produce hybrid talent

Internal pipelines must expose practitioners to the full spectrum of cybersecurity work and the business systems it protects. This requires moving beyond certification-led training toward multi-year development pathways that rotate talent through cloud engineering, identity, data governance, product teams and enterprise risk. Cross-domain exposure builds integrative thinking and architectural intuition, which are capabilities that siloed technical roles rarely produce.

Exclusive Networks' CyberFarm illustrates this approach, employing university students in real cybersecurity roles while they complete their degrees. This creates a pipeline of "pre-qualified" junior cyber talent without shifting full training risk to employers.[20]

Widen entry points by converting adjacent talent into cyber practitioners

Organizations must systematically transition adjacent talent from application development, infrastructure, operations, audit, analytics and risk, and change/learning management into cybersecurity roles. These individuals bring contextual understanding of the business and technology environment, along with communication and collaboration capabilities that accelerate hybrid development.

Reposition cybersecurity as a talent engine, not a talent consumer

Security teams are often expected to create a workforce they are not trained to build. Effective capability development requires collaboration with HR strategists, learning designers, behavioral experts and change managers. Grounding development programs in how adults learn and sustain performance enables organizations to build cybersecurity talent at scale rather than compete endlessly for scarce profiles.

Create a culture that enables retention and capability growth

Culture is as critical as pipelines. Talent systems collapse if the environment doesn't prop up the people within them. With tenure now down to 1.8 years, sustained cybersecurity capability depends on a culture that supports people over time: one where teams can escalate issues early, accountability is shared with the business, priorities are transparent and well-being and stress reduction are embedded into daily operations rather than treated as peripheral. These are the structural conditions that allow expertise to deepen over time.

Break the hyper-specialization cycle by investing in integrator roles

One of the most damaging and least discussed dynamics in cybersecurity is the reflex to add new tools and specialists in response to every emerging threat. Each new challenge leads to another tool and another specialist, forcing an already small workforce to fragment even further. This proliferation fragments systems and teams alike.

Deliberate investment in security architects and integrator roles provides connective tissue across cloud, identity, data, applications and AI. These roles require strong cross-functional understanding (procurement, HR, legal, regulatory) and communication skills to translate technical trade-offs into business decisions. This reduces complexity and enables human-led AI at scale, because AI is only effective when fed with integrated, high-quality telemetry and well-structured control architectures.

Move 2: Redesign roles and career paths

Cybersecurity has become a horizontal enterprise capability, yet its job architecture remains vertically constrained. Too few growth pathways and too narrow a definition of success forces experienced professionals out of the function. This move develops and retains cybersecurity capability by redesigning roles and career paths so cyber professionals grow into enterprise leaders and by deepening executive-level understanding of cyber risk and its strategic implications. This is essential because Conductor-level capabilities, combining technical depth with business acumen and strategic leadership, must be developed through role design, career progression and enterprise exposure, not through hiring alone.

Expand career routes beyond a single vertical ladder

The traditional progression, from analyst to engineer to architect to Security Operations Center (SOC) manager or Chief Information Security Officer (CISO), has become a narrow funnel in a domain that's embedded across every major business initiative. When people reach their ceiling, they often leave, taking their experience with them.

Career paths must widen to reflect the true breadth of modern cybersecurity work. Advancement should extend across product security, cloud platforms, identity strategy, AI and data governance, architecture, regulatory interpretation and transformation programs. It must operate in both directions, with security professionals able to step into product or platform roles to gain commercial fluency and business and technology leaders having clear on-ramps into security. Embedding dynamic, AI-informed skills data into workforce systems creates an updated inventory of employee skills, capabilities and interests to support talent mobility. This deliberate cross-pollination is how organizations cultivate the multidimensional hybrid talent profiles that external labor markets cannot supply. Advancement should reward accumulated experience and breadth, not just role titles or certifications.

The UK Government Security Profession Career Framework, for example, formalizes multidirectional progression across security specializations including risk, architecture, assurance and operations. This allows professionals to move laterally between domains rather than advancing solely within a single vertical hierarchy. By structuring careers around competencies instead of job titles, the framework supports the development of hybrid security leaders capable of operating across technical and strategic functions.[21]

Prepare cyber leaders through enterprise-wide leadership development

Tomorrow's cyber leaders must be able to quantify financial risk, shape investment decisions, influence executives, negotiate trade-offs, communicate complex risk clearly, collaborate across business functions and articulate security's role in value creation. These capabilities do not emerge organically in technical roles. Cyber leadership pathways must therefore integrate with enterprise-wide leadership development programs. Cyber professionals should receive the same sponsorship, training and development opportunities as future leaders in finance, operations or product development.

Embed cybersecurity capability where risk is created

Talent models must reflect the reality that cybersecurity is inseparable from product design, cloud adoption, AI deployment, production and operational resilience. This also requires reframing security as a distributed responsibility rather than a single team's mandate. Cyber capability must be embedded wherever technology decisions are made and risk is created, including product development, change management and IT operations. When security sits at these intersections, talent gains context, business fluency and influence. This shift transforms cybersecurity from a centralized control and governance function into a distributed enterprise capability.

Google Cloud, for example, embeds security engineers directly into product and platform teams like DevSecOps and product security, ensuring security is built into design rather than reviewed after the fact. Security leaders rotate across engineering, product and risk roles, building deep business fluency alongside technical depth. This illustrates how cybersecurity becomes a distributed enterprise capability rather than a centralized control function.[22]

Move 3: Augment the human workforce with AI, architecture and partnerships, putting people in the lead

68%
of employees say AI saves time on routine tasks

Even a redesigned workforce cannot keep pace with the volume, speed and sophistication of modern cyber threats. The third move focuses on intelligent augmentation: scaling human judgment and decision authority rather than replacing it.

Use AI to absorb volume while elevating human judgment

Threat actors already use AI to automate reconnaissance, generate convincing deepfakes and personalize intrusion attempts at scale. Defenders must respond with equivalent acceleration. When mapped to people's actual workflows, AI can assume a substantial share of high-frequency tasks like alert correlation, behavioral anomaly detection, misconfiguration analysis, investigation support and secure code generation. This allows security practitioners to focus on intent interpretation, architectural trade-offs and strategic risk decisions, areas where human judgment remains critical. It also builds AI competency through hands-on usage. Across functions, employees are already seeing the value, with 68% saying AI saves time on routine tasks and 59% saying it improves work quality.[23]

Softcat used Security Orchestration, Automation, and Response (SOAR) capabilities (via Swimlane) to automate repetitive SOC tasks, freeing analysts to focus on complex incidents. By automating 14 workflows, Softcat onboarded 30% more customers with no increase in headcount, while upskilling junior staff and improving retention.[24]

Automation, however, introduces a developmental challenge: foundational technical work like deep troubleshooting, log analysis and incident reconstruction helps build intuition. If AI assumes too much too early, future leaders may not acquire the experiential base that informs good judgment.

Organizations must therefore preserve foundational learning through deliberate simulation environments like SOC exercises, threat-emulation labs, red–blue scrimmages, architecture walkthroughs and scenario-based learning. This ensures that emerging professionals develop solid intuition and judgment while still benefiting from automation.

Build foresight into workforce strategy

Because attackers continuously adapt, workforce strategy must be forward-looking. Organizations need to identify future cybersecurity jobs and skills early (using tools like Skyhive or Lightcast) and develop a deliberate portfolio of future cyber skills. This portfolio should be continuously refreshed by intelligence from across the ecosystem to prepare for threats three to five years ahead.

Use connected architectures to amplify cyber capabilities

AI's value to the workforce is entirely dependent on the environment it operates within. Fragmented telemetry and disconnected tools blunt AI's effectiveness. Connected security architectures reduce complexity, integrate workflows and provide the unified control environment required for both humans and AI to operate effectively. Architecture accelerates learning and amplifies capability.

Treat long-term partners as capability multipliers

Cybersecurity has become too complex to be supported by rotating vendors selected primarily on cost. Today's secure enterprise needs partners that can evolve along with it, not ones that are replaced every five years to cut spending.

Long-term partners, both system vendors and cybersecurity consultancies, bring continuity, institutional memory and the ability to co-create and co-deliver. These partnerships must be treated as strategic extensions of the workforce, not interchangeable delivery vendors. When partners remain embedded over time, they accumulate context, evolve with the business and strengthen internal teams rather than displace them. Short-term, cost-driven vendor rotation undermines the capability precisely where organizations need stability and long-term memory. Cybersecurity-as-a-Service becomes a capability platform, extending expertise, accelerating modernization and reinforcing internal teams.

Prioritizing long-term vendor and consulting partnerships preserves continuity and institutional knowledge while unlocking the ability to co-create and deliver.

Activate ecosystem intelligence to close the knowledge and capability gap

As cyber threats evolve faster than any single organization can observe or respond to alone, effective defense increasingly depends on collective intelligence. Leading operating models treat cybersecurity as an ecosystem capability, participating in structured threat-sharing, joint defense collaborations and cross-sector coordination to improve foresight, accelerate learning and align skills development with emerging attacker tradecraft. This collective approach enables organizations to augment internal talent with continuously refreshed, externally sourced knowledge, strengthening resilience without relying solely on private solutions.

Singapore's Cyber Security Agency (CSA) has established several workforce development efforts, in collaboration with Information Sharing and Analysis Centers (ISACs) such as OT-ISAC and industry partners like ISC2 and the SANS Institute, to strengthen the cybersecurity talent pipeline, leveraging professional certifications and training programs to upskill the workforce.[25,26] CSA demonstrates how cross-sector collaboration can build hybrid cyber talent and disseminate workforce development risk across an ecosystem.[27]

Together, these three moves shift cybersecurity from a function that erodes under pressure to a capability that compounds over time. Internal pipelines build sustainability, redesigned roles deepen Conductor-level capability. AI, architecture and partnerships extend human capacity while keeping humans in the lead of decision-making, accountability and risk ownership. Continuous learning from across the broader cyber ecosystem ensures capabilities evolve along with threats and techniques.

Experience is retained, complexity is reduced and capability strengthened with each cycle. The result is a cybersecurity workforce that grows more resilient, coherent and business-aligned year after year.

These three moves shift cybersecurity from a function that erodes under pressure to a capability that compounds over time.

What leaders can do next

Six key decisions separate organizations that build durable cyber capability from those that remain perpetually behind. Leaders who act on these decisions will build a cyber workforce that grows stronger with every disruption.

01 **Shift cybersecurity from an IT function to an enterprise capability**: Shared accountability across business, technology and risk is the precondition for everything else on this list.

02 **Build hybrid talent from within**: The external market cannot supply Conductor-level talent at the speed or scale required. Organizations that wait for the market to solve this will fall behind.

03 **Redesign roles so experienced professionals grow**: With the average tenure dropping to 1.8 years, every career roadblock that limits progression is a drain on institutional knowledge. Career paths must reward breadth and business fluency, not just vertical title movement.

04 **Build a culture that supports individuals and deepens expertise**: One in five cybersecurity professionals is considering leaving the field. Well-being, workload transparency and shared accountability are the structural conditions that allow expertise to compound over time.

05 **Use AI to elevate judgment, not replace learning**: Automation that absorbs foundational work too early produces analysts who cannot reason without a tool. Preserve simulation environments and deliberate learning alongside AI deployment.

06 **Treat partners as capability extensions**: Cost-driven vendor rotation resets institutional knowledge at exactly the moment you need it most. Long-term partners who stay embedded accumulate context, strengthen internal teams and accelerate recovery.

When leaders stop competing for scarce cyber talent and start building it, the benefits will resonate. They'll create faster recovery cycles, stronger regulatory postures and the agility to stay ahead of emerging threats. A strong cybersecurity function builds organizational confidence and customer trust, keeping the organization both protected and thriving.

How Accenture can help

Closing the gap between the cyber workforce organizations have today and the one the business now demands is rarely a hiring problem alone. It requires changes to roles, career paths, learning and leadership, in concert. Our work in this area is organized around three areas of focus.

Talent and workforce. Accenture helps organizations redesign cyber roles, career structures and operating models so professionals develop the business acumen, judgment and cross-functional fluency that hybrid roles now require. AI-powered skills intelligence gives leaders a current view of capability and informs the shift from job-based structures toward skills-based deployment. Because tenure and burnout now shape capability as much as hiring does, we pair structural change with the retention, mobility and culture practices that allow expertise to compound over time.

Learning. Through LearnVantage, we build continuous, role-based development into the flow of work, pairing technical content with the communication, problem-solving and decision-making practice that distinguishes Conductors from Operators.

Cyber leadership. Accenture works with cyber leaders and their teams to operate confidently under regulatory scrutiny, translating technical risk into business decisions and building the cross-functional trust that distributed cyber capability requires. Through executive coaching and leadership development, we help leaders and their organizations work with greater clarity, alignment and purpose.

We work with clients on any one of these, or all three together, depending on where the gap is widest.

About the research

We conducted a cross-regional labor market analysis using one year of Lightcast data (October 2024–October 2025), covering more than 550,000 cybersecurity job postings and professional profiles across Africa, APAC, Europe, the Middle East and North America. We used AI-assisted coding techniques to enhance classification accuracy and streamline data extraction. Roles were classified into strategic and technical based on standardized role definitions and underlying skill requirements. This role-based framework enabled a like-for-like comparison between the capabilities employers are seeking and those currently available in the workforce. Technical cybersecurity roles are predominantly execution-oriented, focused on implementing controls, monitoring threats and operating security systems, and therefore require a higher concentration of core cyber skills. In contrast, strategic cybersecurity roles are closely aligned to enterprise priorities and decision-making. They typically require deeper experience and a balanced combination of technical expertise, strategic judgment, risk oversight and commercial acumen.

Our analysis examined differences in education, certifications, skills and experience across both role types and contrasted these requirements with the actual characteristics of cybersecurity professionals. The analysis found minimal variation in education and experience across roles, enabling a primary focus on skills alignment. To complement the quantitative analysis, we conducted interviews with Accenture's cybersecurity and talent subject matter experts, and AI-augmented research supporting systematic evidence-gathering and synthesis. We use generative AI in our research production process. Our research experts review and validate the generative AI outputs with traditional research methods where possible, applying Accenture's Responsible AI standards.

Note: Job postings often list multiple skills. If a posting requires both Skill A and Skill B, it contributes to the totals for each skill. As a result, the share of postings requiring each skill may exceed 100%, although aggregate skill mentions always sum to 100%.

References

1. **Accenture, Talent Reinventors: Delivering Value with and for People in the Age of AI,** March 16, 2026.
2. **ISACA, State of Cybersecurity 2025, September 29,** 2025.
3. **"World Economic Forum in collaboration with Accenture, Global Cybersecurity Outlook 2026,** January 12, 2026.
4. **CrowdStrike, 2026 Global Threat Report,** 2026.
5. **Cybersecurity Study Programs, arXiv,** February 18, 2025
6. **ISC2, 2025 ISC2 Cybersecurity Workforce Study, December** 4, 2025.
7. **ISACA, State of Cybersecurity 2025, September 29,** 2025.
8. **ISSA & ESG, Cybersecurity Skills Crisis Continues for Fifth Year, Perpetuated by Lack of Business Investment,** July 28, 2021.
9. **Accenture, State of Cyber Resilience 2025,** June 25, 2025.
10. **ITU, Global Cybersecurity Index 2020.**
11. **UNESCO, The Global Education Monitoring Report,** July 27, 2023.
12. **ENISA, CyberHEAD: Cybersecurity Higher Education Database.**
13. **World Economic Forum in collaboration with Accenture, Global Cybersecurity Outlook 2026,** January 12, 2026.
14. **Accenture, State of Cyber Resilience 2025,** June 25, 2025.
15. **A. Babineau and N. Chen, MGM Resorts Is Operational After Cybersecurity Issue, CNN,** September 11, 2023.
16. **Brown & Brown, A Look Back at the MGM and Caesars Incident.**
17. **Cloudflare Snared Internet's Greatest DDoS Threat in Another Record-Breaking Attempt, SDxCentral,** January 2026.
18. **Per Scholas, Per Scholas and JPMorganChase Have Partnered for More Than 20 Years.**
19. **The Role of the Council and the Influence of CyBOK, UK Cyber Security Council, March 2, 2021.**
20. **Exclusive Networks Looking to Address Cybersecurity Talent Shortage With CyberFarm, CRN,** December 2025.
21. **UK Government Security, Government Security Profession Career Framework, accessed** February 26, 2026.
22. **How Google Cloud's Security Team Helps Build Securely, Google Cloud Blog,** May 2025.
23. **Accenture, Talent Reinventors: Delivering value with and for people in the age of AI.** March 16, 2026.
24. **Swimlane, Softcat Overcomes the Cybersecurity Labor Shortage with Swimlane.**
25. **SC2, ISC2 Partners with CSA to Boost Cybersecurity Talent in Singapore,** October 2023.
26. **Cyber Security Agency of Singapore, Singapore Updates Operational Technology Cybersecurity Masterplan,** August 20, 2024.
27. Ibid.

Acknowledgements

The authors would like to acknowledge the following individuals for their contributions to this report.

Contributors: Michael Teichmann

Economic modelling: Carolina Basile

Research Lead: Shachi Jain

Editors: Gargi Chakrabarty

About Accenture

Accenture is a leading solutions and global professional services company that helps the world's leading enterprises reinvent by building their digital core and unleashing the power of AI to create value at speed across the enterprise, bringing together the talent of our approximately 786,000 people, our proprietary assets and platforms and deep ecosystem relationships. Our strategy is to be the reinvention partner of choice for our clients and to be the most AI-enabled, client-focused, great place to work in the world. Through our Reinvention Services we bring together our capabilities across strategy, consulting, technology, operations, Song and Industry X with our deep industry expertise to create and deliver solutions and services for our clients. Our purpose is to deliver on the promise of technology and human ingenuity and we measure our success by the 360° value we create for all our stakeholders. Visit us at **accenture.com**

Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data-science-led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value and deliver on the power of technology and human ingenuity. Visit us at **accenture.com/research**