seemplicity

The 2026 State of the Cybersecurity Workforce Report

Operational strain, skill evolution, and governance challenges in an AI-driven landscape

Table of Contents

The Operational Reality of the AI-Enhanced Threat Landscape 1

Key Findings 1

About the Data & Methodology 2

The Human Cost of Security Operations 3

The Soft Skill Imperative 5

The Cyber Leader of the Future 6

The AI Investment-Enablement Gap 8

The Trust Architecture in AI Systems 9

The Path Toward Sustainable Security Operations 11

The Operational Reality of the AI-Enhanced Threat Landscape

The cybersecurity industry has reached a point of diminishing returns on human effort. AI was expected to ease the burden on already overstretched teams, but the reality reflected in this research tells a different story. This report moves past the hype of AI to focus on the ground-level impact on the workforce.

Based on a survey of cybersecurity leaders across organizations of different sizes and levels of maturity, this report examines how the fundamental nature of the security team is changing. What emerges is a profession that is more committed than ever, yet operating under sustained, systemic strain. This strain increasingly limits teams' ability to improve real security outcomes.

The following sections analyze five critical dimensions of this evolution:

1. **The Human Cost:** Quantifying the "sixth day" of labor and the psychological tax of persistent readiness.
2. **The Competency Shift:** Exploring the rising necessity of interpersonal skills and business alignment over traditional technical silos.
3. **The Future Profile:** Defining the emerging requirement for AI oversight and governance as the primary leadership differentiator.
4. **The Execution Gap:** Identifying the disconnect between robust AI investment and insufficient professional enablement.
5. **The Trust Architecture:** Establishing the requirements for transparency and human-in-the-loop control as the prerequisites for automated defense.

As organizations accelerate their reliance on intelligent systems, the focus must shift from procuring tools to empowering the people who manage them. This report serves as both a diagnostic of the current state of the cybersecurity workforce and a strategic guide for building a more sustainable model of defense.

Key Findings

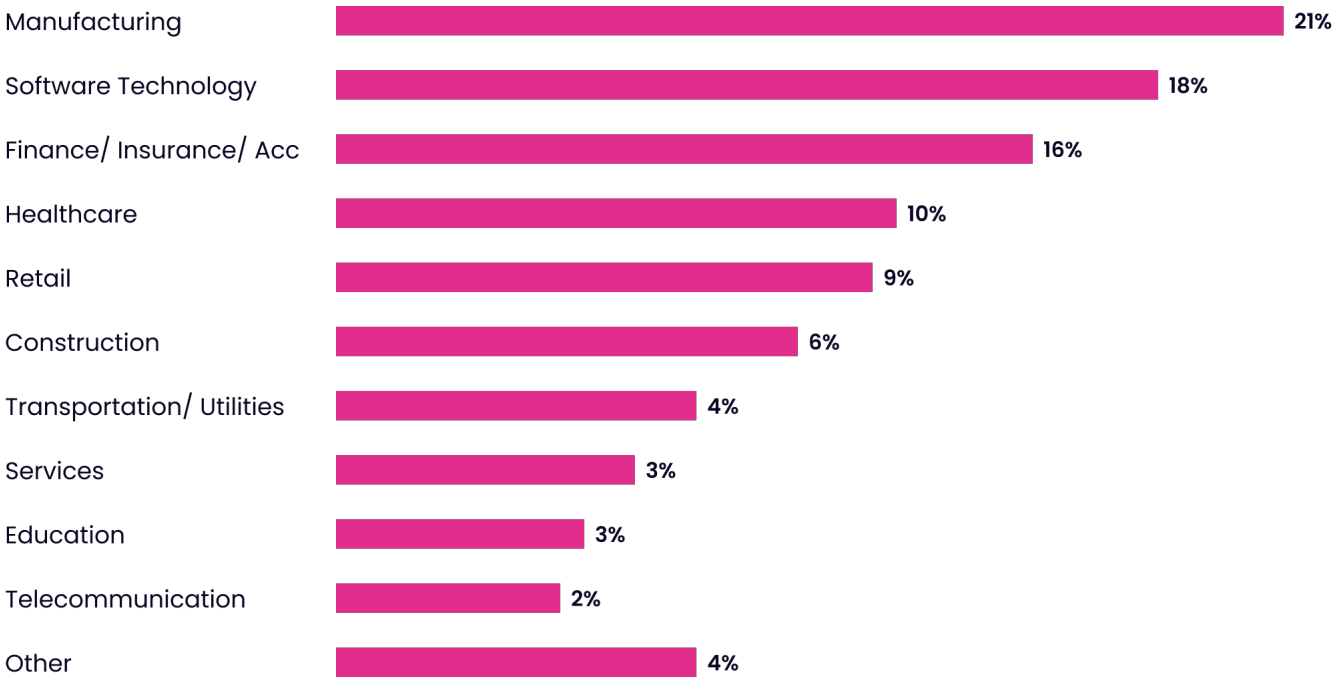
Five critical insights into the current state of the cybersecurity workforce:

1. **Institutionalization of the "Sixth Day:"** Cybersecurity leadership is currently operating on a baseline of persistent overtime. Professionals work an average of 10.8 extra hours per week.
2. **Inversion of Technical vs. Interpersonal Skills:** A definitive shift in professional requirements is underway, with 82% of leaders stating that people skills are more central to their success than they were five years ago.
3. **Emergence of the "Risk Governor" Profile:** AI oversight and governance has overtaken technical engineering as the most important capability for the future professional, cited by 73% of respondents.
4. **Investment-Enablement Gap:** While financial resources are accessible, with 64% of leaders reporting sufficient AI budgets, a significant training deficit exists.
5. **Prerequisites for Automated Trust:** Technical accuracy is no longer the sole requirement for trust. While 62% of leaders prioritize consistent accuracy, over half identify clear accountability and human-override capabilities as essential, followed closely by the need for transparent explanations of AI decisions.

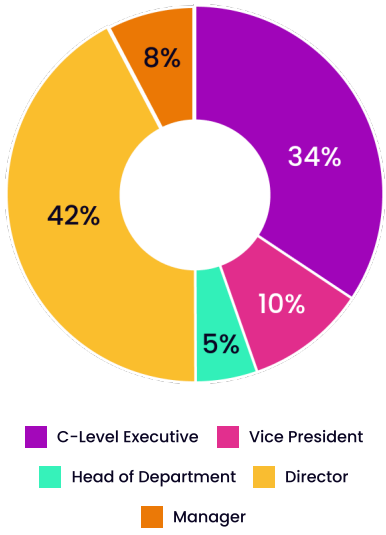
About the Data & Methodology

This report is based on a primary research study by Seemplicity. Seemplicity commissioned research agency Sapio Research to capture responses from 300 cybersecurity and IT professionals based exclusively in the United States. The survey was conducted in January 2026. Percentages shown in charts and tables are rounded for presentation purposes. Consequently, aggregate totals may not equal 100%.

Industry

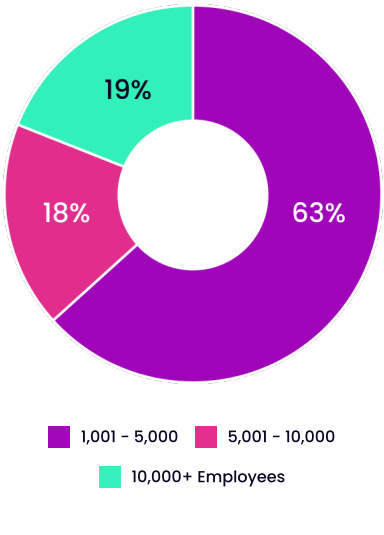


Job Role



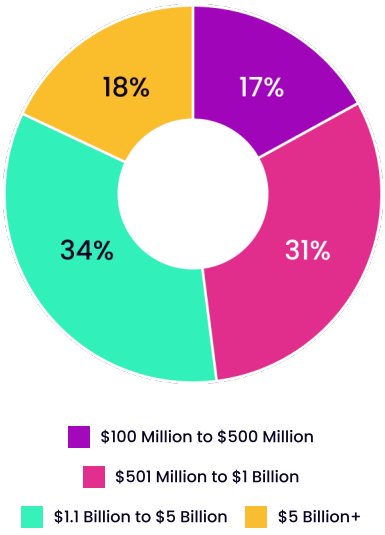
Organization Size

[No.of Employees]



Organization Size

[Annual Revenue]



The Human Cost of Security Operations

The contemporary cybersecurity leadership role has evolved into a high-stakes endurance test. While industry discourse frequently centers on the skills gap, research indicates a more immediate systemic threat: the over-extension of the existing workforce. This section examines the discrepancy between contractual expectations and the operational reality of defending modern digital infrastructure.

The Baseline of Persistent Overtime

Data indicates that cybersecurity professionals are no longer operating within standard business hours. On average, leaders are logging **10.8 extra hours** per week beyond core expectations (Figure 1). This effectively represents a hidden sixth day of labor that has become the foundational requirement for maintaining organizational security posture.

The intensity of this workload is disproportionately high among a significant cohort of respondents. Findings show that 45% of the workforce logs 11+ extra hours weekly, with one in five working more than 16 additional hours. This segment of the workforce is essentially performing the workload of seven days within a five-day work week (Figure 1).

On average, how many hours per week do you work beyond your contracted or expected schedule? Select one

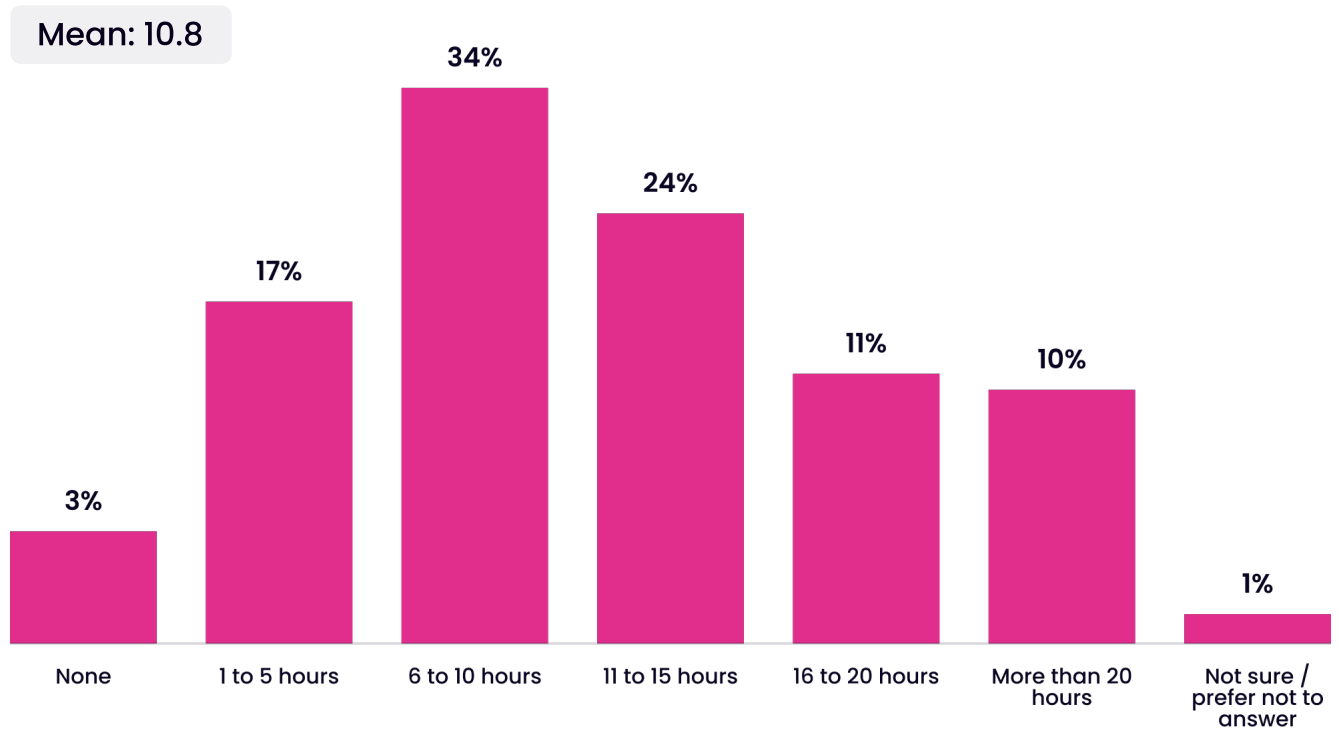


Figure 1: Average weekly overtime volume beyond contracted hours

Psychological and Operational Friction

This sustained level of exertion is now producing measurable psychological and operational strain. Cybersecurity is inherently a high-alert discipline, but current volume requirements are shifting the role from a demanding technical pursuit to a state of perpetual readiness that is increasingly difficult to sustain.

Based on a matrix analysis of workforce sentiment (Figure 2):

- 44% of respondents report that their job feels emotionally exhausting more often than it feels rewarding. Notably, this sentiment is significantly more pronounced at the executive tier, with 56% of C-level respondents reporting this imbalance.
- 43% indicate an inability to take time off without creating a disproportionate amount of stress upon their return, suggesting a lack of redundant coverage or effective delegation structures.
- 32% of the workforce regularly experiences the "Sunday Scaries," characterized by chronic anticipatory anxiety regarding the upcoming work week.

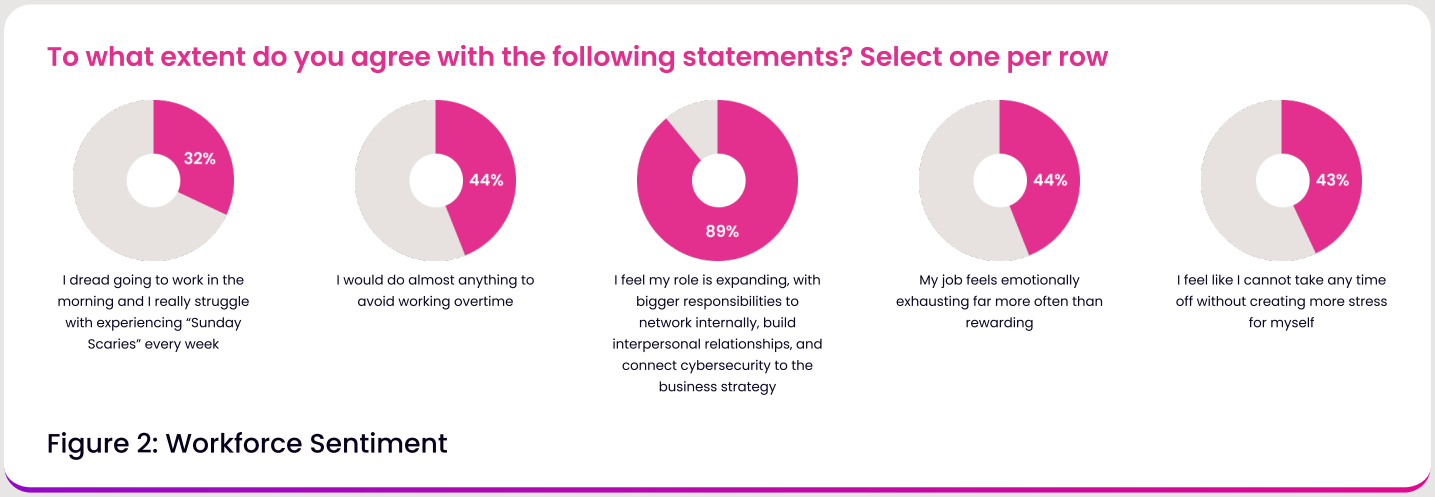


Figure 2: Workforce Sentiment

Systemic Failure vs. Individual Dedication

Despite the documented levels of exhaustion, the data refutes the narrative of a declining interest in the field. In a significant display of professional resilience, 94% of respondents stated they would still choose cybersecurity again as a career (Figure 3).

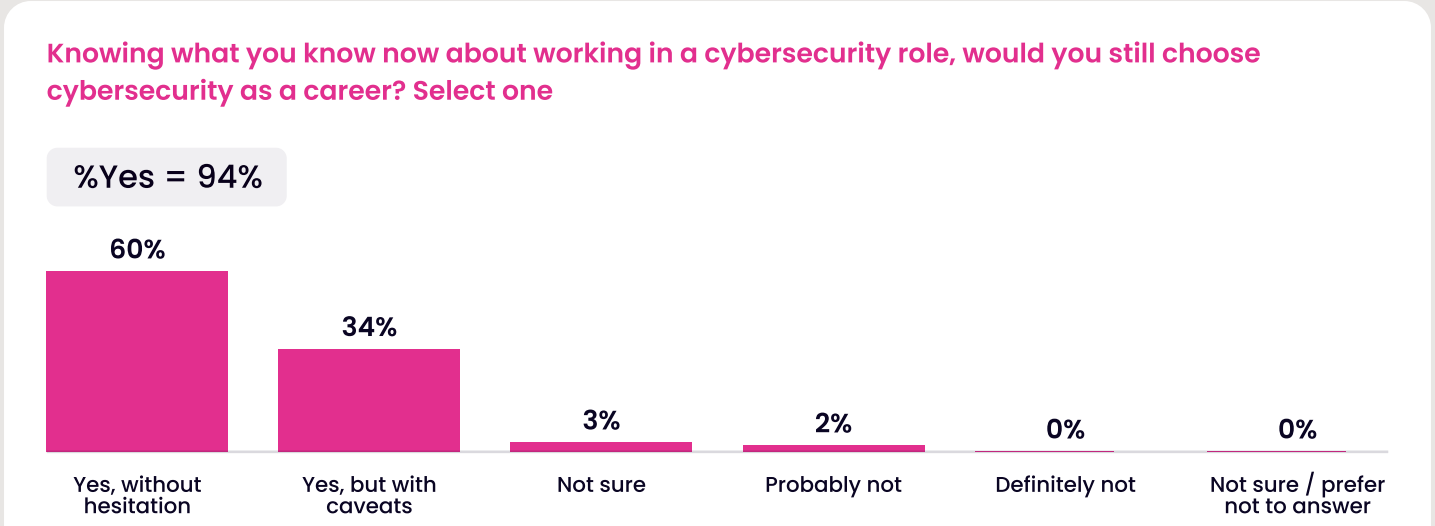


Figure 3: Cybersecurity career re-selection rate

This results in a Resilience Paradox: the workforce is not lacking dedication, but operating within a framework that requires constant overextension to succeed. The burnout observed is not a failure of individual resilience, but a systemic one. Organizations are relying on the personal commitment of their leaders to compensate for gaps in process and an escalating threat landscape.

The Soft Skill Imperative

The operational boundaries of the cybersecurity function are undergoing a fundamental shift. As automation begins to absorb routine technical execution, the role of the cybersecurity leader is expanding into organizational influence and strategic alignment. This transition marks a move away from the isolated technical silo toward a more integrated business leadership model.

Shift Toward Cross-Functional Integration

The data indicates that the modern security role is no longer defined solely by technical defense. An overwhelming 89% of respondents report that their position now requires significant cross-functional collaboration and business alignment (Figure 2). This level of integration suggests that security has moved beyond a peripheral IT concern and has become a core component of the broader business strategy.

AI-Driven Skill Evolution

The integration of AI is creating an immediate mandate for new competencies. The data shows that 85% of leaders feel moderate to significant pressure to strengthen their communication, interpersonal, and business skills as a direct result of AI adoption (Figure 4). This shift suggests that as technical processes become more automated, the human role is increasingly defined by the ability to interpret outputs and manage their organizational implications.

With the rise of AI tools in cybersecurity, do you feel increased pressure for cyber professionals to demonstrate strong interpersonal, communication, and business skills? Select one

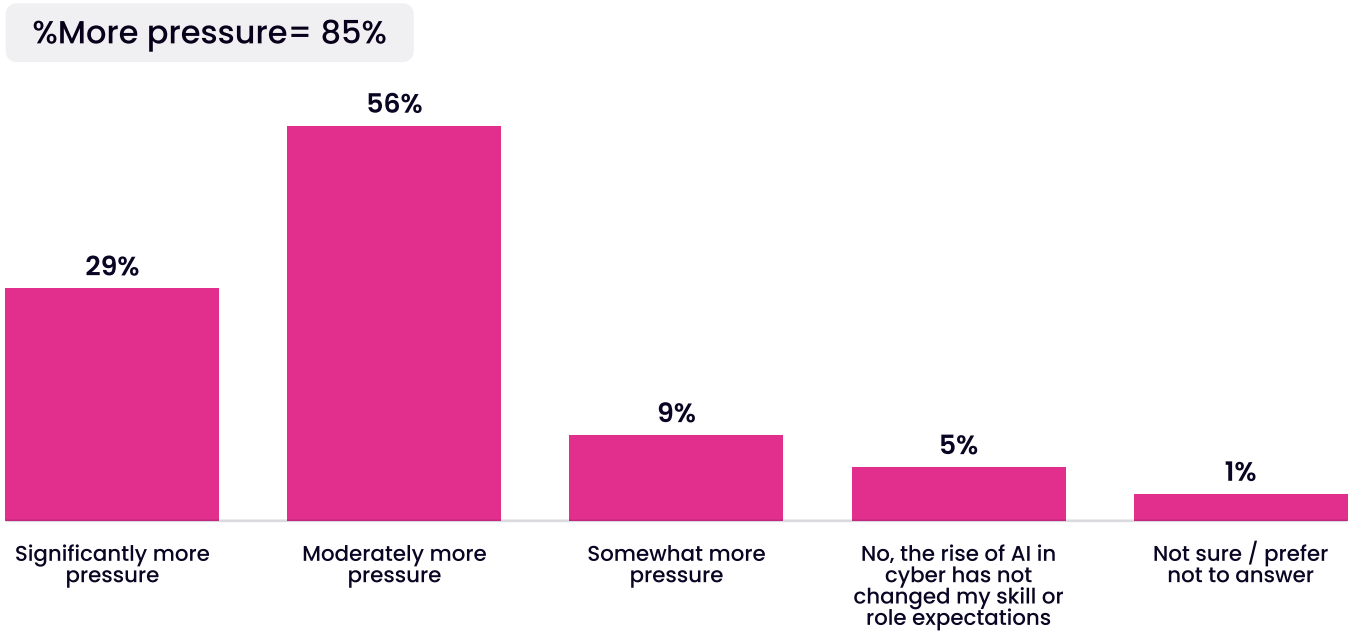


Figure 4: AI-Driven Pressure for Non-Technical Skill Mastery

This AI-specific pressure accelerates a broader professional trajectory. 82% of leaders report that people skills, such as communication and empathy, are more central to their success today than they were five years ago (Figure 5). While the shift toward interpersonal skills predates the current AI surge, the technology is now acting as a primary catalyst for mastery in these non-technical domains.

Interestingly, the perceived importance of people skills scales inversely with organization size: while 75% of leaders in large enterprises (10,000+ employees) identify this shift, the figure rises to 86% among those in smaller enterprises (1,001 to 5,000 employees). This pattern suggests that leaders in smaller environments may face more immediate demands for direct cross-functional influence than their counterparts in larger, more stratified corporations.

Compared to five years ago, how central are people skills (communication, influence, judgment, and stakeholder management) to your effectiveness as a cyber leader today? Select one

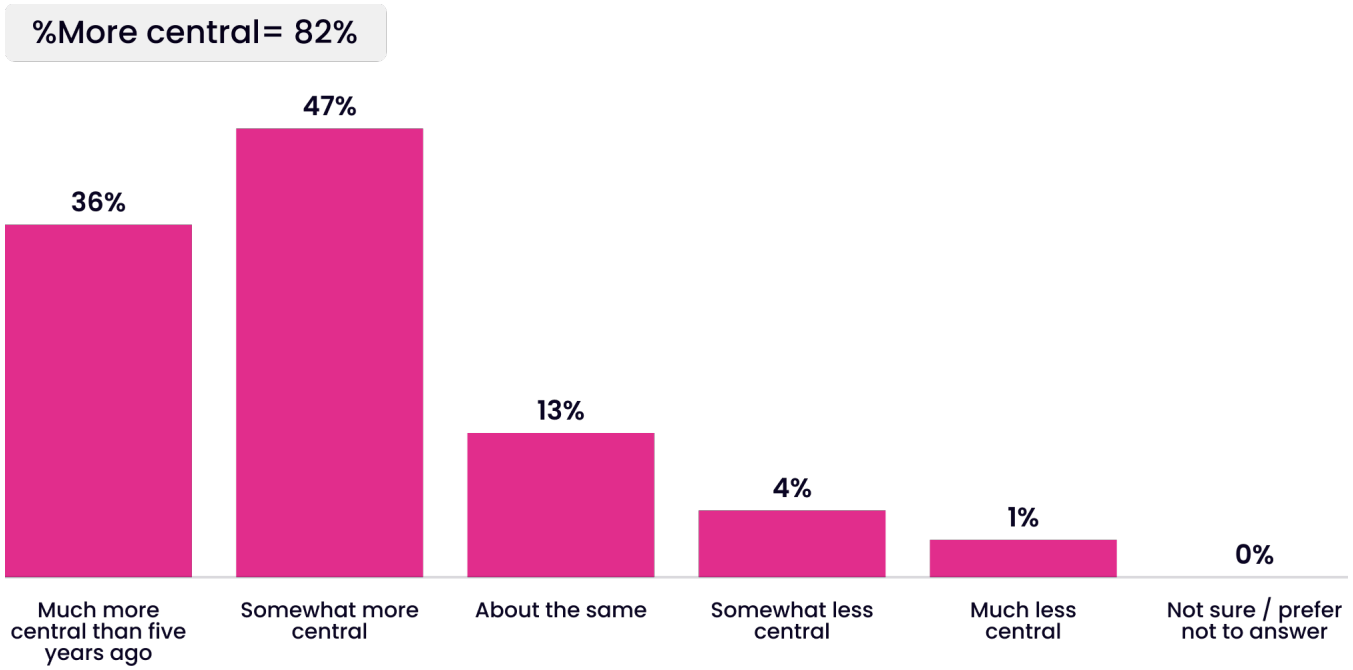


Figure 5: Increased centrality of people skills in leadership effectiveness

From Technical Execution to Strategic Judgment

The findings suggest that the maturity of AI tools is moving the human center of gravity from execution to interpretation. As automated systems generate more outputs and handle more low-level remediation, cybersecurity leaders are increasingly responsible for resolving ambiguity, justifying trade-offs, and translating technical risk into business-relevant terms.

In this new environment, skills previously categorized as secondary have become operational requirements. The data confirms that as the speed and scale of automated decision-making increases, the requirement for human oversight and cross-organizational influence increases. Organizations that fail to adapt to this shift risk creating a governance gap, where automated tools operate without the necessary human-centric guardrails to align them with business goals.

The Cyber Leader of the Future

The evolving requirements for new skill sets and cross-functional integration are fundamentally redefining the profile of the future cybersecurity professional. As organizations move beyond early AI adoption toward sustained integration, the criteria for leadership success are transitioning from manual technical mastery toward high-level system oversight and strategic governance.

Prioritization of System Oversight

While technical proficiency remains a foundational requirement, it is no longer the primary differentiator for future professional success. According to the data, AI oversight and governance is identified by 73% of respondents as the most critical capability shaping the future of the profession (Figure 6).

This indicates a structural shift in the hierarchy of cybersecurity responsibilities. The ability to manage, audit, and secure intelligent systems is now viewed as more vital than traditional technological and engineering prowess, which was cited by 68% of respondents (Figure 6). The findings suggest that the cybersecurity professional is increasingly being redefined as a risk governor responsible for the integrity of automated processes, rather than a practitioner focused solely on manual defense.

Which of the following areas will define the cybersecurity professional of the future most? Select up to three

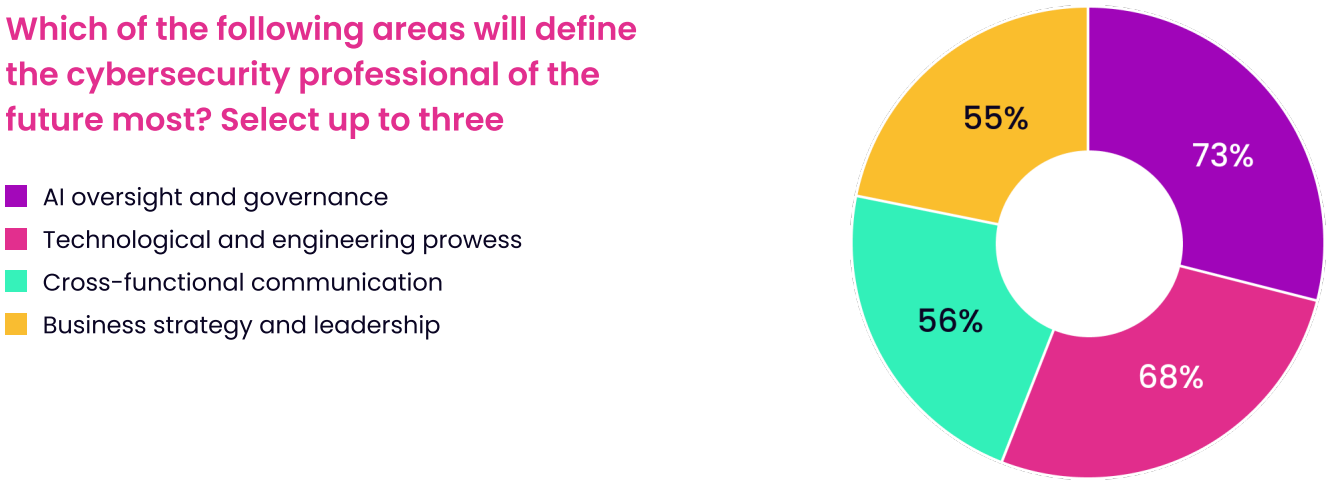


Figure 6: Projected defining capabilities of future cybersecurity leaders

Convergence of Technical and Business Leadership

The data further illustrates a narrowing gap between technical security functions and business operations. A significant share of the respondents now view **c**ross-functional communication (56%) and business strategy and leadership (55%) as defining traits for the next generation of professionals (Figure 6).

The close statistical parity between these two areas emphasizes that the future role is a hybrid model. The modern professional must balance three distinct domains:

1. **Governance:** Ensuring the ethical and secure deployment of AI systems.
2. **Engineering:** Maintaining the underlying technical architecture.
3. **Strategy:** Aligning security decisions and outcomes with broader organizational objectives.

Outcomes-Based Leadership

The shift toward governance and strategy signals a broader change in how cybersecurity value is measured. As AI assumes responsibility for more technical execution, the human professional is responsible for the governing and outcome ownership. This evolution necessitates a shift in how organizations recruit and develop senior security leaders. Roles defined solely by technical depth risk creating a leadership gap in governance and strategic alignment within an AI-driven environment.

The AI Investment-Enablement Gap

As the previous sections established, the cybersecurity professional of the future is increasingly defined by their ability to govern and oversee automated systems. However, for this transition to be successful, organizational investment must extend beyond the procurement of technology to include the development of human proficiency. Current data indicates a significant disconnect between financial allocation for AI tools and the structural support required to use them effectively.

Financial Readiness vs. Operational Capability

There is a clear indication that budgetary constraints are not the primary barrier to AI adoption within security departments. A majority of respondents (64%) report that they currently have sufficient budget for AI features and capabilities (Figure 7). This suggests that at the executive level, there is a recognized mandate to invest in AI as a response to an increasingly complex threat landscape.

Within your organization, does the cybersecurity team have budget available to implement the AI features they need? Select one

- Yes - we have sufficient budget to implement the AI features we need
- Limited - some AI initiatives are funded, but not all needs are covered
- No - budget constraints prevent us from implementing AI features
- Not sure / prefer not to answer

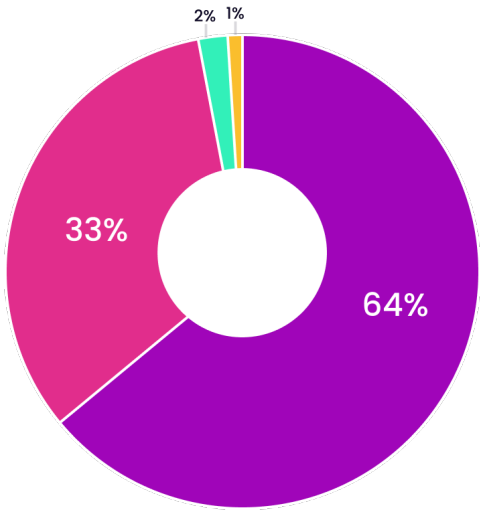


Figure 7: Budget readiness for AI implementation

Notably, this level of financial readiness is most pronounced in smaller organizations; 71% of leaders in smaller enterprises report sufficient funding for AI capabilities, compared to 51% and 54% in mid-sized and large enterprises, respectively. This suggests that smaller organizations may be prioritizing AI investment more aggressively to compensate for leaner headcounts and maximizing resource efficiency.

The Training Deficit in Human-AI Collaboration

Despite this capital investment, there is a clear deficit in the enablement phase of AI adoption. More than half of respondents (52%) describe the training available for effective human and AI collaboration as either limited or insufficient (Figure 8).

This gap creates a high-risk environment where sophisticated tools are deployed without a corresponding increase in the workforce's ability to govern them. And, if leaders are expected to move into roles defined by AI oversight (as identified in Section 3), the lack of specialized training represents a failure to provide the necessary organizational infrastructure required for that transition.

Figure 8: Organizational investment in human-AI collaboration training

Execution Gap: From Investment to Readiness

The discrepancy between financial investment and professional development creates an execution gap. Organizations are deploying AI features, yet the lack of a standardized framework for human-AI collaboration means that the full value of these investments remains unrealized.

This results in a disproportionate burden being placed on the leadership layer. Without formal enablement and clear governance structures, leaders are left to manage the increased complexity and decision-making speed of AI tools through manual oversight. This suggests that many organizations may be conflating financial investment in AI with actual operational readiness. Until investment in human proficiency matches investment in technical features, organizations are more likely to accumulate decision debt and operational friction than realize the efficiency gains promised by AI-powered automation.

The Trust Architecture in AI Systems

For AI to fulfill its potential as an operational force multiplier, it must move beyond technical novelty to earn the trust of the practitioners responsible for its outcomes. The data indicates that trust is not a singular metric, but a multifaceted requirement built on accuracy, transparency, and the preservation of human authority.

Drivers of AI Confidence

Technical performance remains the baseline for trust, but operational safeguards are nearly as critical. 62% of cybersecurity leaders cite consistent, measurable accuracy over time as their primary trust driver (Figure 9). However, accuracy alone is insufficient for professional adoption; it must be accompanied by mechanisms that maintain human control.

The findings show that 54% of leaders require clear accountability and human override controls to trust AI systems, while 53% demand transparent explanations of how decisions are made (Figure 9). These results emphasize that leaders are unwilling to relinquish final judgment to a "black box" system. Furthermore, 53% identify consistent, measurable results and ROI as a key factor, indicating that trust is also tied to the technology's ability to provide tangible relief to the overextended workforce identified earlier in this report.

As a cybersecurity leader, which of the following factors gives you the most confidence to trust AI? Select up to three

- Consistent, measurable accuracy over time
- Clear accountability and human override controls
- Transparent explanations of how decisions are made
- Consistent, measurable results and ROI
- Proven security and data protection practices
- None - I don't trust AI

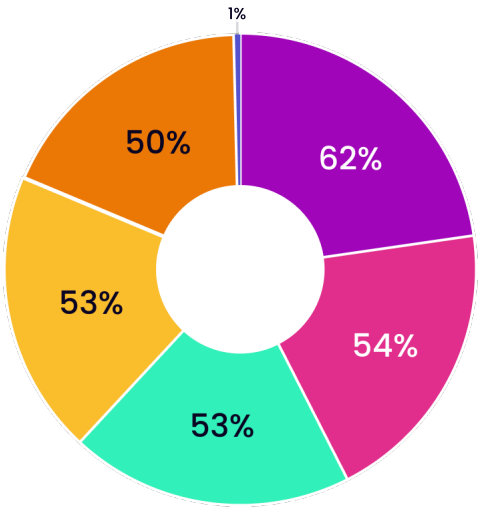


Figure 9: Drivers of professional trust in AI

Internal-External Trust Gap

The requirement for control and visibility is further reflected in how leaders perceive different sources of AI implementation. There is a measurable preference for internal over external AI deployment (Figure 10):

- 87% of respondents express complete or high levels of trust in their internal teams to use AI responsibly.
- 77% express the same level of trust in cybersecurity vendors.

This 10-point discrepancy suggests that trust is intrinsically linked to proximity and oversight. Leaders naturally favor internal teams where they have greater visibility into training protocols and governance frameworks. Conversely, the lower trust in vendors highlights a skepticism toward third-party systems where the logic of the AI and the ability to audit or override its decisions may be less accessible.

How much do you trust each of the following to use AI responsibly? Select one per row

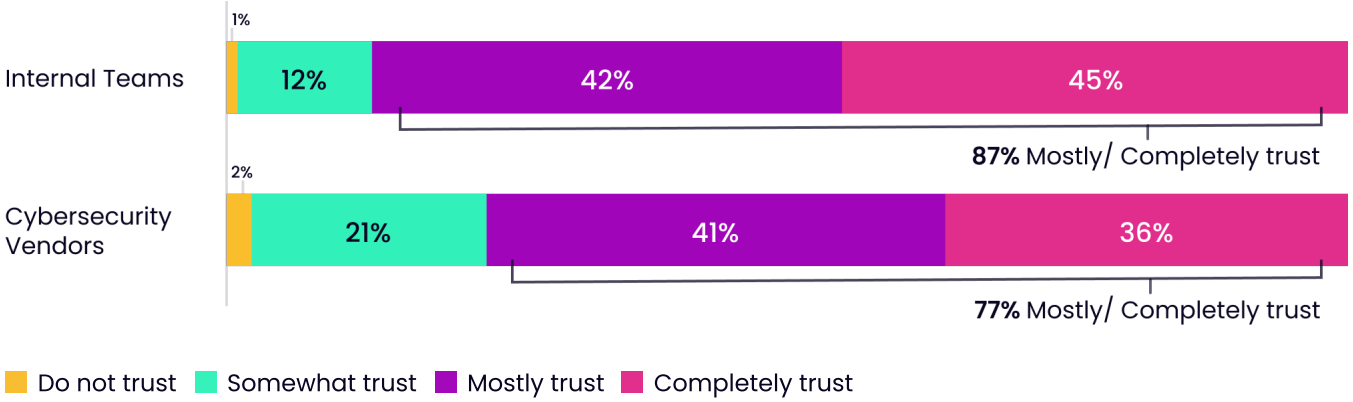


Figure 10: Trust in Responsible AI Usage: Internal vs. Vendors

Trust as a Product of Governance

The data confirms that for cybersecurity leaders, AI does not eliminate accountability; it redistributes it. As systems become more inference-driven, the burden of judgment, override, and explanation falls on the human leader.

When these systems lack transparency or clear lines of ownership, automation ceases to be a solution and instead becomes a new source of operational risk. To bridge the trust gap – particularly with external vendors – organizations and providers must prioritize explainability and human-in-the-loop safeguards. Trust will only be fully realized when leaders feel they are governing the technology, rather than being held responsible for outcomes they cannot fully see or control.

The Path Toward Sustainable Security Operations

The findings of this research present a clear mandate for the next phase of cybersecurity evolution. While the industry has successfully navigated the initial technical adoption of AI, it has yet to reconcile the human and operational costs associated with this transition. The disconnect identified in this report – where 94% of a significantly overextended workforce remains committed to the field despite chronic burnout – reveals a system currently sustained more by individual willpower rather than operational efficiency.

The path forward requires a shift from viewing AI solely as a tool for technical execution to recognizing it as a framework for strategic governance. Our research highlights three critical areas for organizational focus:

- **Closing the Enablement Gap:** Organizations must match their financial investment in AI with a corresponding investment in human-AI collaboration training. Without this, the technology risks pushing the burden of judgment and accountability disproportionately onto security leaders.
- **Formalizing Governance and Oversight:** As AI oversight becomes the defining capability of the future cybersecurity leader, organizations must establish clear accountability structures and human-override protocols to bridge the trust gap.
- **Operationalizing Ownership:** Reducing the hidden sixth day of labor requires moving away from manual, intervention-heavy security models. Efficiency will not come from automation alone, but from the ability to automate prioritization and decision-making clarity.

In summary, the future of the cybersecurity workforce is not a choice between human expertise and automated intelligence, but a requirement for a new model of integrated leadership. To ensure the long-term sustainability of the workforce, the focus must now shift toward providing leaders with the governance structures, transparency, and professional enablement necessary to operate effectively in an AI-driven environment. The objective is no longer just to defend the enterprise, but to build security operations that are as resilient as the people who lead them.