The Shift to Continuous Cybersecurity Micro-Training

How security leaders are rethinking hiring, onboarding, and the way their teams stay ready to tackle emerging threats.

skillbit
CYBERBAY
PROTECTING OUR DIGITAL BORDERS
BELLINI CAPITAL

What security leaders told us

70% of organizations have **few roles available to candidates with under two years of experience**.

57% report a **six-month time-to-value**, while most view three months as the target.

71% prefer **20-minute weekly upskilling sessions** over lengthy annual training.

67% prioritize **foundational problem-solving** over mastery of a specific technology stack.

??? Readiness measurement remains inconsistent: leaders rely on **subjective indicators** rather than standardized, objective performance data.

Bellini Capital and CyberBay have commissioned a comprehensive research study to analyze the training and development landscape within professional cybersecurity departments. Data collected from over 200 senior executives highlights growing demand for microlearning (20-minute, digestible learning segments) to bridge the gap between hiring and full productivity, combat skill decay, build problem-solving skills, and provide objective data senior leaders can use to optimize workforce management.

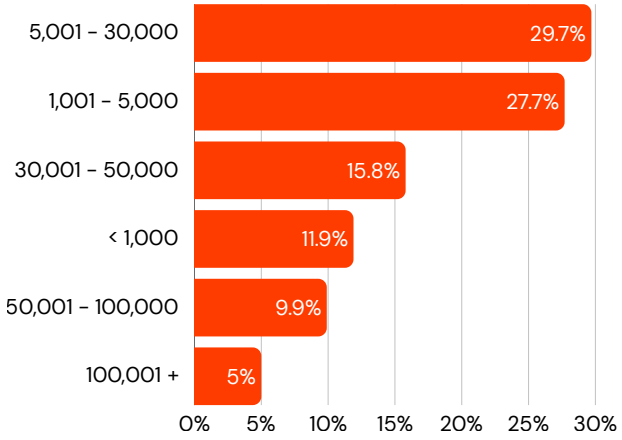
Research methodology and market scope

The survey results, which were collected via a combination of email and telere-search, are statistically significant with an 85% confidence level and a 5% margin of error. Summary specifications are shown below:

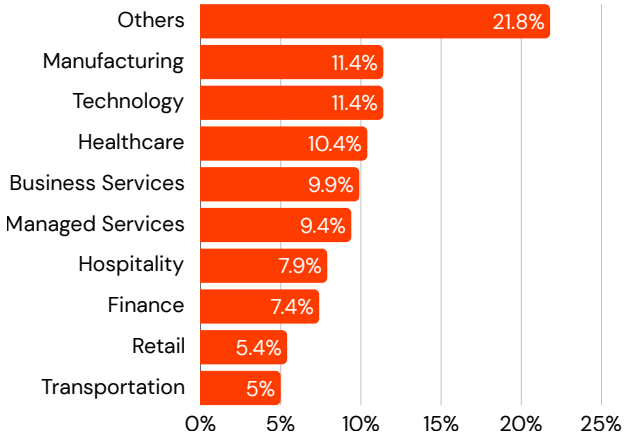
Metric	Details
Total Responses	202 high-level decision-makers (CISOs, CIOs, and VPs of Security Engineering)
Statistical Validity	85% Confidence Level with a 5% Margin of Error
Enterprise Focus	>88% of respondents classified as enterprise-sized organizations (greater than 1,000 employees)
Top Industries	A wide variety of Industries are represented including Technology, Manufacturing, Healthcare, Business Services, Finance, MSPs, and many more. North America only.
Cybersecurity Staffing	>60% have 10+ cyber professionals. A full range is represented as reflected in the chart below.

The research targeted high-level decision-makers, including CISOs, CIOs, and VPs of Security Engineering. These respondents show evidence of being highly intentional regarding the development of their people, with over 80% having utilized their entire 2025 training budgets. Their executive perspective reveals that challenges in the talent development process begin well before the prospective new hire becomes part of the security operations; it starts with a widely shared obstacle, across the surveyed executives, in the junior talent pipeline.

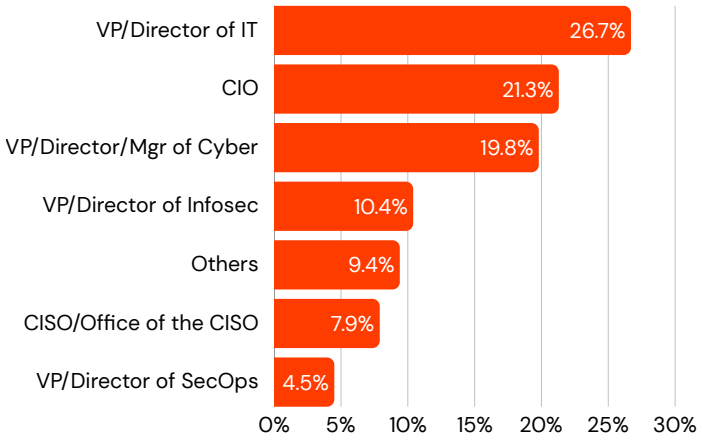
ORGANIZATION SIZE



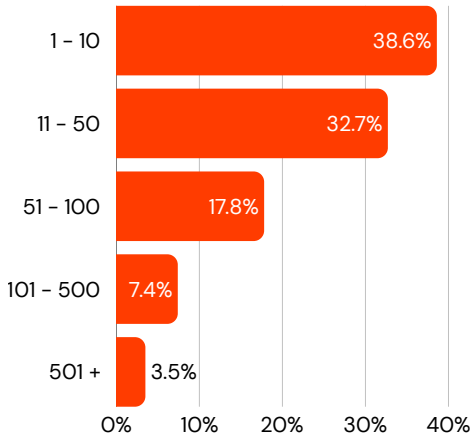
INDUSTRY



JOB FUNCTION



CYBERSECURITY PROS AT ORG.



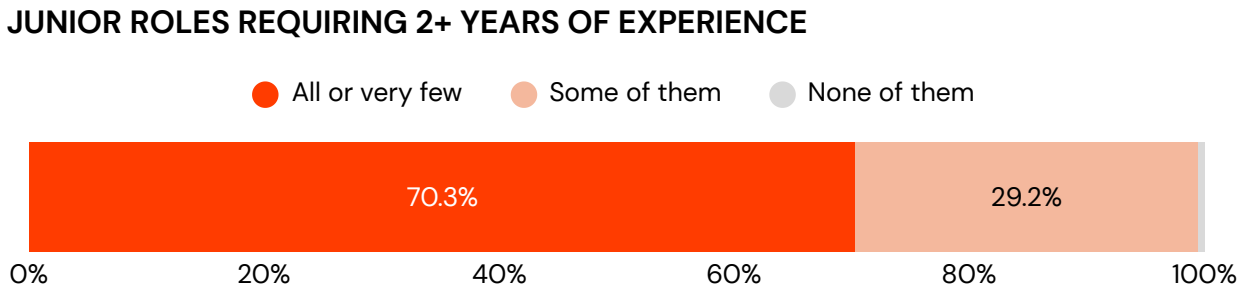
Rethinking the junior talent pipeline

A resume/credential barrier currently restricts the flow of talent into the cybersecurity ecosystem, creating a bottleneck that hinders organizational effectiveness. Companies face an “Experience Paradox”: they need new talent, yet hiring standards create an obstacle.

The Experience Barrier

A need for significant “prior experience” has created a self-imposed talent shortage:

70% of organizations have no junior roles, or very few, that they can fill with candidates having less than two years of experience.



A Potential Shift Toward Simulation

To wrestle with this, cybersecurity leaders are becoming open to the idea of changing the strict 2+ years' experience criterion. 30% of leaders are receptive to “Interactive Lab” formats as a credential substitute, and another 49.5% are open to it if presented with convincing evidence of its effectiveness. By replacing static resumes with interactive challenges, executives can validate a candidate’s ability to perform in a live environment, effectively widening the candidate pipeline without lowering the bar for excellence.

Identifying productivity leaks

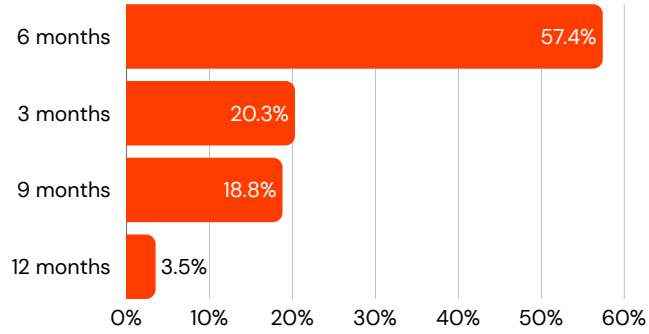
Time-to-Value is a critical metric in workforce strategy, yet our survey shows it remains largely unoptimized. Closing the gap between a new hire's "Day 1" and their point of full proficiency is a financial and readiness boon for the organization.

Expectations vs. reality: the financial leak

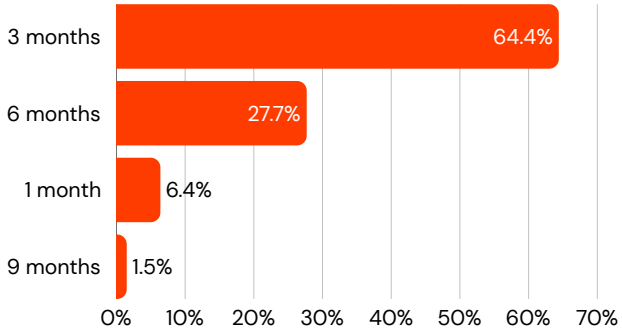
The data highlights a significant lag in reaching operational proficiency that creates a "hidden risk" period:

- **Actual TTV:** 57% of executives report an average TTV of 6 months.
- **Acceptable TTV:** 64% of executives view 3 months as being acceptable.
- **The Delta:** Irrespective of what the executives experience for Actual TTV, 64% are seeing a minimum 3-month lag in Actual versus Acceptable. This creates a prolonged window of vulnerability for the organization.

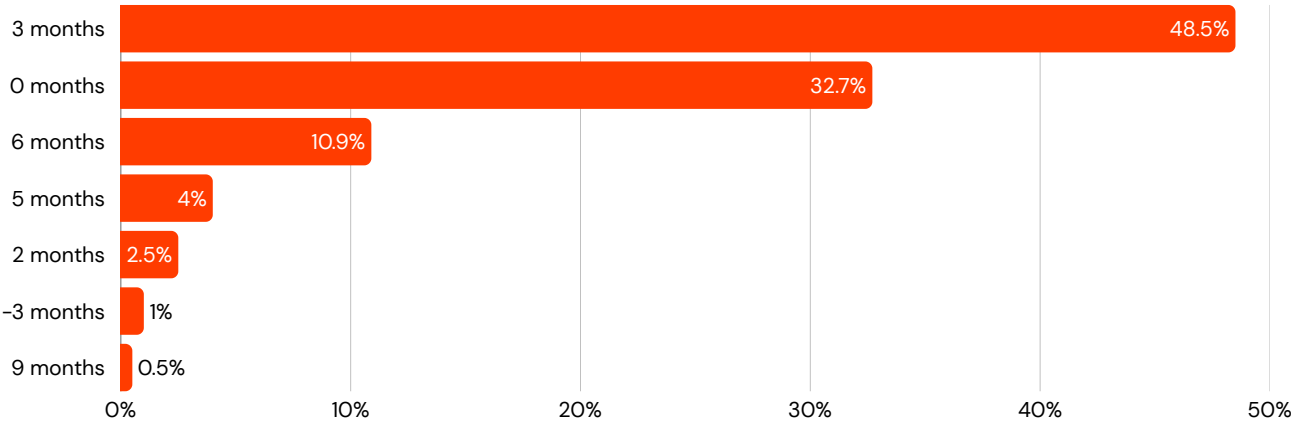
AVERAGE TTV



ACCEPTABLE TTV



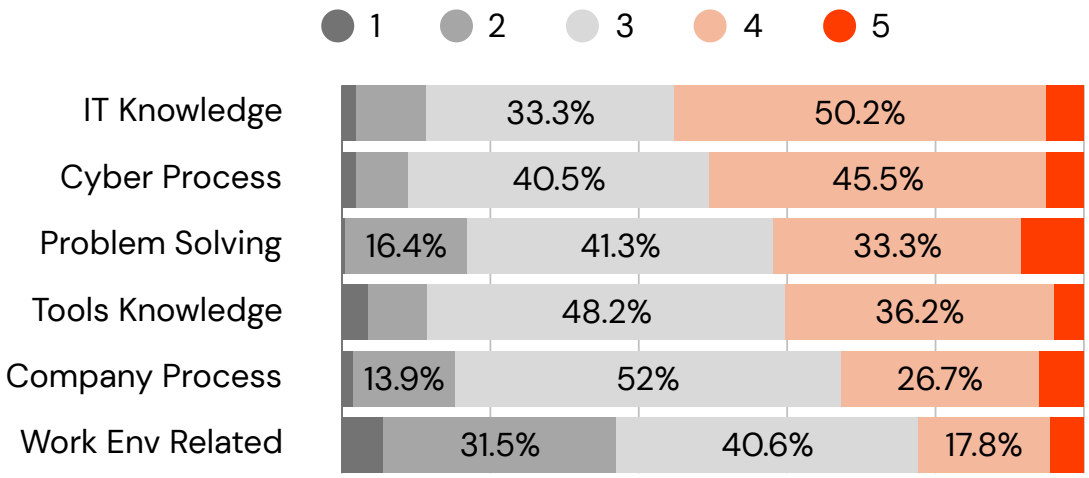
DELTA: TTV MINUS ACCEPTABLE TTV



The primary drivers of TTV delay are foundational, not tool-specific. General IT Knowledge (55%) and Cybersecurity Processes (50%) are cited as the most significant issues. This suggests organizations may be hiring for tool expertise while overlooking broader IT and cybersecurity insights that are hard to assess with today's hiring inputs.

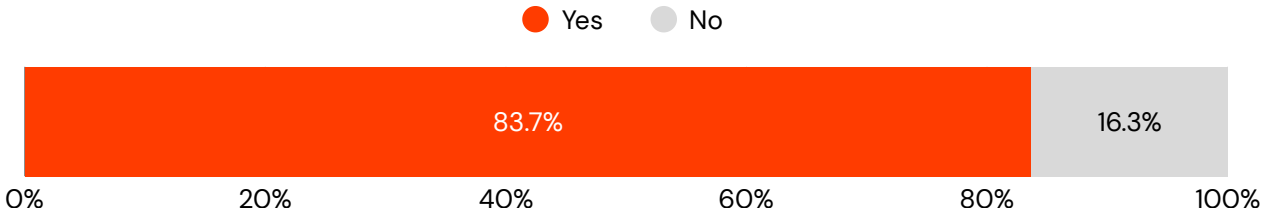
REASONS FOR DELAYS IN TIME TO VALUE

Significance of Issue Rated from 1 - Not particularly Significant to 5 - Very Significant

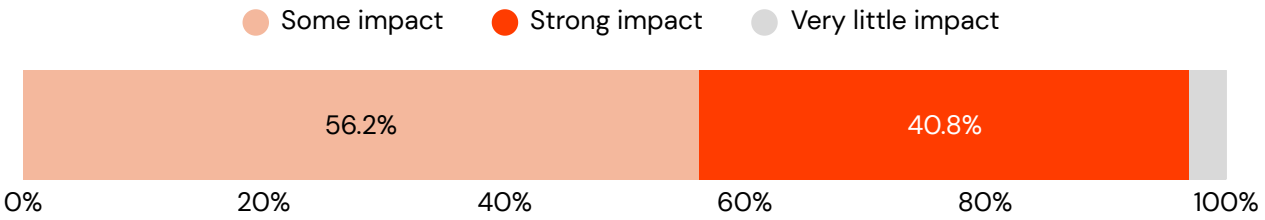


Respondents overwhelmingly (84%) sponsor “Certification” training for their staff, with Vendor Certifications, CISSP, CompTIA Security+, and CCSP as the leading choices in the certification category. Moreover, over 96% report at least some positive impact on staff effectiveness. A significant subset of that number, 41%, claim “Strong Impact”. This suggests that certifications play an important role in developing cybersecurity staff. While the survey did not ask about this, we can also assume certifications matter as a resume builder for individual staff members.

SPONSOR CERTIFICATIONS TRAINING?

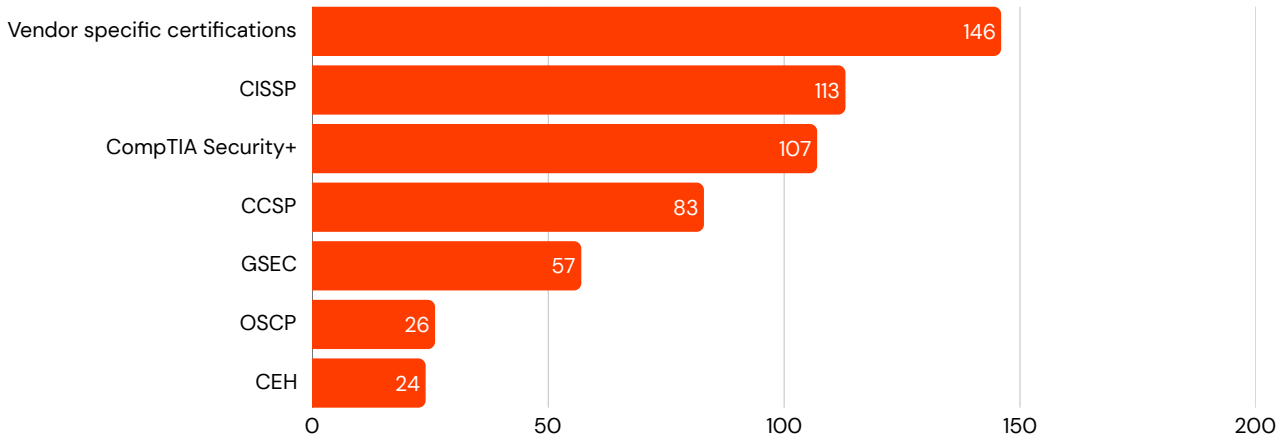


CERTIFICATION IMPACT ON STAFF EFFECTIVENESS



MOST IMPORTANT CERTIFICATIONS

No. of mentions by respondents



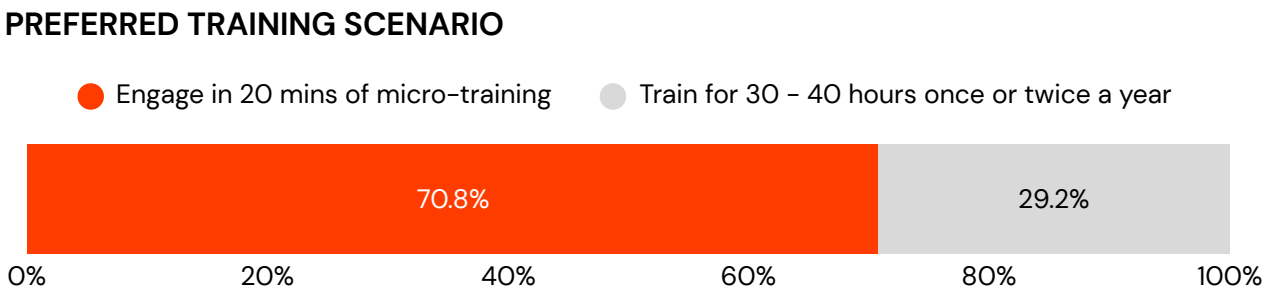
Nevertheless, this data is somewhat at odds with the finding that 71% would prefer training delivered in 20 minutes once a week in an online/interactive format rather than training that requires 30 to 40 hours of commitment once or twice a year.

One potential inference is that certifications are important and useful, even when delivered in a less-than-ideal format. Training that addresses areas certifications don't easily reach, if delivered in a more "snackable" way, could gain favor with executives.

The "snackable" training model

Surveyed executives responded well to a model that integrates training into the daily workflow rather than treating it as a massive annual disruption.

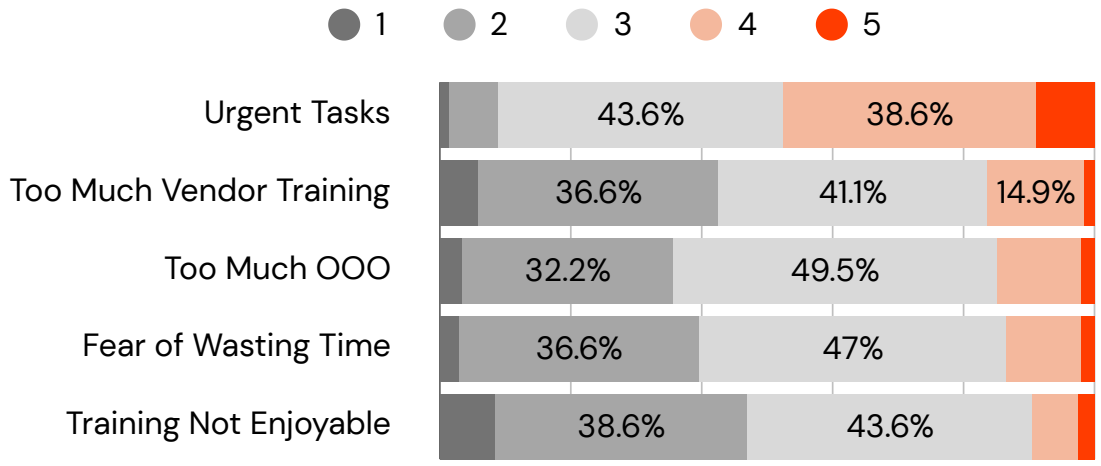
The Preferred Scenario: 71% of executives would prefer 20-minute weekly learning sessions over intensive annual blocks.



The "Urgent Task" Barrier: 47.5% of executives cite daily fires as the primary reason training goals are missed. Micro-learning—the "snackable" model—fits the "rhythm of the business." It lets staff sharpen skills in high-relevance, 20-minute chunks, ensuring professional development survives the "Urgent Task" conflict.

REASONS FOR MISSING DEVELOPMENT GOALS

Significance of Issue Rated from 1 - Not particularly Significant to 5 - Very Significant

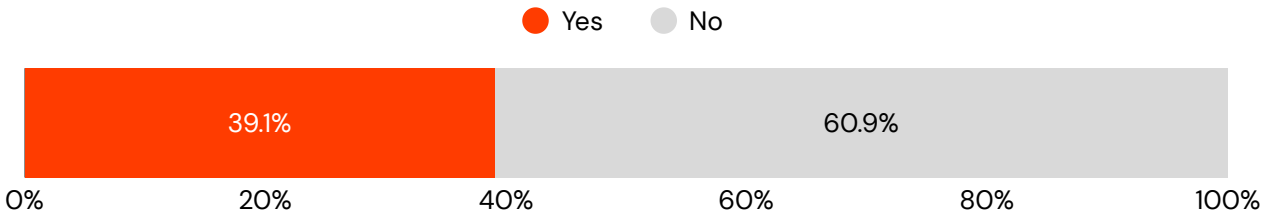


Decay scales with headcount

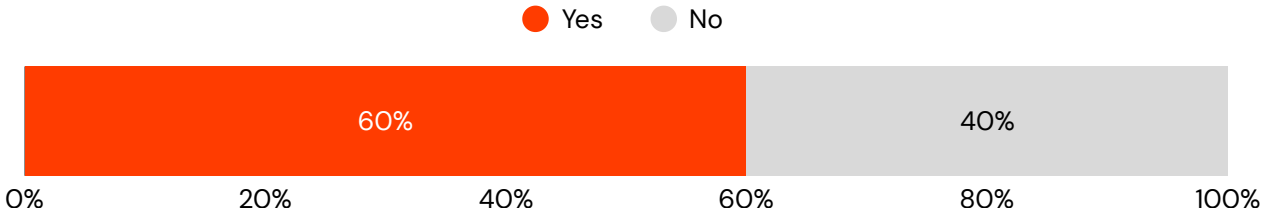
As the pace of technology quickens, largely driven by AI, more and more cybersecurity executives are seeing "skills decay" among their employees. 39% cite skills decay as a problem. The decay issue is more acute with larger companies, however. Among organizations with 50,000 employees or more, 60% cite skills decay as a problem.

DOES YOUR STAFF EXPERIENCE SKILL DECAY DUE TO RAPID INTRODUCTION OF NEW TOOLS AND TECHNOLOGY?

ALL COMPANIES



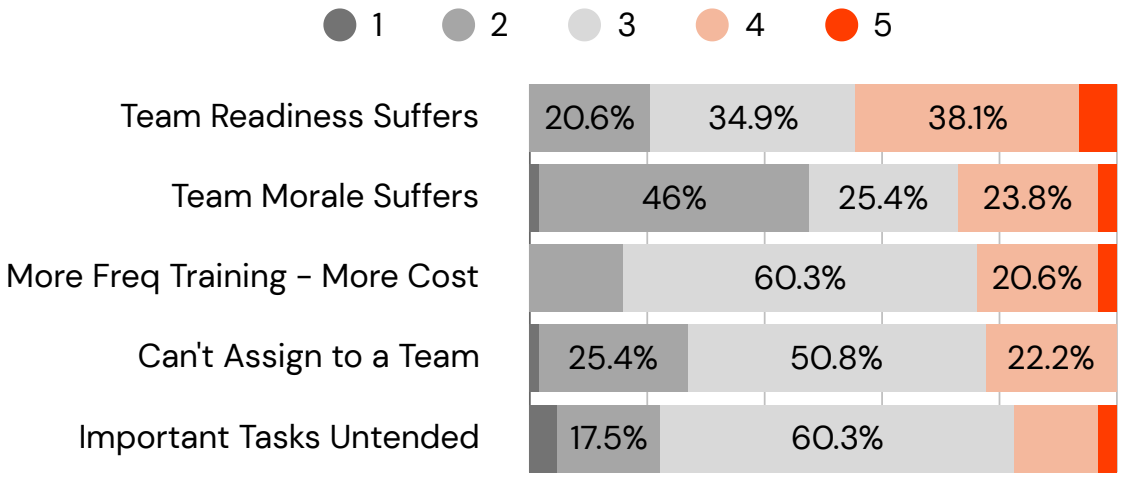
COMPANIES WITH 50,000+ EMPLOYEES



For those who answered “Yes” to the Skills Decay question, the vast majority (75%) say this causes “moderate irritation” (as opposed to minor or substantial irritation). That irritation stems from Team Readiness. It tends to suffer. Team Readiness ranked first (based on a combination of 4s and 5s ratings) among choices that included “Team Morale Suffers”, “More Frequent Training - More Cost”, “Can’t Assign to a Team”, and “Important Tasks Untended”. 44% of executives rated Team Readiness a 4 or 5.

WHAT IS THE IMPACT OF THAT IRRITATION?

Significance of Issue Rated from 1 - Not particularly Significant to 5 - Very Significant



Problem-solving vs. tool mastery

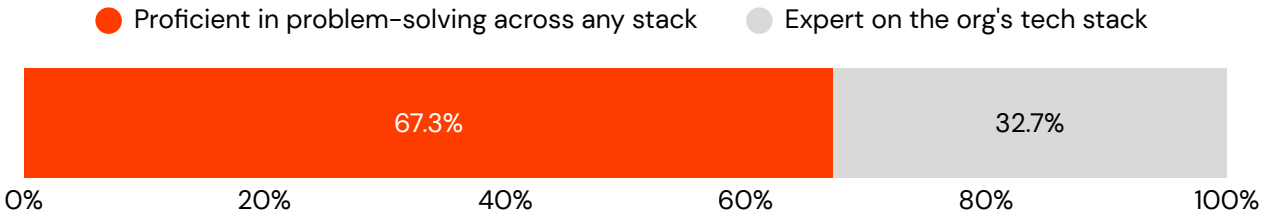
High performance in cybersecurity means shifting from tool-specific knowledge to foundational problem-solving.

The car technician analogy

Consider a car technician: A "certified tool expert" knows how to read the output of a specific brand's diagnostic computer. However, a "Star" understands the engine's internal workings and the systems around it. If the tool changes, the expert is lost; the Star, however, applies foundational logic to any vehicle. The data supports this in the context of cybersecurity:

67.3% of respondents prioritized "Foundational Problem-Solving" over "Stack Expertise" (32.7%).

BETTER TO BE A STACK EXPERT OR PROFICIENT IN FOUNDATIONAL PROBLEM-SOLVING ACROSS ANY STACK?

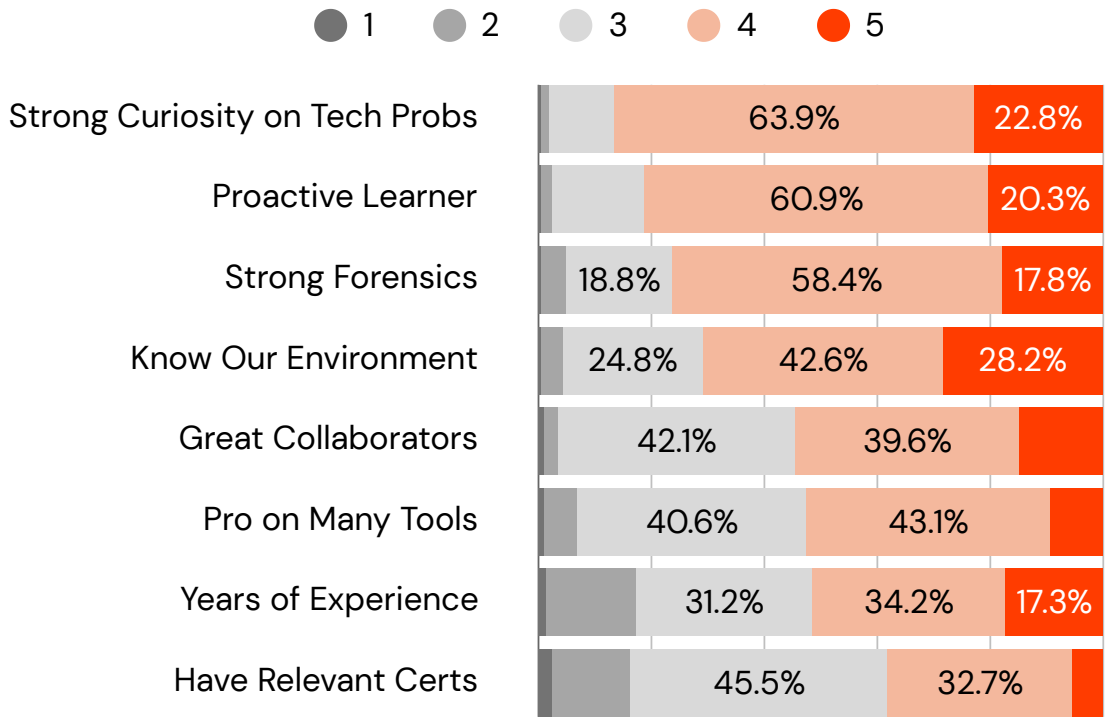


Executives prioritize analysts and thinkers who possess:

1. **Strong Curiosity** in solving technical problems.
2. **Proactive Learning** habits.
3. **Strong Forensics** capability.
4. **Deep Knowledge** of the Environment (understanding the specific organizational context).

KEY CHARACTERISTICS OF THE ORGANIZATION'S STARS

Significance of Issue Rated from 1 - Not particularly Significant to 5 - Very Significant



Confidence vs. data-based insights

The survey also asked whether executives felt they were being well served with data-based insights on their teams. When asked, "How do you rate your current ability to provide objective data that validates team readiness?" nearly everyone expressed some confidence. 59% claim to be somewhat confident and 37% claim to be extremely confident. We then asked, "What is your confidence level in being able to identify high-potential individuals for specialized roles?" The responses varied only marginally from the previous question. 65% said they were somewhat confident, and 33% said they were extremely confident. We know that having objective data on their people is important to them, as 100% responded that it is either somewhat useful or very useful, and we can infer, from their confidence responses, that they are **not experiencing a gap in "talent insight" that rises to the level of an issue for them.**

No clear readiness standard exists

However, in analyzing the verbatim responses to the question, "When reporting to the Board on the readiness of your organization, please provide any insight you can on what information you rely on", it is clear that the information the executives rely on varies broadly from company to company, is often subjective, and that there is a clear gap in the industry with respect to defining a "readiness standard".

Verbatim responses regarding Board reporting mention "personal observation," "trust," and "anecdotal notes." One executive noted, **"Board tends to not want a full update unless something has happened."** Currently, most reporting is a patchwork of audit results, performance reviews, and certification counts that may not reflect the team's ability to stop a live breach.

The mandate for continuous readiness

The study supports the idea that modern cybersecurity leaders should embrace **continuous readiness**. The need to onboard new talent quickly, close the skills-decay gap, overcome the “Urgent Tasks” barrier to meeting development goals, and cultivate problem-solving skills that transcend any specific set of tools speaks to the benefits of “micro-learning.” By adopting a “snackable” model—the 20-minute rule—organizations can integrate skill development into the operational flow. This study points to a future where cybersecurity workforce development will not be measured by the number of certifications on a wall, but by objective, real-time data that proves a team is ready for today's and tomorrow's threats.

Bellini Capital conducted this survey to advance CyberBay's workforce development efforts. SkillBit provided guidance on key micro-training areas of inquiry.