The ROI of Resilience

HOW CYBERSECURITY TALENT MANAGEMENT BEST PRACTICES IMPROVE THE BOTTOM LINE

March 2026

Women in Cybersecurity WiCyS

FourOne Insights

Executive Summary

The cybersecurity workforce is being reshaped by two converging forces: rapid digitization and long-term demographic constraints. New technologies, expanding regulatory expectations, and deeper integration between cyber and core business functions are raising the bar for what organizations expect from their cyber teams. At the same time, an aging population, lower birth and immigration rates, and falling labor force participation are tightening the overall supply of talent. In this environment, pathways into cybersecurity and into leadership roles remain narrow and opaque, especially for women. That leaves the field structurally fragile at the very moment when resilience matters most.

This report examines how employers can widen those pathways and strengthen workforce resilience by focusing on skills-based, talent-friendly practices and by leveraging third-party partnerships to reduce implementation barriers. Our analysis shows that the most effective practices deliver measurable financial returns, improve advancement for underrepresented talent, and are often underutilized today.

Approach

The study integrates three sources of evidence:

Employer survey

Cybersecurity employers and human resources (HR) leaders across the Women in CyberSecurity (WiCyS) community were surveyed on their personal and organizational experiences with specific talent practices.

Organizational analysis

Survey responses were aggregated quantitatively and complemented with qualitative interviews that show how firms operationalize advancement, identify emerging talent, and use external partners to improve outcomes.

Market data

Company-level data from Lightcast, including job postings and professional career histories, were used to examine hiring and talent outcomes such as time to fill, hiring costs, tenure, retention, and women's representation in cybersecurity leadership.

These three data sources were combined to identify the specific talent practices firms employ, and connect them to the talent outcomes they produce.

HOW WE ESTIMATE ROI

We estimate return on investment (ROI) for specific talent practices using a proprietary analytic approach developed by FourOne Insights, grounded in transparent assumptions and publicly-describable inputs. In brief, we link specific talent practices to observed differences in time to fill and average tenure, then translate those differences into conservative estimates of productivity loss avoided.

Unless otherwise noted, results presented in this study are calculated using this methodology.

Key Findings

Skills-based, talent-friendly practices generate the highest returns.

Practices grounded in clear skill expectations, worker empowerment, and reliable data consistently reduce hiring difficulty and extend employee tenure. The highest-impact practices include using skills analytics for workforce planning, offering personalized learning pathways, and creating structured opportunities for individuals to build new capabilities — such as mentorships and stretch assignments. Across a worker's tenure, these practices can return more than $125,000, primarily through faster hiring and improved retention.

These practices benefit the entire workforce and are especially valuable for women.

Panels for promotion decisions, internal skills profiles, and formal mentorship programs all correlate with significantly higher representation of women in cybersecurity management roles. Organizations using these practices see 10–20 percent higher representation of women in cybersecurity leadership than firms that do not. Skills-based promotion criteria and linking incentives to demonstrated skill growth further strengthen both equity and financial performance.

Despite the value of skills-based, talent-friendly practices, adoption is uneven.

Despite the mutual benefit to employers and employees, many high-impact practices are among the least utilized. None of the highest-value practices are leveraged by more than 55 percent of firms. When companies do implement these practices, they often base them on unreliable, subjective data. This threatens worse talent outcomes for organizations, while limiting career development opportunities for individuals.

Third-party partnerships expand capacity and ease adoption.

Membership organizations like WiCyS play an essential role in strengthening both individual and organizational outcomes. Nearly eight in ten respondents find access to such organizations very valuable, and most say they provide stronger professional networks than their employers. Firms that offer this access fill roles 16 percent faster, retain workers longer, and avoid significant productivity losses. These partnerships provide capabilities such as peer learning, industry context, and trusted communities that are difficult for employers to build internally.

Best Practices

The organizations achieving the strongest talent and business outcomes share a common approach: they ground their strategies in objective skills data and align top-down leadership actions with bottom-up employee development opportunities. High-ROI practices, such as transparent promotion processes, executive sponsorship, access to upskilling and mentorship, and engagement with trusted third-party partners, can consistently reduce hiring friction and support retention. Over time, they open advancement pathways that have historically been narrow, especially for women.

These practices are most effective when embedded within an iterative framework: assessing workforce pain points, planning targeted interventions, executing with stakeholder buy-in, and continuously evaluating outcomes. Together, these habits create a durable, self-correcting system that strengthens workforce resilience and ensures that opportunities are genuinely accessible to all talent, not simply expanded in name only.

Implications and Next Steps

Employers should invest in validated skill frameworks, adopt high-ROI talent practices, and use data to track outcomes. WiCyS can deepen employer partnerships, provide benchmarking tools that support the adoption of best practices, and highlight organizations that excel in skills-based talent development. Policymakers and funders can support scalable models for objective, skills-based assessment.

Further research should explore how these practices influence broader indicators of organizational performance, including profitability and long-term resilience. What remains clear is that in a tightening labor market, workforce resilience is a strategic imperative. Skills-based, talent-friendly practices, reinforced by strong third-party partnerships, offer a path to building that resilience at scale.

CONTENTS

1 Introduction

As the economy continues to digitize at a rapid pace, the demand for a dynamic cybersecurity workforce continues to grow. Yet the systems that support career progression have not kept pace with the field's needs. New technologies, rising compliance requirements, and increasing interdependence across business functions are reshaping what organizations expect from their cyber teams. Despite these shifts, pathways into the field and into leadership roles remain narrow and often opaque. That limits the number of people who can step into positions where judgment, communication, and risk coordination matter most. The result is weakened organizational resilience in much the same way that relying on a single vendor or a single technology creates operational fragility. A workforce built on constrained pathways cannot adapt to the speed or complexity of today's cybersecurity environment.

That fragility is amplified by forces well outside the cyber domain. We are entering a period defined by persistent, structural demographic headwinds. An aging population, declining birth and immigration rates, and a steady erosion in labor force participation are converging into a long-term constraint on the supply of talent across the economy.[1] These trends are not momentary fluctuations; they form a backdrop against which every sector, including cybersecurity, will operate for decades. Organizations will not choose whether to work in a talent-scarce environment, but will learn how to endure within one. In such a landscape, expanding opportunity for more workers is no longer a symbolic gesture toward corporate responsibility. It becomes an economic requirement, especially for women, who represent half the population and increasingly hold the educational credentials demanded by roles where analysis, coordination, and risk judgment matter.

Cybersecurity's persistent gender gap further limits the field's talent pool and narrows its resilience at precisely the moment when the general labor supply is tightening. Women make up 24 percent of the cybersecurity workforce, yet their representation drops to roughly 20 percent by the ten-year mark and falls again to 15 percent at the chief information security officer (CISO)-level.[2] This pattern does not reflect a commensurate narrowing in capability. Women in CyberSecurity (WiCyS) research highlights women outperforming their male colleagues in areas central to cyber leadership, including communication, coordination, and risk evaluation.[3] The issue, therefore, is not a shortage of qualified talent; it is the absence of pathways that recognize and retain that talent during the years when careers typically accelerate. In a tightening labor market, that gap becomes a structural liability.

Artificial intelligence (AI) and automation intensify these pressures. As these tools reshape workflows, they introduce new categories of cyber

1 "The Rising Storm: Building a Future-Ready Workforce to Withstand the Looming Labor Shortage." https://lightcast.io/resources/research/the-rising-storm

2 FourOne Insights analysis of worker profile data sourced from Lightcast's Q4 2025 dataset.

3 "WiCyS Cyber Talent Study." https://www.wicys.org/initiatives/the-wicys-cyber-talent-study/

risk that require leaders who can integrate technology across teams and adapt quickly to shifting threat landscapes. They also drive rapid shifts in skill requirements — since 2023, nearly a quarter of key skills demanded in cybersecurity job postings have changed.[4] Yet traditional promotion systems, designed for slower and more linear environments, struggle to keep pace. Opaque evaluation practices and unclear advancement expectations can leave mid-career professionals stalled during the six- to ten-year window that often determines whether they rise into supervisory or strategic roles. A sector already confronting demographic scarcity cannot afford to lose talent precisely when it becomes most valuable.

In this environment, workforce resilience becomes a defining feature of organizational strategy, not a peripheral concern.

This paper examines what it will take to build that resilience: widening advancement pathways, redesigning evaluation systems, and strengthening mid-career development so that organizations can navigate both the demographic currents reshaping the workforce and the technological currents reshaping the work itself. Further, it provides a list of proven best practices to ease the implementation of these findings so that organizations can start building resilient talent pipelines right away.

4 "'The 10 Fastest Growing Skills Transforming Cybersecurity Jobs." https://www.fouroneinsights.com/insights/the-10-fastest-growing-skills-transforming-cybersecurity-jobs

2 Approach

This study integrates employer and individual survey data, qualitative insights, and market-level analytics to understand which cybersecurity talent management best practices are most beneficial across a range of financial and talent-focused outcomes. It also explores how third-party partnerships influence hiring, advancement, and retention in cybersecurity.

The survey population included cybersecurity employers and human resources (HR) leaders, with a mix of WiCyS members and non-members. Questions covered four domains:

1. **Promotion theory, return on investment (ROI), and visibility:** How organizations define promotability, the extent to which employees understand advancement pathways, and which practices employers believe generate measurable returns, such as stronger pipelines, improved retention, or reduced hiring friction.
2. **Standards and assessments for promotion and hiring:** The tools and criteria employers rely on, including competency frameworks, performance evaluations, skills assessments, and structured interview practices, as well as how consistently these standards are applied across teams.
3. **Training and professional development access:** Availability and quality of internal learning programs, access to external training or certifications, and the role third-party organizations play in supplementing firm-based development resources.
4. **Retention and gender representation data:** Organizational patterns in turnover, tenure, and promotion, with specific attention to representation of women across technical and leadership roles and where gaps in progression appear.

Responses were analyzed through quantitative aggregation of organizational data alongside targeted qualitative interviews that illustrate how firms operationalize advancement, identify emerging talent, and use external partnerships to strengthen outcomes. All survey results are reported in the aggregate to preserve individuals' and firms' anonymity. In total, the survey received 111 completed responses. While this provided an adequate sample size to derive valuable insights, our goal for future research would be to increase the number of respondents to increase statistical confidence.

To contextualize survey findings and connect internal talent practices with observed workforce outcomes, the study draws on company-level market data from Lightcast, including online job postings and professional career histories. These data enable comparisons of hiring and talent outcomes such as time to fill, hiring costs, tenure, retention, and female representation in cybersecurity leadership roles.

We combined the talent practices observed at particular firms in the survey responses with the workforce outcomes observed at each firm to calculate the difference between outcomes at firms that did or did not employ specific talent practices. Using the observed impacts of each practice, we were able to estimate the associated financial returns

for particular talent practices that were associated with favorable talent outcomes - such as reduced time to fill or increased tenure.

Together, the survey, qualitative insights, and labor market analytics provide a structured view of how employers build pathways, where gaps persist, and how third-party partnerships support workforce performance. Full methodological details appear in the appendix.

2.1 HOW WE ESTIMATE ROI

This report estimates ROI using a proprietary analytic approach developed by FourOne Insights to translate observed talent outcomes into conservative, employer-relevant cost impacts. In brief, we link the presence of specific talent practices at a firm to differences in two measurable outcomes captured in external labor market data: time to fill cybersecurity job openings and average cybersecurity employee tenure. We then convert those outcome differences into estimated productivity losses avoided, using salary-based assumptions as a minimum proxy for daily productivity.

To protect respondents and preserve the integrity of the analytic approach, we report results in aggregate and do not disclose firm-level estimates or the full internal model specifications. However, the core logic is transparent: practices that reduce time to fill, lower the cost of vacancies, and extend tenure reduce the cost of churn and lost productive capacity. Full details on the data sources, outcome definitions, and calculation steps are provided in the Methodology appendix.

Findings describe associations between reported practices and observed outcomes; results should not be interpreted as causal estimates. Unless otherwise noted, results presented in this study are calculated using this methodology.

3 Key Findings

Despite widespread agreement that the cybersecurity talent pipeline is broken, there is little consensus on how to fix it. Many legacy solutions are either agenda-driven or supply-side focused, often with an emphasis on expanding cybersecurity training and certification. While these steps are necessary, a single-minded focus on the supply side of the talent equation risks misaligning workforce development efforts with employer needs. It also does little to ease immediate employer frustrations. This leaves hiring managers grasping in the dark for levers to improve the resilience of their cyber workforce. It also sidesteps questions about the efficacy of employers' current hiring and talent management practices, which may inadvertently harm the resilience of the cyber talent pipeline, both for their own organizations and for the industry at large.

The result is hiring managers who lack guidance on cybersecurity talent management best practices. The remedy is quantifiable evidence of actions that truly move the needle on cyber talent priorities – both in terms of workforce outcomes and bottom-line business success. This dual lens ensures workforce interventions are both valuable to individuals and considerate of business needs, which accelerates adoption and aligns incentives across stakeholders.

With these considerations in mind, the results of our research are clear: key talent management practices produce a definitive financial benefit to employers. The highest-impact practices produce estimated savings to employers in excess of $125,000 over the course of the average cybersecurity employee's tenure – a striking sum. These savings are largely realized through reductions in hiring difficulty and improved worker retention, both of which extend the lifetime productivity of the average cybersecurity professional.

However, not all talent practices are created equal, and employers must thoughtfully assess which practices are best suited to serve their talent goals. The evidence clearly points to practices that produce high return on investment and indicate the levers through which this value is captured. These findings are explored in the following sections and provide data-backed guidance for leaders searching for ways to build a more resilient cyber workforce.

3.1 HIGH-VALUE TALENT MANAGEMENT PRACTICES ARE SKILLS-BASED AND TALENT-FRIENDLY

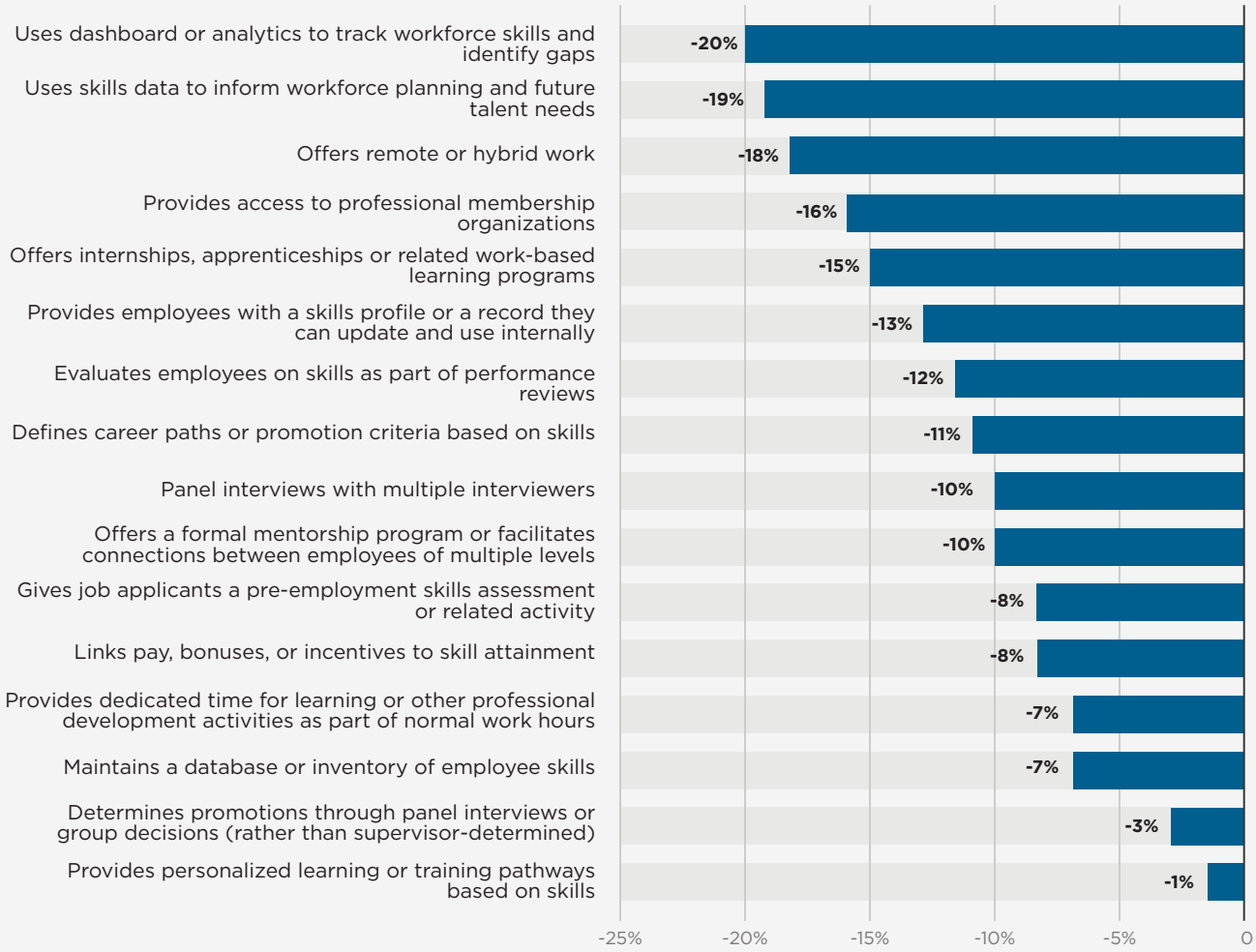
Across virtually all outcomes analyzed, the highest-impact talent practices are consistently skills-based and talent-friendly. These practices often rest on a strong foundation of data, aim to prioritize worker needs and development over short-term efficiency gains, and drive dramatic effects on workforce outcomes over the course of the employee lifecycle.

For recruiting talent, the practices with the strongest impact on reducing hiring difficulty are either directly related to skills-based workforce planning or aim to attract a broader candidate pool. For example, leveraging analytics to track skills and identify gaps and using skills data to inform workforce planning both reduced the average time it took to fill cyber job openings compared to firms that did not employ these practices. These reductions, by 20 percent and 19 percent respectively, represent the largest impact of any of the practices evaluated. This suggests organizations are turning skills-based insights and analytics into actionable hiring strategies.

Offering remote or hybrid work also had a significant impact on hiring difficulty, dropping average hiring time by 18 percent. This implies that firms considering return-to-office mandates must balance the impact of increased hiring difficulty against any perceived benefits of in-person work. Similarly, providing workers access to professional membership organizations decreased average hiring time by 16 percent, likely through increased access to talent and networking opportunities. Additionally, work-based learning opportunities that target early career employees, such as internships or apprenticeships, lowered hiring time by 15 percent.

CHART 1

Average Impact on Time to Fill Cybersecurity Jobs by Selected Talent Practices

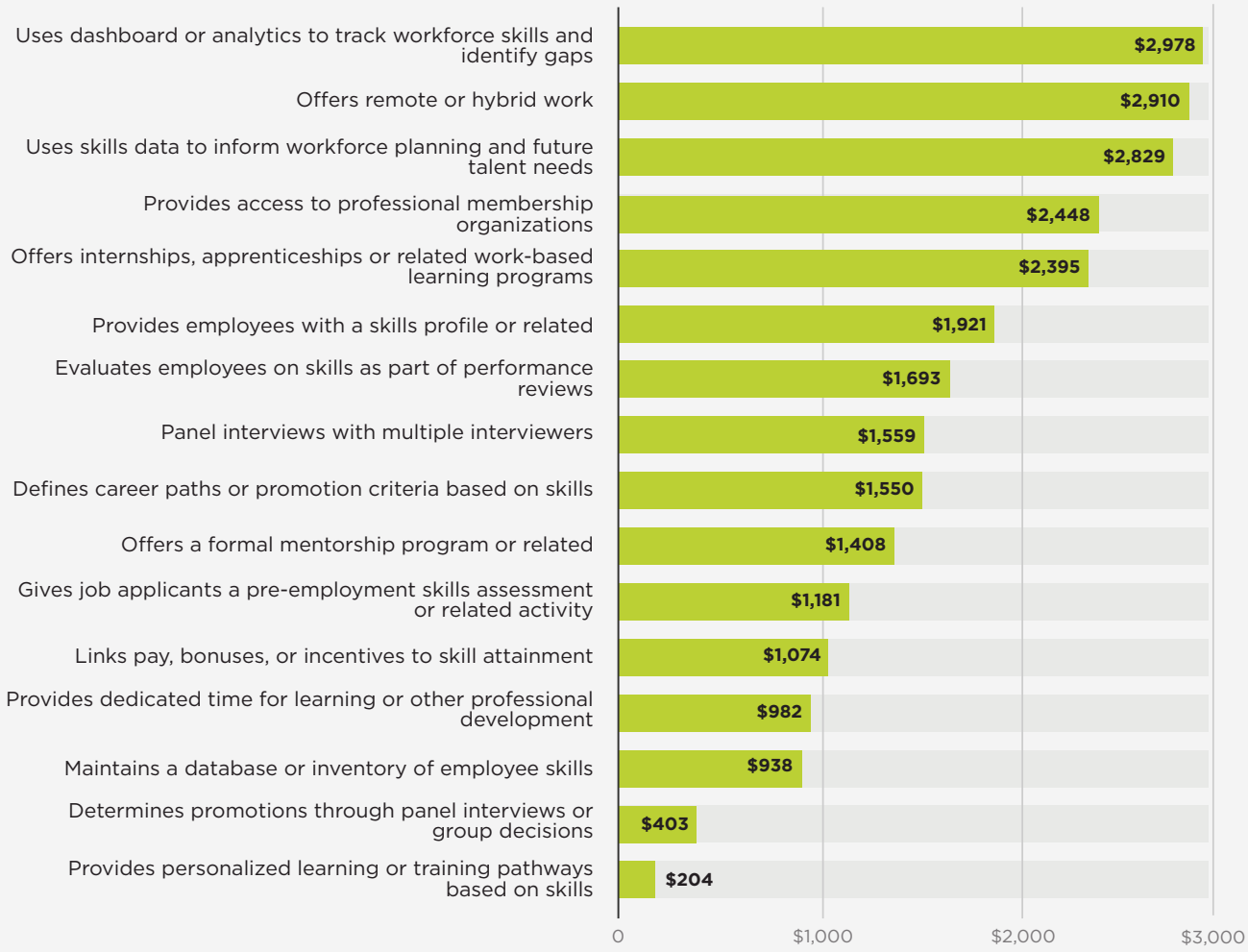


The financial return to filling jobs faster is significant. By assuming each additional day a position sits unfilled reduces worker productivity by at least the daily salary for an average cybersecurity worker, we can estimate that the talent practices most effective at reducing hiring difficulty avoid almost $3,000 in productivity losses per opening, on average. For teams hiring large numbers of cyber professionals, these cost savings add up quickly – to say nothing of their improved digital resilience.

CHART 2

Average Productivity Loss Avoided Per Cybersecurity Job Opening by Selected Talent Practices

(based upon duration of unfilled positions)



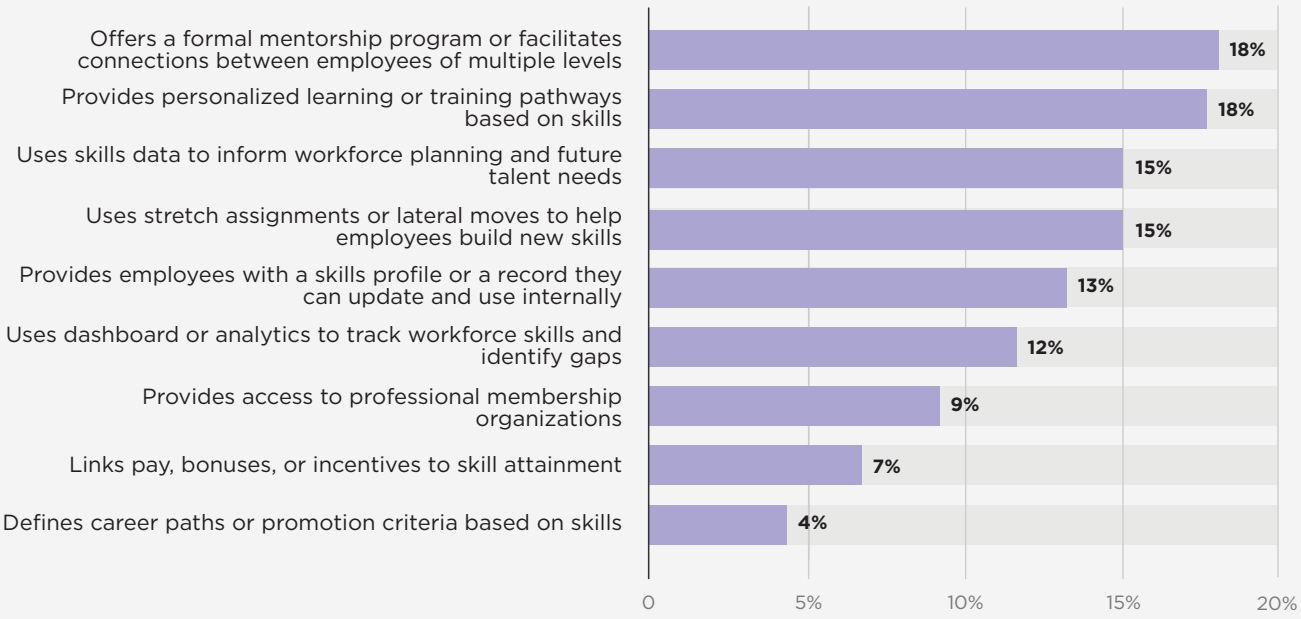
While reducing hiring costs offers clear bottom-line benefits, the greatest value of high-impact talent strategies comes once workers are already in the door. Retaining a productive worker is far more cost-effective than backfilling a role once an employee has departed, so firms have a vested interest in extending the average tenure of their employees – especially in notoriously high-turnover roles such as cybersecurity. Once again, skills-based and talent-friendly practices yield outsized impact on retention.

The two practices associated with the largest increases in retention include offering mentorship opportunities or related programs, and providing personalized, skills-based learning pathways. Both practices increased average tenure for cybersecurity workers by 18 percent in firms who employ them. These practices emphasize investing in individuals' development, suggesting they produce a strong rebound effect: **when companies invest in their employees, their employees become more invested in their company.**

Other practices associated with strong tenure gains are generally skills-based and data-backed. Firms that inform workforce planning with skills data, for example, were able to translate their resulting insights into 15 percent increases in average employee tenure, as did firms leveraging stretch assignments or lateral moves to help workers build new skills.

CHART 3

Average Impact on Cybersecurity Worker Tenure by Selected Talent Practices



The increased retention stemming from these practices can produce staggering value. If we assume longer tenure is associated with productivity gains at least equal to the average salary a worker would be paid during their increased tenure, we can estimate that the highest-impact talent practices avoid well over $100,000 in lost productivity costs during an average cyber employee's time within a company. For example, providing personalized, skills-based learning pathways or offering a formal mentorship program each save over $125,000 in offset productivity losses during the average cybersecurity worker's tenure with an employer. When combined with savings from decreased hiring difficulty, this can translate to towering returns over time, all while dramatically improving resiliency of the cybersecurity talent pipeline.

CHART 4

Average Productivity Loss Avoided Per Cybersecurity Worker by Selected Talent Practices

(based upon average increased tenure and decreased time to fill)

3.2 HIGH-VALUE TALENT MANAGEMENT PRACTICES BENEFIT EVERYONE, ESPECIALLY WOMEN

While strong financial returns may be more than enough to justify an investment in high-value talent practices, they come with another, serendipitous benefit: they are great for employees too. Virtually all of the highest-value talent practices for employers relate to employee growth and development, highlighting the mutual benefit they provide both employers and employees. This is reflected in individuals' own assessment of each practice's value to them personally. For each high-value talent practice, a strong majority of survey respondents rated the value of the practice to them personally as either very or extremely valuable.

TABLE 1 **Talent Savings to Employers vs. Value to Individuals by Selected Talent Practices**

Talent Practice	Average Cost Savings Per Cybersecurity Worker	Share of Survey Respondents Reporting Practice is "Very" or "Extremely" Valuable to Them Personally
Offers a formal mentorship program or facilitates connections between employees of multiple levels	**$127,465**	**67%**
Provides personalized learning or training pathways based on skills	**$127,167**	**81%**
Uses skills data to inform workforce planning and future talent needs	**$114,658**	**64%**
Uses stretch assignments or lateral moves to help employees build new skills	**$112,881**	**73%**
Provides employees with a skills profile or a record they can update and use internally	**$97,077**	**65%**
Uses dashboard or analytics to track workforce skills and identify gaps	**$89,157**	**58%**
Provides access to professional membership organizations	**$71,799**	**79%**

While these practices are valuable across the workforce, their skills-based and talent-friendly nature makes them uniquely valuable to workers who historically faced heightened barriers to advancing their careers in cybersecurity. This is especially true for women, who have long been underrepresented in cybersecurity and often hit a glass ceiling that prevents them from rising to leadership roles within cyber. Therefore, it is critical to identify the practices that most effectively level the playing field and help women overcome obstacles limiting their opportunities in cybersecurity leadership positions.

Three practices in particular stand out for their impact on helping women advance into senior cybersecurity roles: determining promotions through panel interviews or group discussions, providing employees with a skills profile they can use to support their internal career growth, and offering a mentorship program. **Organizations that employ these practices have between 10 to 20 percent more female cybersecurity managers than firms that do not employ these practices.** Other practices that showed positive impact on female leadership in cybersecurity include providing pre-employment skills assessments, defining career paths or promotion criteria based on skills, and linking compensation or other incentives to skill attainment.

Many of these practices are not only beneficial for helping women advance in cybersecurity but also drive significant value for employers. Most notably, offering a mentorship program, providing internal skills profiles, offering skills-based career and training pathways, and linking compensation to skill attainment are all associated with both strong ROI for employers, and increased female representation in cybersecurity leadership.

TABLE 2

Talent Savings to Employers vs. Impact on Female Cybersecurity Leadership

Talent Practice	Increase in Female Cybersecurity Leadership at Firms Leveraging Practice	Average Cost Savings Per Cybersecurity Worker
Provides employees with a skills profile or a record they can update and use internally	15%	$97,077
Offers a formal mentorship program or facilitates connections between employees of multiple levels	11%	$127,465
Defines career paths or promotion criteria based on skills	8%	$35,352
Links pay, bonuses, or incentives to skill attainment	7%	$53,361
Provides personalized learning or training pathways based on skills	1%	$127,167

These findings suggest that breaking the glass ceiling requires three important conditions to be met. First, organizations must introduce more objective promotion practices. Relying upon subjective managerial assessments can introduce biases that prevent merit-based evaluations and promotion decisions. Second, opportunities must be provided for workers of different levels to connect with one another. Self-promotion comes more naturally to most men, so cultural norms must be established that facilitate opportunities for all workers to gain visibility with leadership. Third, skills-based talent management should be utilized to provide standardized, transparent criteria for promotion. This will enable greater consistency and objectivity in the promotion process, allowing workers to compete based upon what they can do, not just whom they know.

3.3 DESPITE THE VALUE OF HIGH-ROI TALENT MANAGEMENT PRACTICES, ADOPTION IS UNEVEN AND EXECUTION IS SUBOPTIMAL

Despite the mutual benefit to employers and employees, adoption of many high-value talent management practices is inconsistent at best. In fact, the highest-impact practices are some of the least utilized. Among the three practices with the largest average cost savings to employers – mentorship programs, personalized learning pathways, and skills-based workforce planning – none are utilized by more than 55 percent of firms included in our survey. This threatens worse talent outcomes for many firms, while limiting opportunities for career development among their employees.

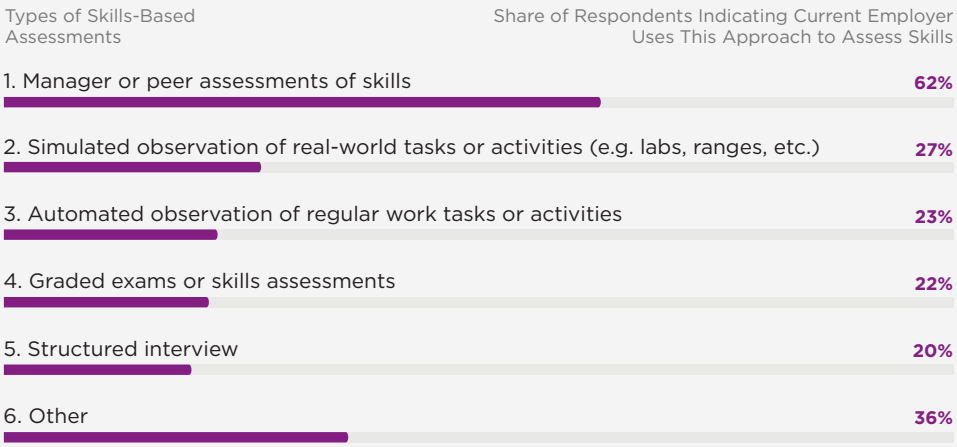
TABLE 3 **Talent Savings to Employers vs. Share of Employers Leveraging Practice**

Practice	Share of Employers Leveraging Practice	Average Cost Savings Per Cybersecurity Worker
Offers a formal mentorship program or facilitates connections between employees of multiple levels	49%	$127,465
Provides personalized learning or training pathways based on skills	55%	$127,167
Uses skills data to inform workforce planning and future talent needs	53%	$114,658
Uses stretch assignments or lateral moves to help employees build new skills	61%	$112,881
Provides employees with a skills profile or a record they can update and use internally	60%	$97,077

Compounding the issue, even when firms do leverage these practices, they are often implementing them in suboptimal ways, especially as it relates to skills-based practices. To ensure skills-based practices deliver value, they must be based upon a trusted foundation of data from reliable internal or external sources. However, 62 percent of survey respondents said their organizations assess skills using subjective managerial or peer assessments, which are notoriously problematic for injecting biases into the skill evaluation process. By contrast, no more than 27 percent of respondents reported their organizations are using more objective means of assessing skills, suggesting that most skills-based efforts may be relying upon questionable data, thus limiting their efficacy.

CHART 5

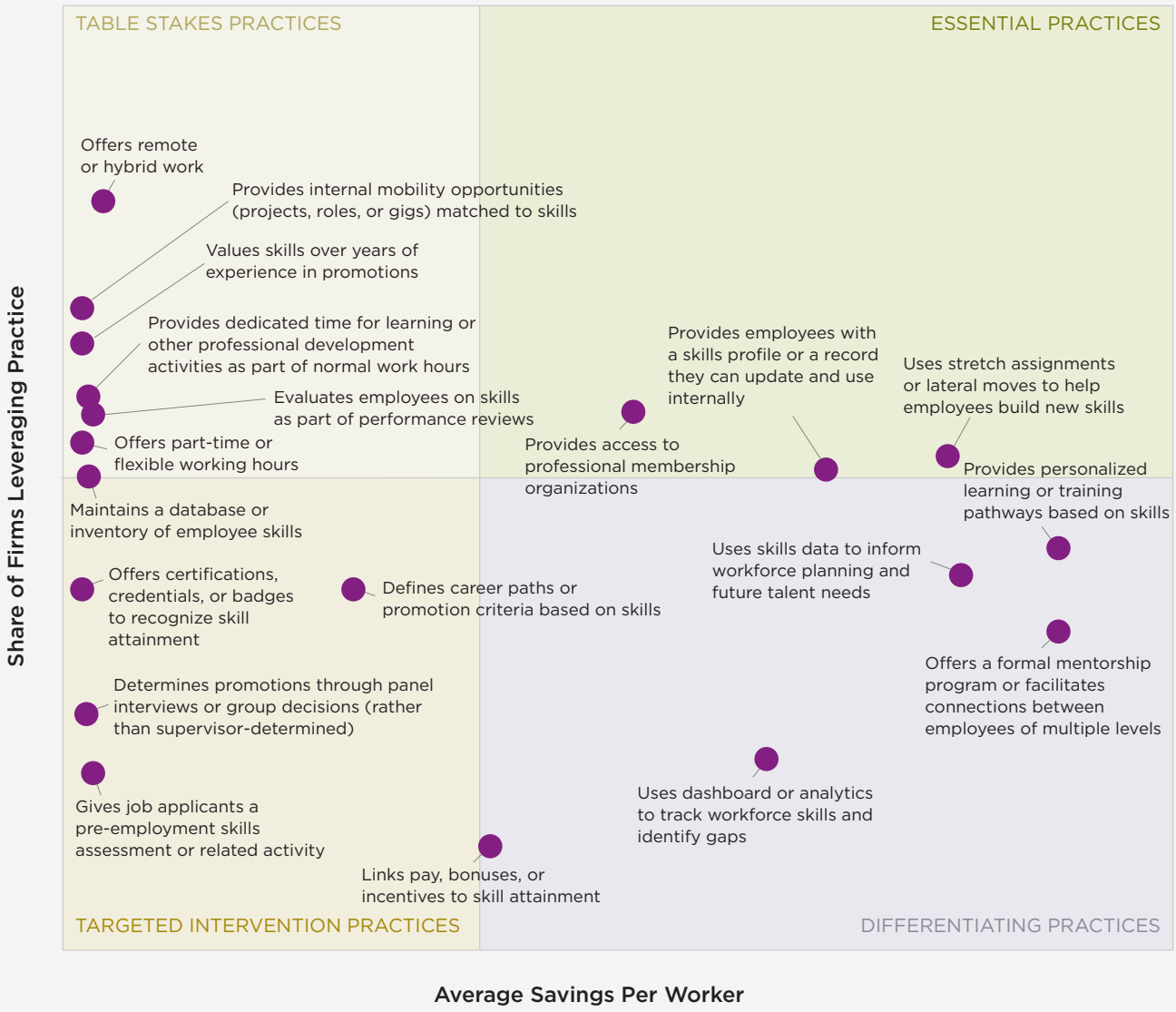
Skills-Based Assessment Practices Currently In-Use



Furthermore, organizations need guidance on the talent practices that deliver the most value and help them differentiate their employee value proposition. Many of the most-utilized talent practices have relatively low financial benefit, suggesting many firms are missing opportunities to optimize their talent strategies. However, this doesn't mean the more commonly used practices don't have value. They may have simply become so widely adopted that there is minimal incremental value to adding them. There still may be a downside to being the only employer not utilizing them, and they may provide non-financial benefits, such as access to specific talent pools or strategically important skillsets.

This suggests firms can differentiate their talent strategies by adopting underutilized talent practices that deliver strong ROI, while taking a targeted approach to adopting less lucrative – but strategically important – practices. The following Talent Practice Prioritization Matrix illustrates how current adoption of each talent practice compares to average cost savings associated with each practice. Leaders can use this to quickly assess which practices will differentiate their talent strategies, and identify practices that are either table stakes in the market or are best suited for targeted interventions.

CHART 6 | **Talent Practice Prioritization Matrix**



3.4 THIRD-PARTY PARTNERSHIPS EASE IMPLEMENTATION

Across the research, a consistent pattern emerges: third-party organizations expand the capacity of both individuals and firms to adapt to change. These partners operate as structural supports that help workers build connections, gain visibility into industry practices, and access learning opportunities that many employers struggle to provide on their own. Membership and professional organizations, in particular, play an outsized role in strengthening the workforce ecosystem.

Survey data illustrate the depth of this value. Nearly eight in ten respondents report that access to membership organizations such as WiCyS is very valuable. For WiCyS specifically, 77 percent say the organization helps them build professional connections, compared with 49 percent who receive this support from their employers. This gap signals a structural limitation within firms: most lack the scaffolding to support the networks and peer communities that workers need to navigate a rapidly evolving field. WiCyS helps fill that gap by offering spaces where members can exchange insights, gain mentorship, and identify pathways for advancement. Respondents also note the importance of WiCyS' research, insights, and opportunities to learn new skills — elements that strengthen professional judgment in an environment where roles and expectations continue to shift.

Furthermore, the benefits extend beyond individual members: firms that provide access to these organizations see measurable operational gains. **On average, these employers fill cyber job openings sixteen percent faster, experience tenure rates nine percent longer, and avoid more than $71,000 in lost productivity per worker.** These results suggest that third-party organizations supply capabilities that are otherwise costly or difficult for employers to build internally, such as sustained peer learning, industry-wide knowledge flows, and trusted professional communities.

Taken together, the findings reinforce that third-party partnerships are not peripheral supports but essential catalysts. They create mobility in a labor market where pathways can be opaque, and they ease implementation for employers by strengthening retention, accelerating hiring, and expanding access to develop new skills. In a system where adaptation is increasingly a shared responsibility, these organizations help distribute the work of workforce development and make the broader ecosystem more resilient.

CHART 7

Value of WiCyS Membership to individuals

4 Best Practices

Based on the findings of this research, the following best practices offer leaders practical guidance and actions to align cyber talent goals with high-impact outcomes. Leaders should evaluate these practices within the unique context of their organizations to develop personalized, meaningful, and sustainable talent management strategies. They should also seek out trusted third parties, such as WiCyS or similar partners, that provide community, visibility, and resources to support organizations throughout their talent management journey.

4.1 ALIGN TOP-DOWN AND BOTTOM-UP LEVERS AND PERSONALIZE TALENT STRATEGIES TO ORGANIZATIONAL GOALS

High-impact workforce interventions connect leadership-driven initiatives with employee-driven development opportunities. This requires a mix of top-down and bottom-up levers, such as the following:

- **Top-down levers:** promotion transparency, executive sponsorship, skill and task-level metrics tracking, and leadership accountability.
- **Bottom-up levers:** access to upskilling pathways, mentorship programs, and employee resource groups that empower workers, build belonging, and support professional growth.

When these levers operate together, they create a cohesive ecosystem where individuals are empowered to grow, and leaders are equipped to support them.

The right levers will differ by organizational priorities, culture, and cost sensitivity, however, so leaders must personalize their talent strategies to their unique talent goals and operational realities. Using evidence from our research, the following table provides illustrative examples for how leaders can connect common talent goals with high-impact top-down and bottom-up practices.

CHART 8 | **Talent Goals Aligned to High-Impact Practices**

Goal	Reduce Hiring Difficulty	Increase Retention and Tenure	Expand Leadership Pathways	Increase Internal Mobility	Increase Prevalence of Emerging Skills
High-Impact Top-Down Practices to Consider	• Use skills analytics to inform workforce planning • Offer remote or hybrid work	• Use skills analytics to inform workforce planning	• Determine promotions through panel interviews or group decisions (rather than supervisor-determined)	• Prioritize skills over years of experience in promotions	• Assess skills pre-employment
High-Impact Bottom-Up Practices to Consider	• Provide access to professional membership organizations	• Offer mentorship or related programs • Provide personalized learning pathways	• Provide employees with a skills profile to use internally and document progress towards goals • Offer mentorship or related programs	• Provide access to professional membership organizations • Offer stretch assignments or lateral moves	• Provide dedicated time for learning or other professional development activities as part of normal work hours • Offer credentials to recognize skill attainment

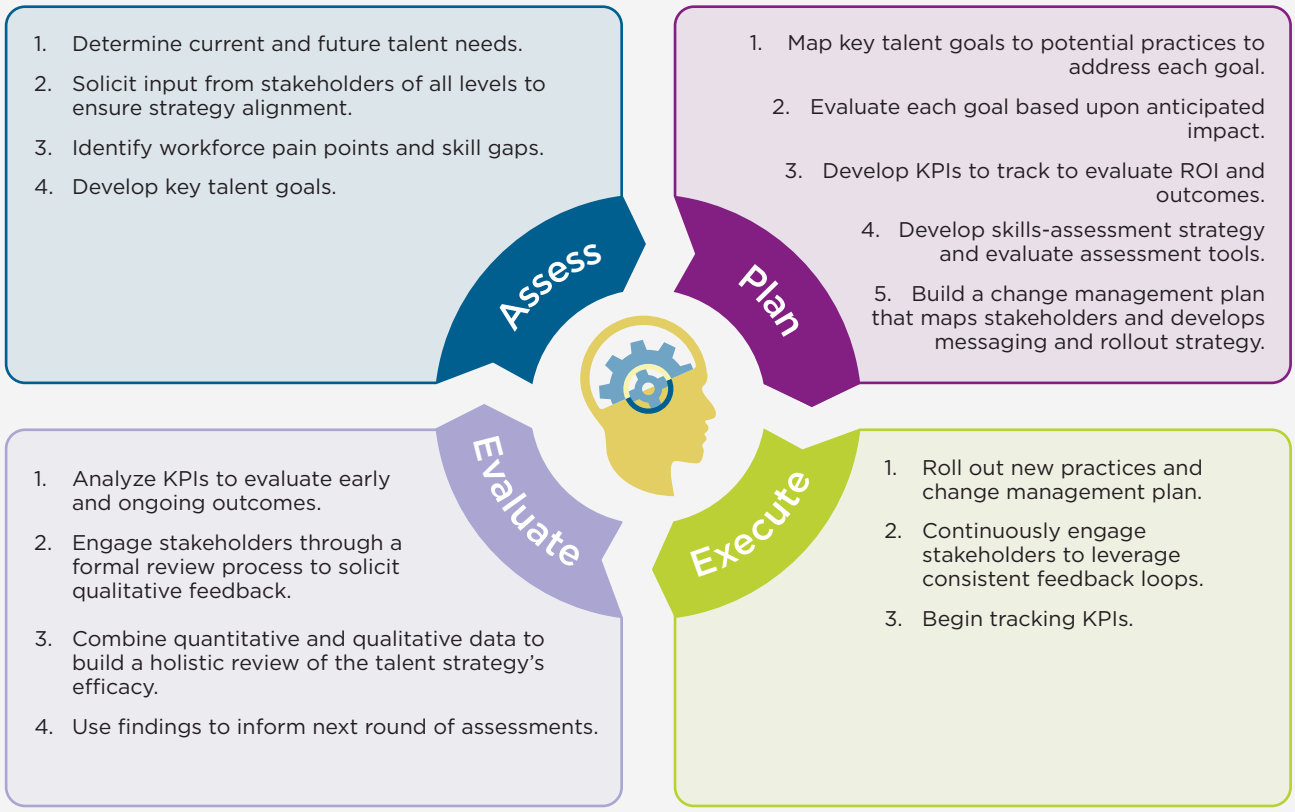
4.2 BUILD A REPEATABLE PROCESS TO CONTINUOUSLY OPTIMIZE TALENT MANAGEMENT

Workforce needs evolve rapidly, so organizations must treat talent management as an iterative process. To do so, they can leverage the following framework, supported by this report's findings, which enables continuous alignment between talent goals and high-ROI practices. It is comprised of the following steps leaders can take to continuously optimize their talent management practices:

1. **Assess**: Identify workforce pain points and define talent goals at the team or organizational level.
2. **Plan**: Determine which practices will have the greatest impact on those goals and develop a change management and evaluation plan.
3. **Execute:** Implement selected practices and ensure active engagement from relevant stakeholders.
4. **Evaluate**: Continuously measure ROI, workforce outcomes, and program effectiveness, adjusting strategies as needed to sustain impact.

These steps are illustrated in the following chart, along with key steps necessary for implementation.

CHART 9 **Continuous Talent Optimization Framework**



4.3 STRENGTHEN THE TALENT MANAGEMENT FOUNDATION WITH OBJECTIVE, TENABLE SKILLS DATA

All talent practices rely on a strong foundation of accurate, defensible skills data. This requires organizations to implement objective skills assessments that reliably measure workforce capability. Ideally, these assessments are:

1. **Vendor-neutral**, ensuring comparability and reducing bias; and
2. **Rooted in observed performance,** such as real-world tasks, lab-based simulations, or other realistic skills evaluations.

Such data allows leaders to validate hiring decisions, support development planning, and measure the effectiveness of talent initiatives over time.

4.4 OPEN ACCESS TO OPPORTUNITY THROUGH WORKER EMPOWERMENT AND EXPANDED LEADERSHIP PATHWAYS

The evidence points to skills-based, talent-friendly practices as the most effective means for delivering strong workforce outcomes. These practices inherently open access to opportunity by empowering workers and expanding pathways into leadership — especially for women in cybersecurity. In an era where talent resilience is a mission-critical concern, expanding advancement opportunities for a population comprising roughly half of the workforce takes on singular importance.

However, this is not simply about increasing female representation for its own sake. Instead, the objective is to build resilience by ensuring that opportunities are genuinely accessible to everyone deserving, and that organizations retain talented workers long enough to progress into leadership roles. This elevates worker empowerment to a mechanism for strengthening the cyber workforce, not an end in itself.

5 Implications and Next Steps

For employers:

Strengthening workforce resilience begins with clearer, more reliable information about skills. Employers should invest in validated skill frameworks, adopt skills-based practices that have demonstrated impact, and embed data-driven approaches to tracking promotion and advancement. These steps create greater visibility for workers and more consistent decision-making for managers. Employers should also work with trusted third-party partners, such as WiCyS, to extend their internal capacity and provide employees with access to networks, learning opportunities, and professional communities that are difficult to build alone. These steps come with varying levels of financial and non-financial investment – from no-cost, low-effort actions to large, multi-year transformations – so employers must align their efforts with internal cost and resourcing constraints.

For WiCyS:

There remains an opportunity to help employers translate best practices into operational routines. WiCyS can expand its partnerships with firms, offer benchmarking dashboards and practical resources that guide implementation, and recognize organizations that excel through initiatives such as a "Skills-Based Excellence" award. These efforts would reinforce the value of data-backed, talent-friendly workforce strategies and support broader adoption across the field.

For policymakers and funders:

A more resilient cybersecurity workforce will require scalable, trusted methods for verifying skills. Policymakers and funders can support this shift by encouraging third-party validation models that emphasize objectivity, transparency, and portability across employers. These frameworks can help standardize expectations in a field where job requirements evolve quickly.

Next research phase:

Future work should deepen the analysis of how skills-based metrics align with long-term workforce outcomes and expand representativeness through larger survey samples. This includes examining the connection between skill attainment and retention, and expanding the scope to assess potential links to organizational performance indicators such as profitability or stock market returns. Additional research is also needed to evaluate the relative cost and effort associated with each practice, so organizations across all sizes may pinpoint actions that align with their cost and operational constraints. These insights would help clarify the full value of skills-based talent management and guide investment across employers, educators, and partners.

Appendix A: Methodology and Data Sources

To quantify the impact of various talent management practices on cybersecurity workforce outcomes, this report leveraged a combination of three primary data sources: an original survey administered by FourOne Insights in collaboration with WiCyS, job posting data from labor market analytics provider Lightcast, and professional social profile data, also from Lightcast.

Information about each data source and their roles in the analysis is detailed below.

Survey of WiCyS Network

In October 2025, a survey was administered to members of the WiCyS network to collect information about the talent practices employed at respondents' organizations along with related details. This survey was informed by a series of qualitative stakeholder interviews with WiCyS member organizations and others throughout the cybersecurity community. Survey respondents were asked questions about a list of 22 talent practices identified for this research – such as whether each practice was employed by respondents' current employers, the perceived value of each practice to the individual and their companies, and related information – as well as basic descriptive information such as respondents' job titles, career levels, current employers, and similar details. A related line of questioning was included about respondents' experience as members of the WiCyS community. In total, the survey received 111 completed responses. While this provided an adequate sample size to glean valuable insights, our goal for future research would be to increase the number of respondents to increase statistical confidence.

Job Posting Data from Lightcast

This report leveraged job posting data sourced from labor market analytics provider Lightcast. This dataset includes billions of historical job postings sourced from tens of thousands of job boards. These job postings are rigorously deduplicated and machine read to extract dozens of data points about each job posting, such as job title, occupation, skill and credential requirements, education and experience requirements, industry, employer, geographic location, opening duration (which is a proxy for the time to fill an open position), advertised salaries, and more.

Unless otherwise noted, job posting data used in this report reflect the 12-month period from November 2024 through October 2025.

Professional Social Profile Data from Lightcast

This report also utilized data on professional worker histories sourced from Lightcast's dataset of professional social profiles. This dataset includes hundreds of millions of professional worker histories and includes information on dozens of variables for each professional profile, such as employer, job title, occupation, gender, skills and credentials, educational history, years of experience, and more.

Data used in this report came from the October 2025 version of Lightcast's professional social profile database.

Defining the Core Cybersecurity Workforce

Each of the job postings and professional social profiles from Lightcast are classified into an occupational taxonomy developed by Lightcast. This taxonomy is intended to track job categories with more granularity and timeliness than traditional occupational taxonomies such as O*NET or similar governmental sources. For the purposes of this report, cybersecurity occupations were identified within this taxonomy to isolate the hiring and workforce outcomes within cybersecurity roles. This resulted in the following 11 Lightcast occupations forming the basis for our definition of the core cybersecurity workforce:

- Chief Information Security Officer
- Cyber Crime Analyst / Investigator
- Cyber Security Analyst
- Cyber Security Architect
- Cyber Security Consultant
- Cyber Security Engineer
- Cyber Security Manager / Administrator
- Cyber Security Specialist / Technician
- Incident Analyst / Responder
- Vulnerability Analyst / Penetration Tester
- Security Operations Center Analyst

Combining Data Sources to Estimate Impact of Talent Practices on Workforce Outcomes

To estimate the impact of specific talent practices on various cybersecurity workforce outcomes, data from all three sources were combined.

First, employers listed by survey respondents were mapped to corresponding employers in Lightcast's job posting and professional social profile databases. This resulted in a list of 56 companies that were present in both the survey responses and the Lightcast datasets.

Next, survey responses were used to determine which companies employ each talent practice included in the survey. At firms that did employ each practice, their cybersecurity hiring and workforce outcomes were compared to the outcomes at firms that did not employ each practice. Specific outcomes evaluated at each company included average job opening duration, average employee tenure, female representation in cybersecurity roles, employee internal mobility, and prevalence of emerging cybersecurity skills.

To estimate the ROI from each talent practice, the differences in outcomes between firms that did or did not employ various talent

practices were used to estimate the typical impact a given practice had on each outcome. For outcomes that could be translated into an increase or decrease in a worker's tenure in a role – such as opening duration and average tenure – the differences in outcomes were translated into an average number of days a worker remained in a role at a given company. The minimum daily productivity of an average cybersecurity worker was then estimated by assuming the average advertised salary in cybersecurity job postings reflects the minimum amount of value they add to their employer, since employers would have no economic incentive to keep them employed if this was not the case. We estimated the average monetary impact of each talent practice by multiplying the average minimum daily productivity by the number of days a talent practice was found to increase worker tenure in a cybersecurity role.

While many factors may determine talent outcomes, and additional analysis would be valuable to further control for these factors, this approach enables quick identification of practices that appear to correlate with outsized differences in cybersecurity talent outcomes. Additional analysis would also be useful to determine other monetary considerations relevant in ROI calculations – such as implementation costs, impact on shareholder returns, reputational value, and similar factors.

Geography and Timeframe

Data for this report were sourced for the United States. Unless otherwise noted, all data were collected during September, October, and November 2025.

Appendix B: Glossary

ORGANIZATIONAL CONTEXT AND ROLES

WiCyS (Women in CyberSecurity)

A global membership organization dedicated to advancing the recruitment, retention, and advancement of women in cybersecurity. WiCyS partnered with FourOne Insights to conduct the research presented in this report.

Core cybersecurity role

A position in which cybersecurity is the primary job function, such as a security analyst, engineer, architect, or incident responder.

Cybersecurity-adjacent role

A role that is not primarily a core cybersecurity role but supports or regularly interfaces with cyber teams or cyber risk, including information technology (IT) operations, privacy or cyber law, governance and compliance, risk management, and HR roles supporting cyber talent.

Student

An individual currently enrolled in high school or a postsecondary institution, including community colleges, undergraduate programs, or graduate programs.

Junior / early-career professional

An individual in an entry-level cybersecurity role, often titled analyst or technician, typically within the first few years of professional experience.

Mid-career individual contributor

An experienced cybersecurity professional operating without direct people-management responsibilities, such as a senior analyst or engineer.

Senior-level individual contributor

An advanced technical expert role, such as principal engineer or security architect, characterized by deep specialization and strategic technical influence without formal supervisory authority.

Supervisor

A front-line management role responsible for overseeing staff, often serving as the first formal leadership step in a cybersecurity career.

Senior leader

A high-level management role, such as director or vice president, with responsibility for teams, functions, or organizational strategy.

Executive

Top-tier organizational leadership roles, including Chief Information Security Officer (CISO), Chief Executive Officer (CEO), and board-level positions.

TALENT MANAGEMENT AND HIRING PRACTICES

Skills inventory / skills database

An organizational system used to catalog, track, and analyze the skills present in the workforce and identify gaps relative to current or future needs.

Skills-based hiring

A hiring approach that prioritizes demonstrated skills and capabilities over traditional proxies such as degrees, job titles, or pedigree.

Pre-employment skills assessment

An objective evaluation or test administered to job candidates to measure relevant skills prior to hiring.

Work-based learning

Structured opportunities for individuals to develop skills through practical experience, including internships, apprenticeships, or other paid, on-the-job learning models.

ADVANCEMENT, MOBILITY, AND CAREER DYNAMICS

Internal mobility

Opportunities within an organization, such as short-term projects and roles on other teams or in different departments, allowing employees to apply or expand their skills without leaving the firm.

Lateral moves

Role changes at the same organizational level intended to broaden skill sets, experience, or domain knowledge rather than provide immediate promotion.

Skill-linked incentives

Compensation mechanisms that tie pay, bonuses, or rewards directly to the acquisition or demonstration of new skills.

Sponsors or advocates

Senior individuals who actively support an employee's advancement by providing visibility, endorsement, and access to opportunities; the absence of sponsorship is a common barrier to progression.

Subjectivity of promotion decisions

A barrier to advancement characterized by unclear criteria, opaque evaluation processes, or reliance on informal or individual judgment rather than defined standards to select individuals for promotion.

Visibility

The degree to which an employee's work, skills, and contributions are recognized by decision-makers, often influenced by networking, high-impact assignments, or speaking opportunities.

Validation

Career reinforcement gained through peer communities, professional organizations, or external networks that affirm skills, identity, and belonging.

CORE ANALYTICAL CONCEPTS

Demographic constraints (Demographic headwinds)

Long-term structural trends that include, but are not limited to, population aging, declining birth and immigration rates, and reduced labor force participation that constrain the overall supply of talent across the economy.

Productivity loss avoided

A financial metric estimating the value preserved by reducing hiring time or extending employee tenure. It is calculated by assuming that each day a role remains unfilled or a worker departs early reduces productivity by at least the worker's average daily salary.

Return on investment (ROI)

The measurable financial benefit employers realize from specific talent practices, primarily through faster hiring and improved retention. High-impact practices identified in this report can return over $125,000 per cybersecurity worker across their tenure.

Skills-based practices

Talent management approaches grounded in objective skill data and clearly-defined expectations, rather than subjective assessments or credentials alone.

Talent-friendly practices

Workforce practices that prioritize long-term employee development and well-being, such as mentorship, flexible work arrangements, and personalized learning, rather than short-term efficiency gains.

Workforce resilience

An organization's ability to adapt its cybersecurity workforce to rapid technological change, evolving threats, and labor market constraints. Resilience is strengthened by widening advancement pathways and building durable, self-correcting talent systems.

HIGH-IMPACT TALENT PRACTICES

Mentorship programs

Formal initiatives that connect employees across levels to share knowledge, expand networks, and support advancement. These programs are associated with increased tenure and higher representation of women in management.

Personalized learning pathways

Tailored development plans based on individual skill profiles; cited as both highly valuable to workers and a top driver of retention.

Skills profile

A standardized, employee-maintained record of skills used internally to support fair competition for roles and advancement based on demonstrated capability.

Stretch assignments

Structured opportunities that allow employees to develop new skills through experience beyond their core responsibilities.

Third-party partnerships

Collaborations with external organizations, such as WiCyS, that provide capabilities that are difficult or costly for employers to build internally, including peer learning, professional networks, and industry context. Firms leveraging these partnerships fill roles significantly faster and improve retention.

METHODOLOGICAL TERMS

Lightcast

A labor market analytics provider supplying job posting data (e.g., time to fill, salary) and professional career history data (e.g., tenure, gender representation) used in this analysis.

Time to fill (Opening duration)

The length of time a job posting remains active, used as a proxy for hiring difficulty. Skills-based practices are associated with reductions in time to fill of up to 20 percent.

Acknowledgements

The authors would like to thank the dozens of cybersecurity professionals, executives, WiCyS strategic partners, and other stakeholders who generously offered their time and insights to support this research.

REPORT AUTHORS

This report was written by Will Markow, Seeyew Mo, and Analiese Wagner.

Strategic guidance was provided by Mary Jane Partain and Lynn Dohm.

ABOUT WICYS

Women in CyberSecurity (WiCyS) is a nonprofit organization with international reach dedicated to the recruitment, retention and advancement of women in cybersecurity. Founded by Dr. Ambareen Siraj through a National Science Foundation grant given to Tennessee Tech University in 2013, WiCyS offers opportunities, trainings, events, and resources for its community and members. Strategic partners include — Tier 1: Akamai Technologies, Amazon, Bloomberg, Cisco, Ford Motor Company, Google, Lockheed Martin, Palo Alto Networks, SentinelOne; Tier 2: Adobe, Flare, Microsoft, Navy Federal Credit Union, PayPal, Pepsico, PSEG Services Corporation, Tenable, The MITRE Corporation.

To partner, visit www.wicys.org/support/strategic-partnerships/.

ABOUT FOURONE INSIGHTS

FourOne Insights is a research and advisory firm focused on the future of work and the impact of emerging technologies on jobs, skills, and organizations. We help companies, training providers, government agencies, and nonprofits understand workforce trends, make data-driven decisions, and prepare for rapid change. Through research, analytics, and strategic guidance, we equip leaders with the insights they need to anticipate disruption and build a resilient, future-ready workforce. Learn more at www.fouroneinsights.com.

Women in Cybersecurity WiCyS

FourOne Insights