CYBER
TALENT
INSTITUTE

RECRUITING AND RETAINING CYBER STARS

Three Essential Practices to Become a Great Place to Work for Top Cyber Talent

ONE

SUPPORT TRAINING THAT ENSURES CYBER SKILLS ARE KEPT UP-TO-DATE AND CONSTANTLY IMPROVING.

TWO

BUILD A GOOD REPUTATION FOR SUPPORTING A STRONG SECURITY CULTURE.

THREE

PROVIDE DIVERSE, HIGH-IMPACT, AND CHALLENGING PROJECTS.

THE BOTTOM LINE:

ADOPTING AND SUPPORTING THESE THREE PRACTICES WILL ENABLE YOU TO COMPETE MORE EFFECTIVELY FOR SCARCE CYBERSECURITY TALENT AND RETAIN THAT TALENT ONCE YOU HAVE IT.

"I want to work for someone who cares about cybersecurity and has a manager that understands cyber."

– Survey Respondent

WHAT ARE CYBER STARS AND WHY DO THEY MATTER?

Cyber Stars are the high-end technical cybersecurity wizards who anchor nearly every effective team we need to help us build and protect our critical IT systems. They have both deep technical skills and practical experience in one or more of the important sub-specialties of cybersecurity, ranging from building and designing defensible systems to threat hunting, continuous monitoring, penetration testing and digital forensics.

You are competing in one of the tightest labor markets in years.

Vulnerable organizations – meaning *all* organizations – are competing in a challenging labor market. Attracting top talent is the first step, of course, but equally vital is retaining and maintaining that talent. By "maintaining" we mean constant upskilling and reskilling, which are critical components in keeping up a robust cybersecurity capability. The technologies that we are defending are constantly evolving, as are the capabilities and attack vectors of those who would do us harm. Ten years ago, few C-Suite executives were talking about ransomware, for example, but today it is a board-level topic of concern.

Unless you make becoming an employer of choice for both current cybersecurity professionals and future recruits, you place your organization at a serious disadvantage.

"Earlier this year, an article in the Harvard Business Review summed up the plight: 'The majority of chief information security officers around the world are worried about the cybersecurity skills gap, with 58 percent of CISOs believing the problem of not having an expert cyber staff will worsen."

CLICK TO READ THE ARTICLE →

"Over the eight-year period tracked, the number of unfilled cybersecurity jobs is expected to grow by 350 percent, from one million positions in 2013 to 3.5 million in 2021. And of the candidates who are applying for these positions, fewer than one in four are even qualified, according to the MIT Technology Review."

CLICK TO READ THE ARTICLE →

HOW DO WE KNOW THESE ACTIONS WILL MAKE A DIFFERENCE?

In a survey conducted in June 2021, we asked 500 cybersecurity professionals to rate the relative importance of factors that (a) make an organization an employer of choice and (b) motivate them to stay with their current employer. The survey built upon and updated a 2016 Center for Strategic and International Studies paper, Recruiting and Retaining Cybersecurity Ninjas, which sought to identify factors that help high-performing cybersecurity organizations build and keep a critical mass of high-end specialists.

We publicized the survey through a variety of channels that reach more technically oriented cybersecurity professionals. In addition to closed-ended questions that asked respondents to rate a number of factors, we included several open-ended questions that allowed respondents to add their own thoughts. A description of our methodology, a copy of the survey instrument, and the detailed results are attached as Appendices A, B and C, respectively.

On attracting talent, more than half of respondents ranked three factors as *very important:*

1. The employer supports training to ensure cyber skills are up to date and improving (86.63%)
2. The employer is known to prioritize computer security (66.09%)
3. The employer offers exposure to diverse, high-impact computer security projects (59.69%)

On retaining talent, predictably, hygiene factors[2] such as competitive compensation and flexible work schedules were rated as very important by most respondents (81.29% and 72.32% respectively), but paid training to facilitate skills development at 83.04% ranked slightly higher even than competitive compensation.

[2] In his work on employee motivation, Herzberg found that, once basic needs were met, increasing investments in what he called hygiene factors, like pay and safe working conditions , did little to motivate employees. Failing to meet some minimum set of expectations, however, could be a significant de-motivator.

Of the other factors, five were rated as *very important* by more than half of respondents:

4. Managers who prioritize cybersecurity appreciate and support technical competence (76.37%)
5. Opportunities for career advancement (63.74%)
6. Ability to be promoted without becoming a manager (58.09%)
7. Colleagues whom I like (57.42%)
8. Mission criticality (the work makes a difference) (50.1%)

WHAT DOES THIS MEAN?

The comments we received reinforced the priorities above. Not surprisingly, work-life balance and competitive pay and benefits (hygiene factors) were mentioned most frequently. That said, few respondents indicated that show they would go to the highest bidder or the employer who provided the best cookies and pastries, as it were.

On training, the survey respondents made it clear that additional skill development matters. Indeed, the data tell us that a robust, well-funded training program is critical for attracting and retaining talent. One survey respondent stated simply and directly what is needed:

> *"A training budget that enables me to take at least one course annually ... including paying for travel to another site if I choose that delivery method."*

Another respondent was equally direct and specific:

> *"New training and certification available each year. Training is good only if you can do [a] new one each year [and] certification must be a part of the training. Getting the training but not having the opportunity to get the certification is a failure in a training process."*

Two others spelled out exactly why they would leave their current employer:

> *"Removing access to training from industry leaders"*

> *"Reduced funding for training and continuing education"*

It's also important to note that training opportunities must go beyond a learning environment where teams can share knowledge, as reflected in two other comments from respondents:

> *"Look for people who are team players, who want to mentor our young employees ... people who are willing to train others and help people learn new skill sets will help strengthen the team."*

> *"Engage the employee in a way that they grow as a security person, [even if you end up losing them in the market.] That builds a corporate reputation that pays off in the end."*

In an environment of ever-changing technologies and threats, skills age quickly. Cybersecurity is much like modern medicine. The pathogens that threaten us are constantly evolving and new modalities for prevention and treatment are being developed every day. Organizations that fail to invest in keeping their cybersecurity staffs up to date put themselves needlessly at greater risk.

"Engage the employee in a way that they grow as a security person, [even if you end up losing them in the market.] That builds a corporate reputation that pays off in the end."

On building a security culture: A security culture is hard to define and even harder to measure. For us, a security culture is one where strong cybersecurity is seen to be a business imperative, even if the core mission is not security or technology, and where technical competence is valued. Both criteria are highly subjective and hard to measure – you will know it when you see it – so we need other measurable indicators that show a company values cybersecurity. These could include spending on training and the technical credentials of the management team. Consider these comments from survey respondents:

> *"I want to work for someone who cares about cybersecurity and has a manager that understands cyber."*

> *"Having a solid team, and leaders that know and have been [in] the 'trenches'."*

"Having a solid team, and leaders that know and have been [in] the 'trenches'."

Another respondent cited some reasons why cybersecurity staff leave organizations:

> *"Support for cyber security in words only. Not providing resources (people, time, software, equipment, training, etc.) for security to be implemented effectively or consistently. Implementing security as an ad hoc process instead of a programmatic strategy with consistent policy, procedures, and awareness across an organization."*

And this comment sums it up:

> *"Top performers like to work with other top performers. This is one of the most important points for me. I want to work with the absolute best in the biz. This means I have to upgrade my own skills and keep sharp. But it also means getting the best work and always raising the standards for performance."*

On challenging, high-impact work: How do organizations like the National Security Agency continue to attract and retain some of the best of the best when many of their employees could earn substantially more money elsewhere? The answer is clear: the work is intellectually challenging and the mission of the organization makes a difference in the world. Survey respondents' comments reinforced that view. In their own words, they want:

> *"An impactful, multifaceted role."*

> *"[To have] the opportunity to be given interesting, fulfilling work."*

> *"Less paperwork, metrics, and dashboarding. More time threat hunting and actually impacting the security stack."*

> *"Purpose that I care about, work [that] is valued by leadership, impactful and meaningful..."*

WHERE IS THE PIPELINE TO FILL THE CRITICAL SHORTAGE OF TOP CYBER TALENT?

Building a sustainable talent pipeline is a long-term endeavor, but actions you can take today will enable development of a home-grown talent pipeline for the future. Multiple efforts are under way today to address the severe shortage of top-tier cybersecurity professionals. Competitions like CyberPatriot from the Air Force Association, picoCTF from Carnegie Mellon, the National Cyber League, and the Collegiate Cyber Defense Competition encourage young people to develop their skills and are great places to find talent. The federal government's Scholarship for Service offers students large scholarships and guides them into jobs in federal agencies. These programs are terrific, but the total number of top-tier cyber candidates they produce is far below the nation's needs.

The National Cyber Scholarship Foundation (NCSF) has launched a mechanism to build a much larger national cyber talent pipeline. Modeled after the Israeli program that discovers world-class cyber talent, NCSF enables every high school and college student in the United States to play an online game to discover whether they have an aptitude to excel in cybersecurity. Those who continue in the game learn loads of foundational technology and cyber skills. Each May, NCSF awards $2 million in college scholarships and millions more in advanced training grants to students who have discovered their aptitude and taken advantage of the free program to advance their skills.

All employers that want to help facilitate a larger pipeline of skilled cyber talent can take a simple step to make that happen: use their existing relationships with high schools and colleges to let the administrators know that their students are eligible to play the free CyberStart, and that millions in scholarships are available. On or after October 5, 2021, employers can ask those educational institutions to encourage every student who likes puzzles and problem solving to try the game. High school students should visit CyberStartAmerica.org and college students should visit Cyber-FastTrack.org.

WHY DOES THIS MATTER?

An organization's cybersecurity posture – its ability to prevent and/or recover from adverse events and attacks – can be no stronger than the skill level of the cybersecurity professionals it employs. Without skilled cyber talent, security tools have repeatedly failed to protect organizations. Every major cybersecurity breach and disruption that has captured the headlines in recent years could have been prevented (or its adverse impact substantially mitigated) had the affected organization (a) adopted and deployed basic security best practices, such as the CIS Controls; (b) implemented a robust suite of defensive tools, and (c) maintained a staff of highly skilled cybersecurity professionals.

APPENDIX A

SURVEY METHODOLOGY

The Survey Instrument was posted at SurveyMethods.com and its availability was announced in the NewsBites newsletter, a technically oriented cybersecurity newsletter with 260,000 subscribers, and in direct emails sent to cybersecurity professionals who had earned at least 2 technical cybersecurity certifications from SANS, ISC2, or OSCP. To verify that respondents were highly-skilled cybersecurity professionals, we asked each respondent to provide a work breakdown between technical tasks and non-technical cybersecurity tasks. Technical tasks include system and application pen testing, secure coding and DevSecOps, security monitoring, forensics, security engineering and architecture, malware and vulnerability analysis, configuring security defenses, and building new security tools. Non-technical cybersecurity tasks include audit and compliance, security awareness education, general and project management, policy, and contracting. As shown in the table below, 55% of respondents spend at least 50% of their time on technical tasks and a full 90% spend at least 10% of their time on those tasks. Further confirming the technical skills of the respondents, 89% reported they hold at least two technical cybersecurity certifications. For the purpose of validating technical cybersecurity skills, we did not count more basic IT certifications such as A+ and Network+

What we know about who responded

They work in organizations large and small

Respondents by organization size

Number of employees	Percent of responses
Greater than 100,000	12.0%
10,000 – 99,999	24.7%
1,000 – 9,999	23.1%
100 – 999	18.2%
Less than 100	7.9%
No response	14.1%

They perform technical as opposed to administrative functions

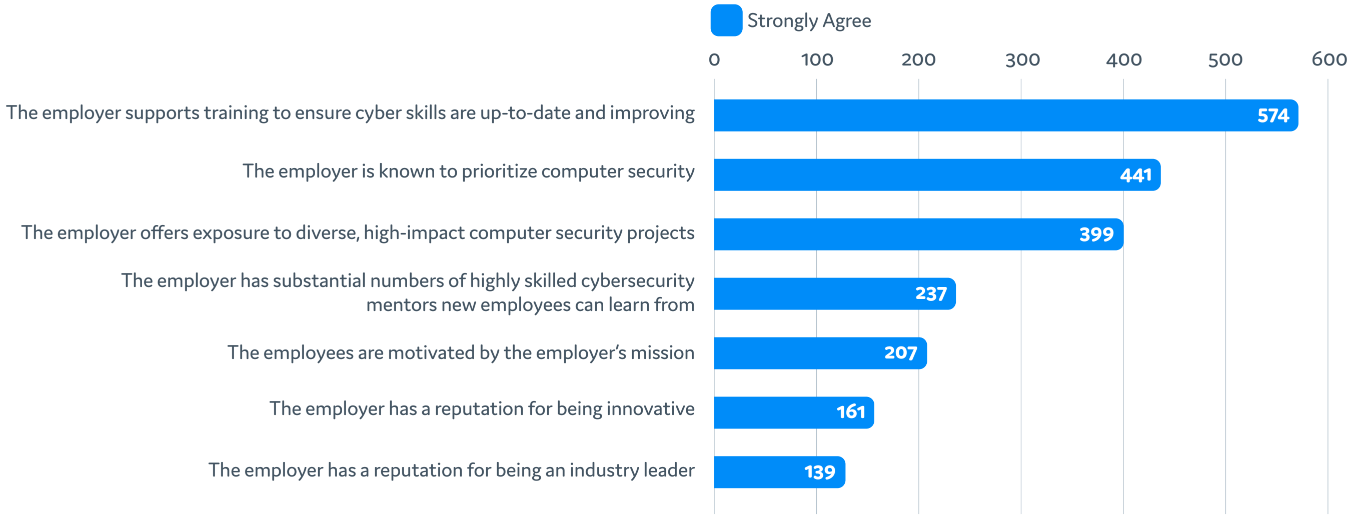
Percent of working time spent on technical tasks

Tasks	75% or more	50%-75%	Less than 50%
System and application pen testing, secure coding and DevSecOps, security monitoring, forensics, security engineering and architecture, malware and vulnerability analysis, configuring security defenses, and building new security tools	33%	22%	45%
Audit and compliance, security awareness education, general and project management, policy, and contracting	9%	13%	78%

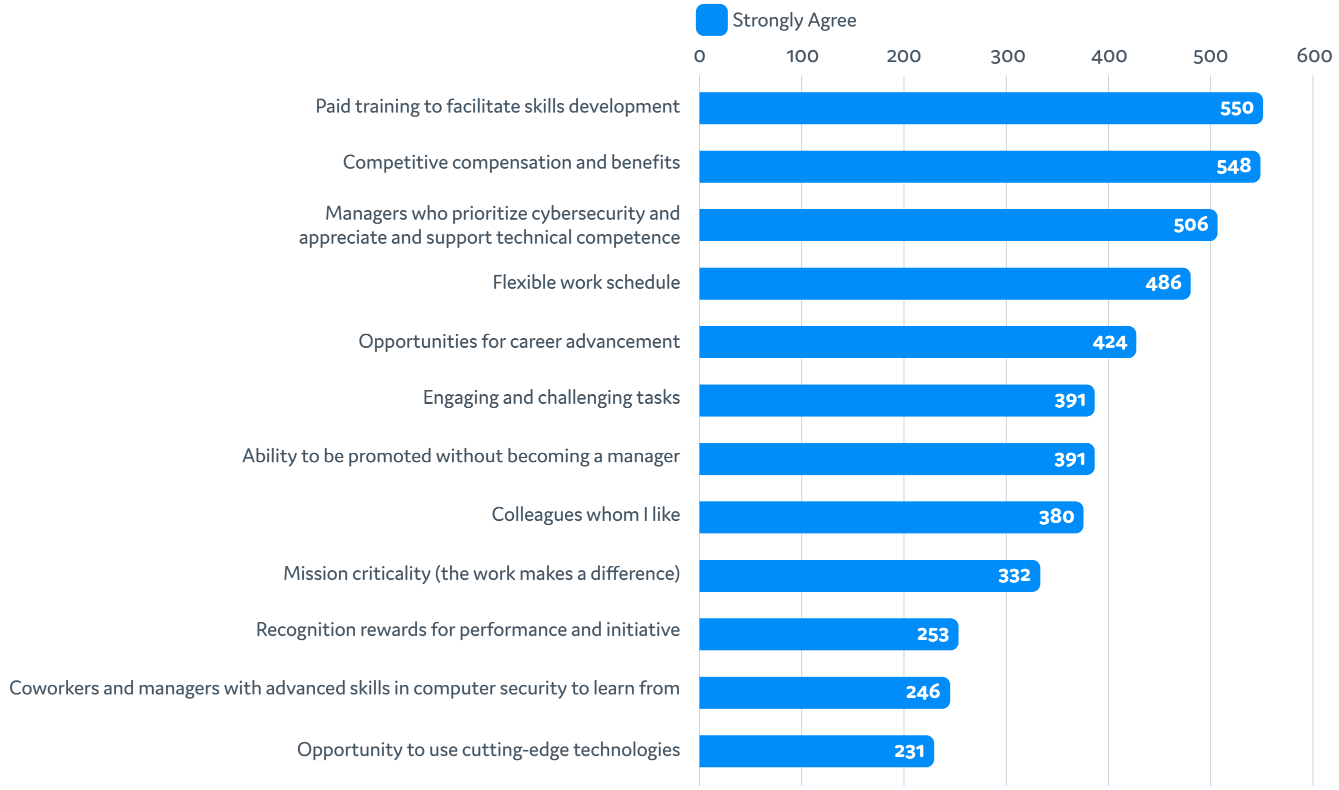
APPENDIX B

SUMMARY OF RESULTS

For an organization that wants to attract highly skilled computer experts, the following factors are the most important:

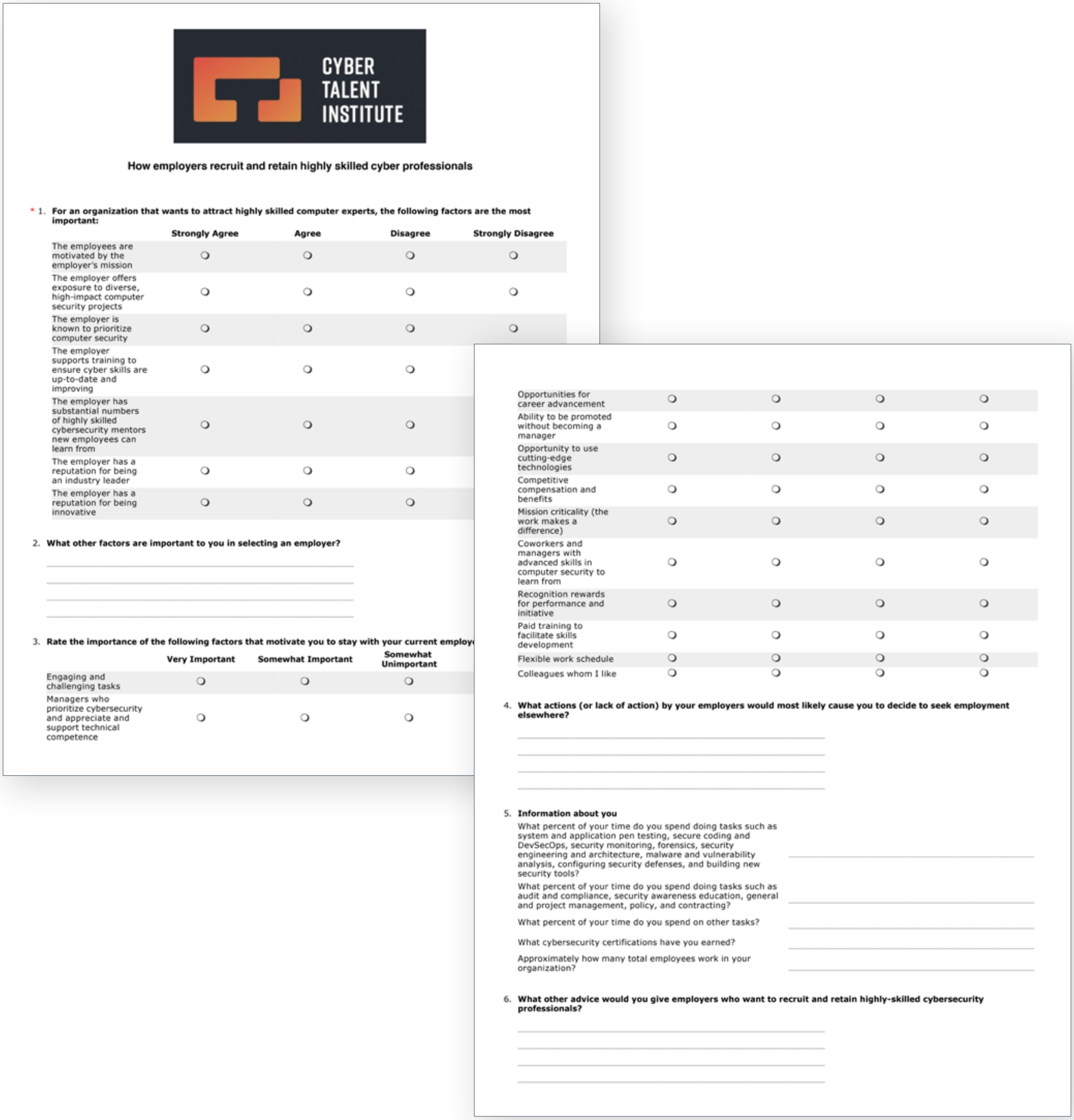


Most important factors in motivating highly skilled cyber professionals to stay in their position:



APPENDIX C

SURVEY INSTRUMENT



CYBER TALENT INSTITUTE

How employers recruit and retain highly skilled cyber professionals

* 1. **For an organization that wants to attract highly skilled computer experts, the following factors are the most important:**

	Strongly Agree	Agree	Disagree	Strongly Disagree
The employees are motivated by the employer's mission	○	○	○	○
The employer offers exposure to diverse, high-impact computer security projects	○	○	○	○
The employer is known to prioritize computer security	○	○	○	○
The employer supports training to ensure cyber skills are up-to-date and improving	○	○	○	
The employer has substantial numbers of highly skilled cybersecurity mentors new employees can learn from	○	○	○	
The employer has a reputation for being an industry leader	○	○	○	
The employer has a reputation for being innovative	○	○	○	

2. **What other factors are important to you in selecting an employer?**

____

____

____

____

3. **Rate the importance of the following factors that motivate you to stay with your current employ**

	Very Important	Somewhat Important	Somewhat Unimportant	
Engaging and challenging tasks	○	○	○	
Managers who prioritize cybersecurity and appreciate and support technical competence	○	○	○	
Opportunities for career advancement	○	○	○	○
Ability to be promoted without becoming a manager	○	○	○	○
Opportunity to use cutting-edge technologies	○	○	○	○
Competitive compensation and benefits	○	○	○	○
Mission criticality (the work makes a difference)	○	○	○	○
Coworkers and managers with advanced skills in computer security to learn from	○	○	○	○
Recognition rewards for performance and initiative	○	○	○	○
Paid training to facilitate skills development	○	○	○	○
Flexible work schedule	○	○	○	○
Colleagues whom I like	○	○	○	○

4. **What actions (or lack of action) by your employers would most likely cause you to decide to seek employment elsewhere?**

____

____

____

____

5. **Information about you**

What percent of your time do you spend doing tasks such as system and application pen testing, secure coding and DevSecOps, security monitoring, forensics, security engineering and architecture, malware and vulnerability analysis, configuring security defenses, and building new security tools? ____________________

What percent of your time do you spend doing tasks such as audit and compliance, security awareness education, general and project management, policy, and contracting? ____________________

What percent of your time do you spend on other tasks? ____________________

What cybersecurity certifications have you earned? ____________________

Approximately how many total employees work in your organization? ____________________

6. **What other advice would you give employers who want to recruit and retain highly-skilled cybersecurity professionals?**

____

____

____

____

CYBER
TALENT
INSTITUTE

www.cybertalentinstitute.org

info@cybertalentinstitute.org