Achieving Diversity in the U.S. Cybersecurity Industry

Sponsored by

Independently conducted by Ponemon Institute LLC
Publication Date: November 2022

Achieving Diversity in the U.S. Cybersecurity Industry

Prepared by Ponemon Institute, November 2022

The purpose of this research is to learn important information about the possibility of a "diversity gap" among the cybersecurity workforce or function today. Sponsored by Security Innovation and Cyversity, Ponemon Institute surveyed 3,870 individuals in the United States who are cybersecurity practitioners about the state of diversity in their organizations.

Cyversity's mission is to achieve the consistent representation of women and underrepresented minorities in the cybersecurity industry through programs designed to diversify, educate and empower. Cyversity offers scholarship opportunities, diverse workforce development, innovative outreach and mentoring programs. In the context of this research, the diversity gap refers to organizations' goal to have a diverse cybersecurity workforce but more proactive measures are needed to close the gap.

Most respondents view a diverse cybersecurity staff as important but recognize that more needs to be done to close the diversity gap. According to Figure 1, 69 percent of respondents say a diverse cybersecurity staff is important. However, only 39 percent of respondents say they work in a diverse cybersecurity workplace. Unfortunately, according to 59 percent respondents, it is not likely (34 percent) or there is no chance (25 percent) that this gap will shrink in the next two to four years.

Figure 1. The diversity gap in the cybersecurity workplace

In other Ponemon Institute studies, a challenge most organizations are having in order to achieve a strong cybersecurity posture is the ability to hire and retain skilled cybersecurity professionals. This recognition should encourage more organizations to take such steps as:

- Establishing cybersecurity apprenticeship programs,
- Allocating resources to fund organizations' efforts to develop cybersecurity diversity programs;
- Providing financial support to cover the costs of certification programs

It is also important to start outreach early on. Organizations should encourage high schools and community colleges to invite cybersecurity practitioners to speak to and mentor students about cybersecurity career opportunities.

Top Level Takeaways

The following findings illustrate the current state of diversity in the workplace

Women are underrepresented in the cybersecurity profession.

More mentoring and recruitment of African American IT security practitioners needs to be done.

Cybersecurity is a young profession.

Not all jobs require an extensive background and education in cybersecurity.

Most respondents have been in their current position less than three years, indicating a high rate of turnover.

Respondents are satisfied with their careers in cybersecurity.

Inability to retain diverse talent makes it difficult to close the diversity gap.

To improve diversity in the workforce, organizations should ensure job candidates understand the expectations they have when hiring.

Key findings

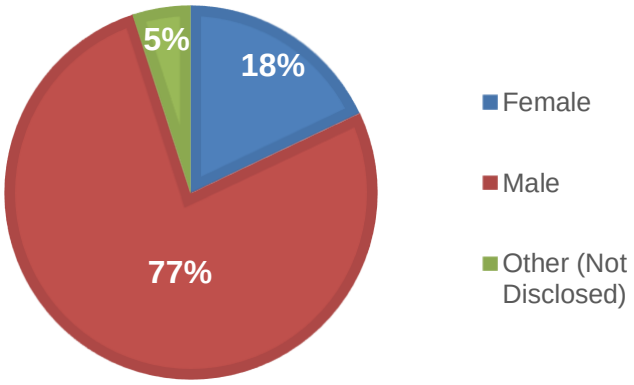
In this section, we analyze the findings of the research. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics.

- Profile of respondents
- Organizational characteristics
- The diversity gap
- Cybersecurity skills in demand

Women are underrepresented in the cybersecurity profession.

According to Figure 2, the cybersecurity profession is dominated by males with only 18 percent of respondents female.

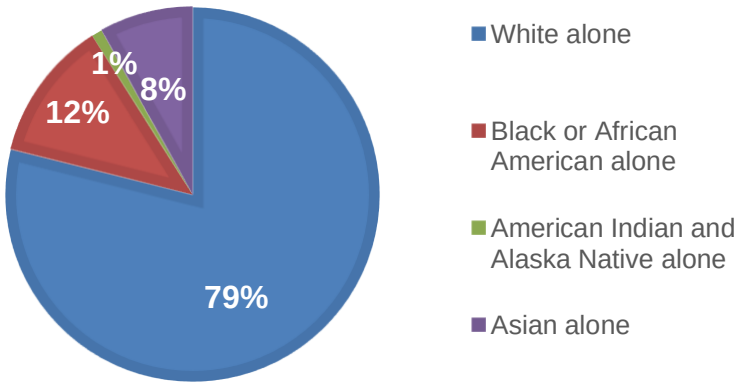
Figure 2. Workforce gender



Today's workforce is not diverse.

Sixty-nine percent of respondents say a diverse cybersecurity staff is important. However, only 39 percent of respondents report that they work in a diverse workplace currently. Further, only 12 percent of respondents are identified as African American, which is a full percentage lower than the 13 percent of African Americans in the total US workforce, according to 2018 US Bureau of Labor and Statistics data.

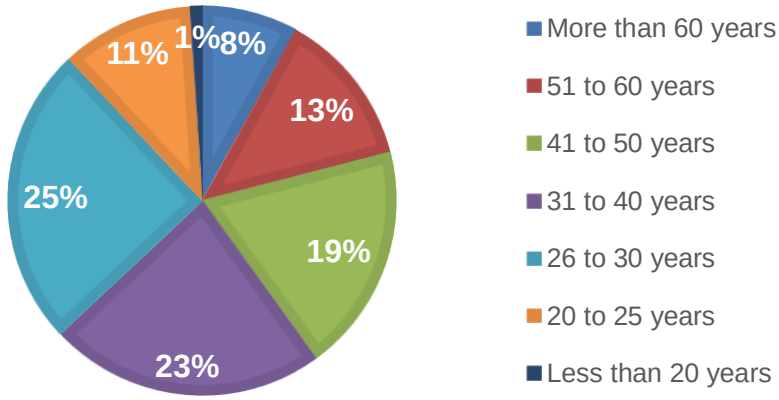
Figure 3. Race of workforce



Cybersecurity is a young profession.

As shown in Figure 4, 60 percent of respondents are below the age of 40. To achieve a more age-diverse workforce, organizations should be reaching out to those who are older and more seasoned cybersecurity practitioners.

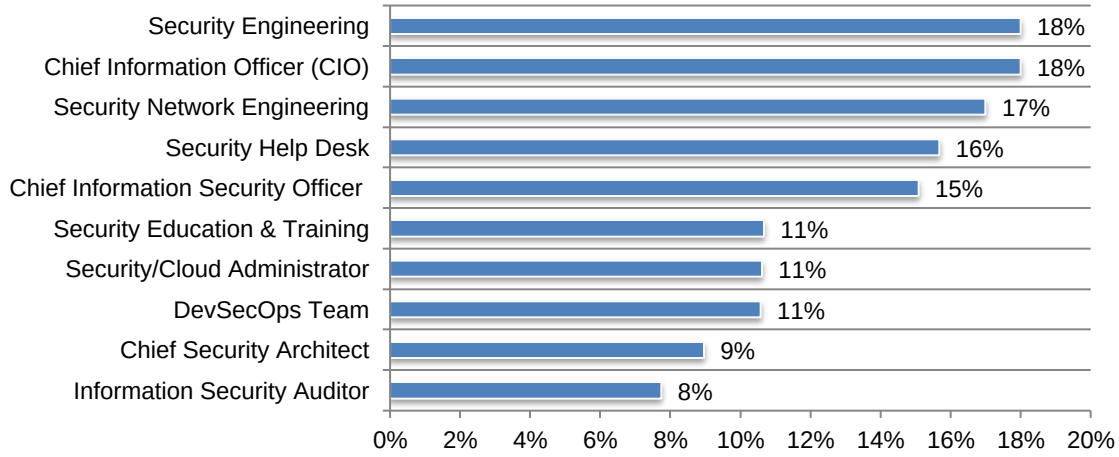
Figure 4. Age range of respondents



The top professions represented in this research require extensive background and education in cybersecurity. Figure 5 presents a list of the job titles of respondents. Eighteen percent of respondents say they are security engineers and CIOs. Seventy-five percent of respondents have at least one professional certification. However, only 37 percent of respondents have a four-year degree (23 percent) or a graduate degree (14 percent). As discussed previously, one step to take to improve the hiring and retaining of individuals from different ethnic and gender groups is to offer reimbursement for those who pursue certification.

As shown in this research, 61 percent of respondents say certifications and 56 percent of respondents say education are ideal characteristics of a diverse workforce.

Figure 5. Job titles

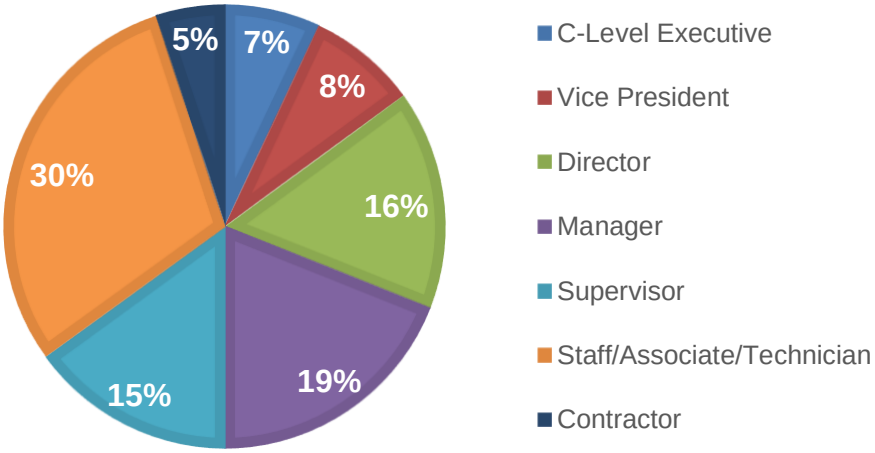


Cybersecurity expertise of respondents

The largest segment of position level is staff/associate/technician.

As discussed previously, cybersecurity is largely comprised of younger individuals (60 percent). According to Figure 6, this could be reflected in the position level of respondents. Almost half (45 percent of respondents) are either a supervisor (15 percent) or staff/associate/technician. Only 31 percent of respondents are at the director level or above.

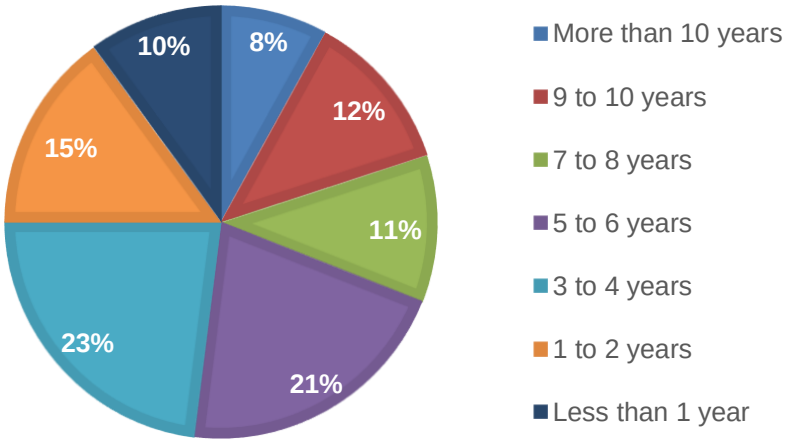
Figure 6. Current position level



Most respondents have been in their current position less than three years.

The most significant barrier to closing the diversity gap is the inability to retain a diverse cybersecurity workforce. Fifty-nine percent of respondents have been in their current position three years or less. Only 20 percent of respondents say they have been in their current position nine years or more. This could indicate respondents' changing organizations or changing current positions within their organizations.

Figure 7. Length of time in respondents' current position

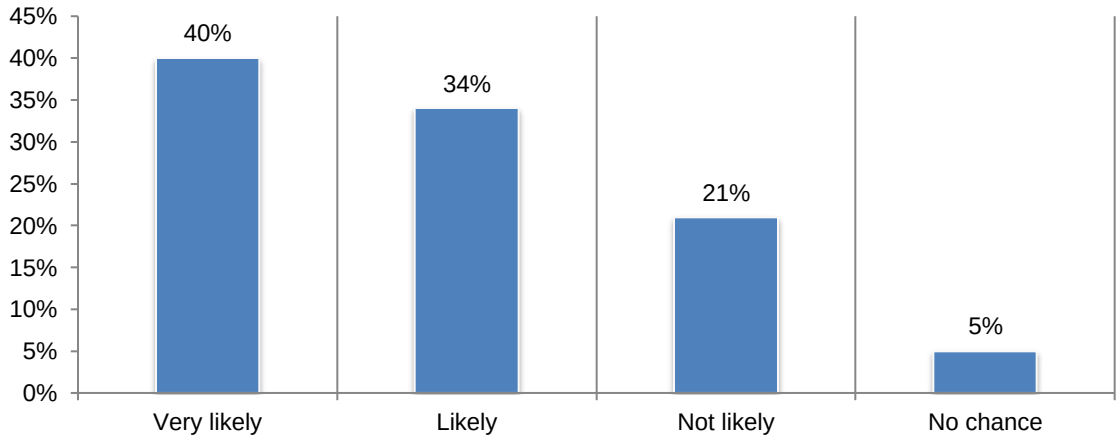


Respondents are positive about staying in the cybersecurity profession.

Although retaining cybersecurity practitioners is considered a problem, 74 percent of respondents say they are very likely (40 percent) or likely (34 percent) to remain in the cybersecurity profession—but not necessarily in their current organization.

- Almost half of respondents (49 percent) say they spend at least 61 percent of their time on cybersecurity activities.
- Salaries and benefits are considered adequate or more than adequate by 83 percent of respondents.

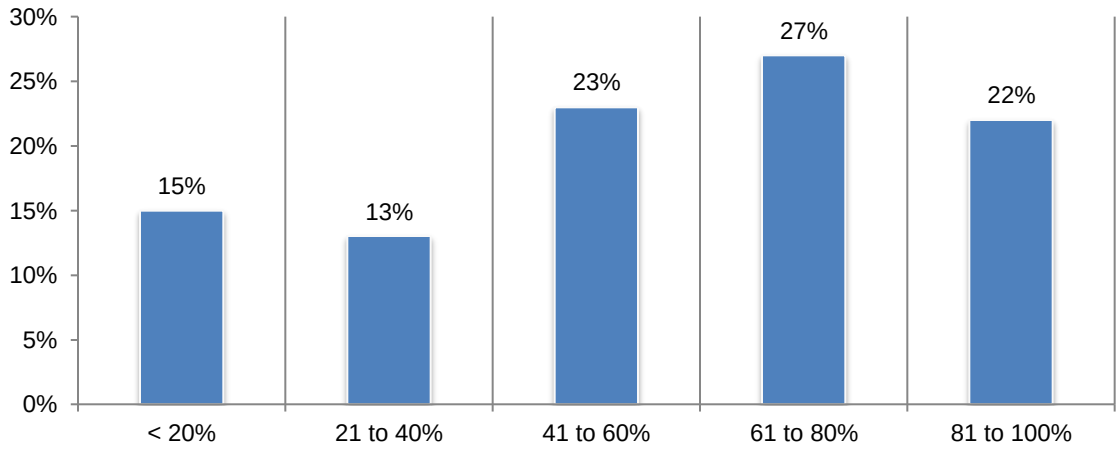
Figure 8. Likelihood of remaining in the cybersecurity profession over the next two-to-four years



Most respondents are spending the majority of their time in cybersecurity activities.

According to Figure 9, almost half of respondents (49 percent) say they spend at least 61 percent of their time on cybersecurity activities.

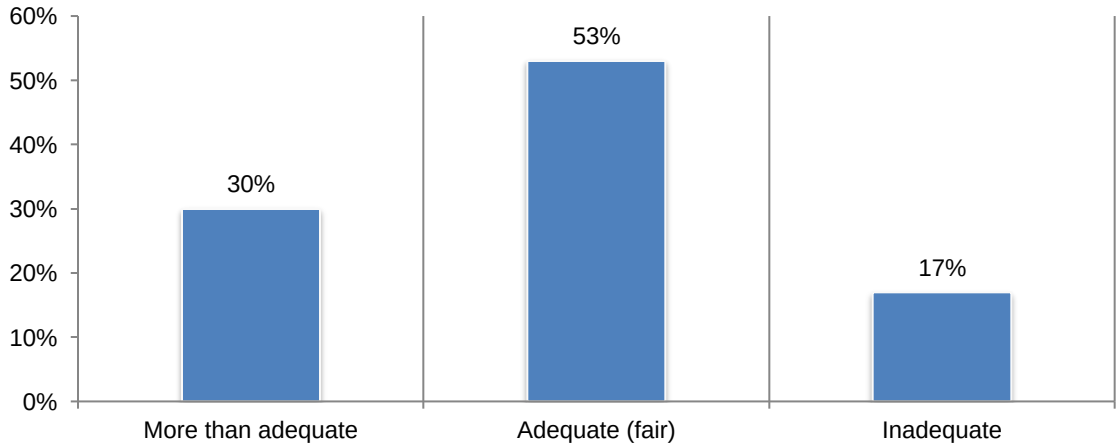
Figure 9. Percentage of respondent's job role dedicated to cybersecurity



Salary and benefits are considered adequate or more than adequate.

As shown in Figure 10, 53 percent of respondents say their benefits are fair and 30 percent say benefits are more than adequate.

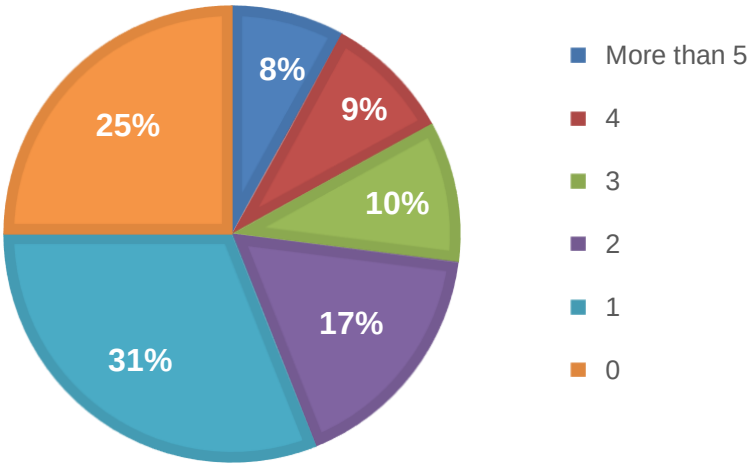
Figure 10. Adequacy of salary and benefits



Most respondents have at least one professional certification.

As shown in Figure 11, 75 percent of respondents have at least one certificate and 17 percent of respondents have at least four.

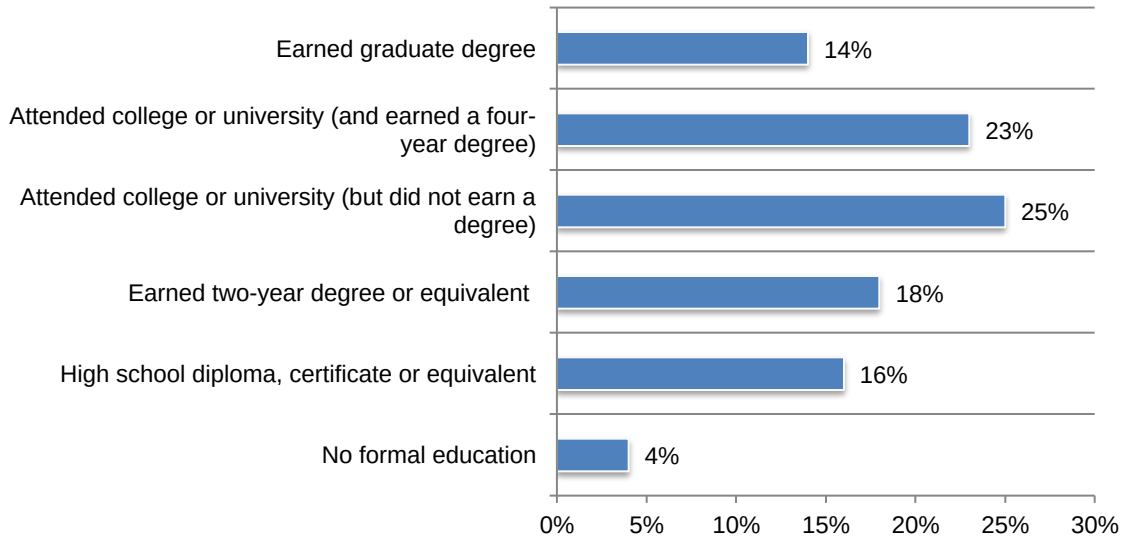
Figure 11. Professional certifications



While most respondents have a professional certification, few have advanced degrees.

Only 37 percent of respondents have a four-year degree (23 percent) or a graduate degree (14 percent), as shown in Figure 12.

Figure 12. Highest level of education

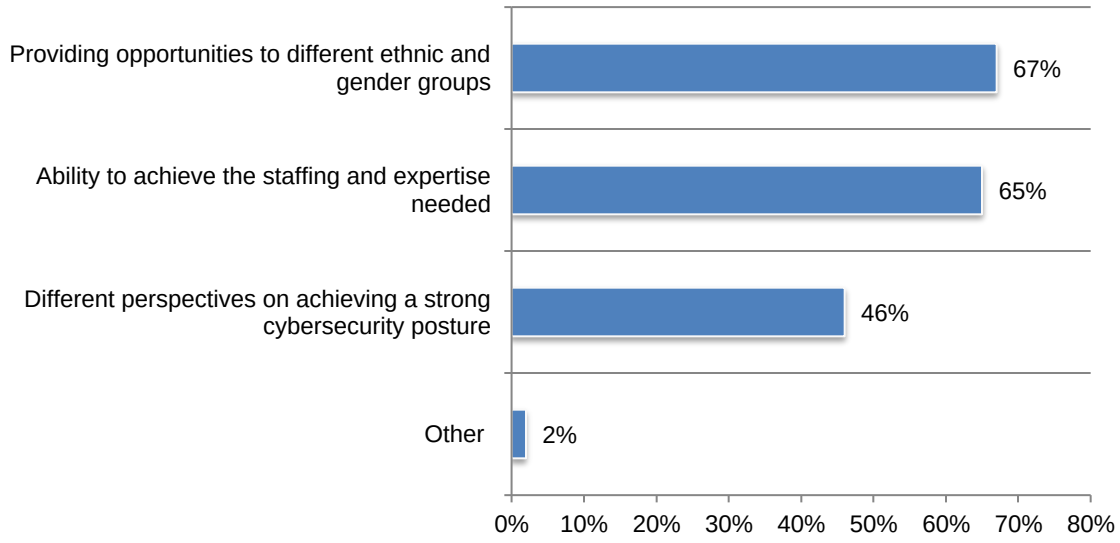


The diversity gap

Providing employment opportunities and having the necessary expertise are the top benefits from closing the diversity gap.

According to Figure 13, 67 percent of respondents say it is the ability to provide opportunities to different ethnic and gender groups and 65 percent say it is have the staff and expertise to achieve a strong cybersecurity posture.

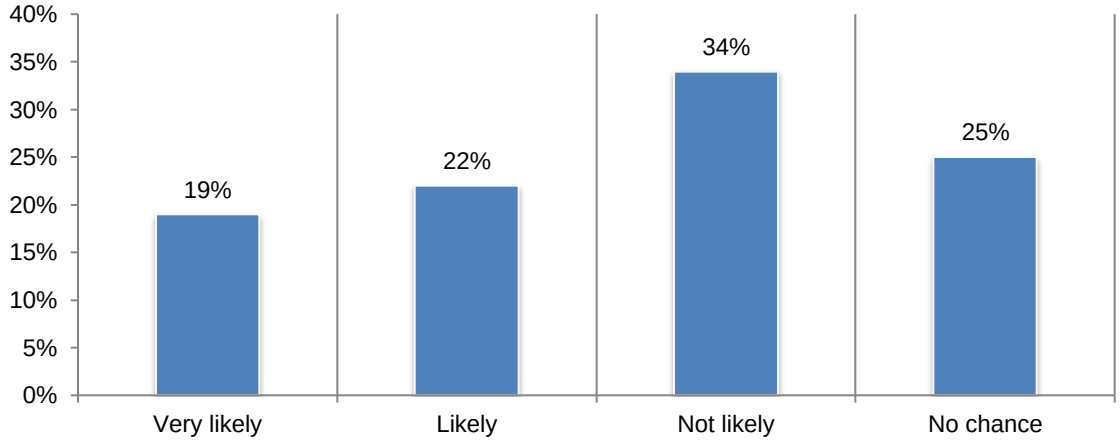
Figure 13. The benefits of a diverse cybersecurity workforce
More than one choice permitted



There is little optimism that the diversity gap will shrink.

According to Figure 14, 59 percent of respondents say it is not likely or no chance that their organizations will become more diverse.

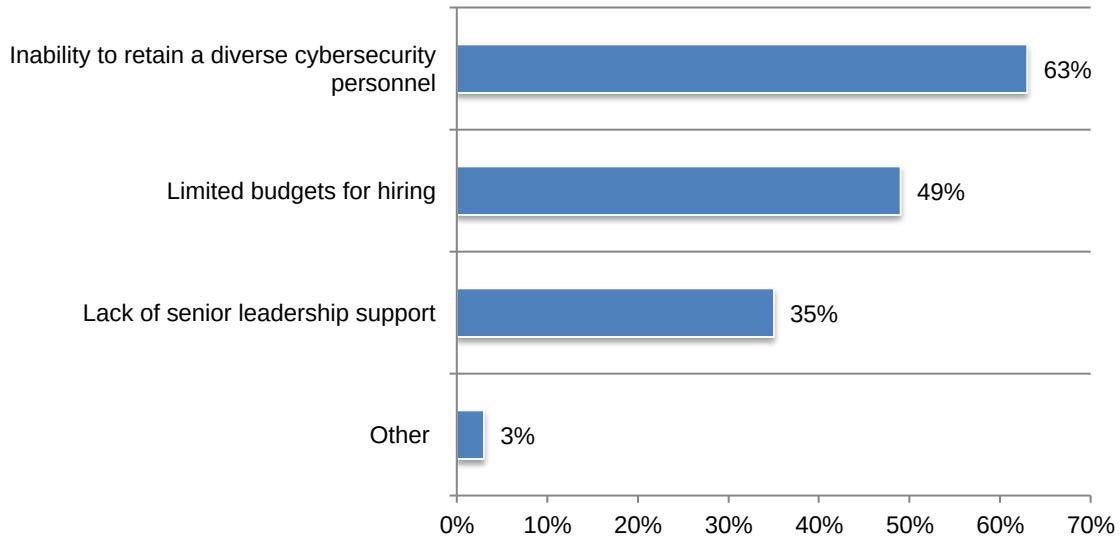
Figure 14. Likelihood the diversity gap will shrink over the next two-to-four years



The inability to retain a diverse cybersecurity workforce is making it difficult to close the diversity gap.

According to Figure 15, 63 percent of respondents say retaining women and other underrepresented individuals is the main reason for not having a diverse workforce. Budgets and lack of senior leadership support are not as much a barrier.

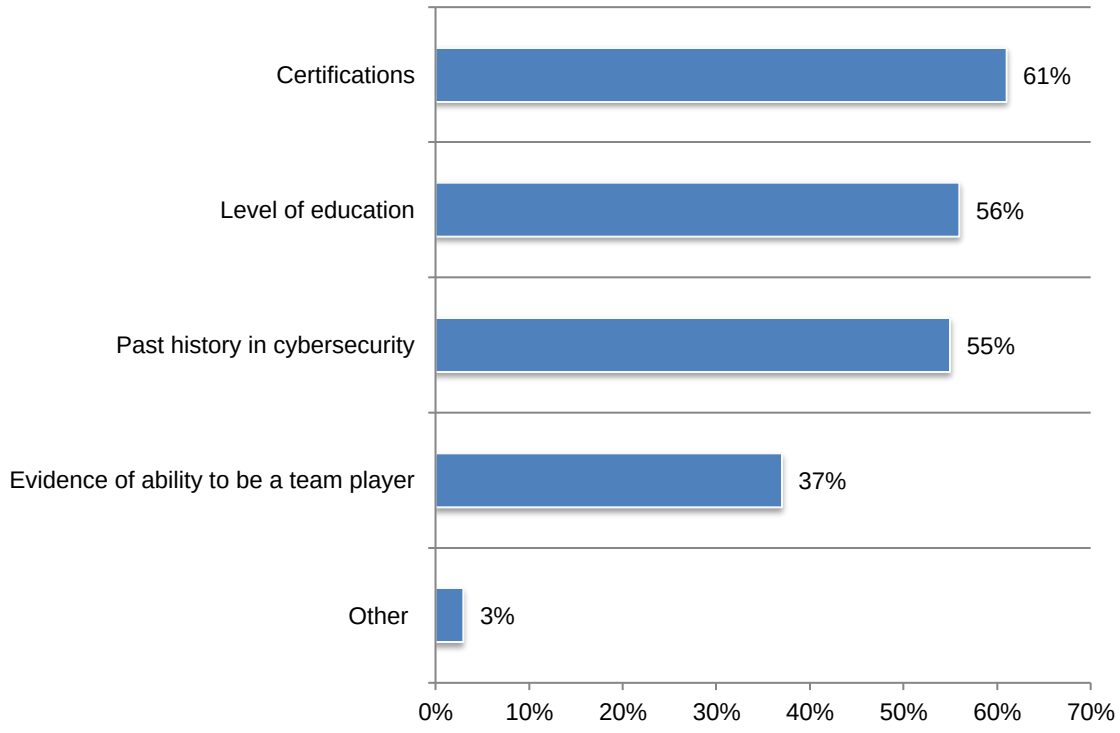
Figure 15. The significant barriers to achieving a diverse cybersecurity workforce



Organizations prefer job candidates with cybersecurity certifications and education.

As shown in Figure 16, 61 percent of respondents say certifications and 56 percent of respondents say education are important when hiring a diverse workforce.

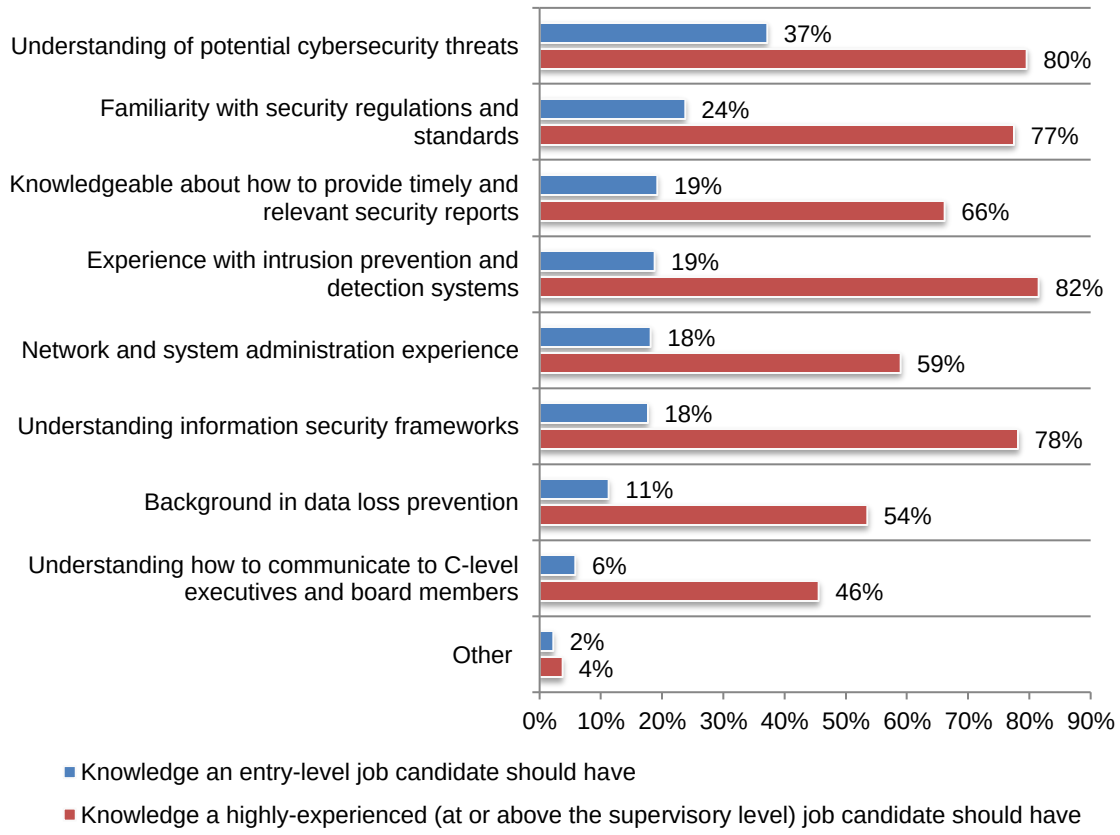
Figure 16. What are the ideal characteristics of a diverse workforce?
More than one response permitted



To improve diversity in the workforce, organizations should ensure job candidates understand the expectations they have when hiring.

An understanding of potential cybersecurity threats is important for both entry-level and highly experienced job candidates.[1] In another Ponemon Institute study, IT and IT security practitioners were asked what knowledge and experience are desired by their organizations. As shown in Figure 17, highly experienced job candidates are expected to be knowledgeable about a wide range of governance and technology issues. These include an understanding of potential cybersecurity threats, experience with intrusion prevention and detection systems, and familiarity with security regulations and standards. According to another Ponemon Institute study, entry-level job candidates are expected to have more tactical technical skills, such as installing firewall and data encryption programs and maintaining security records of monitoring and incident response activities.

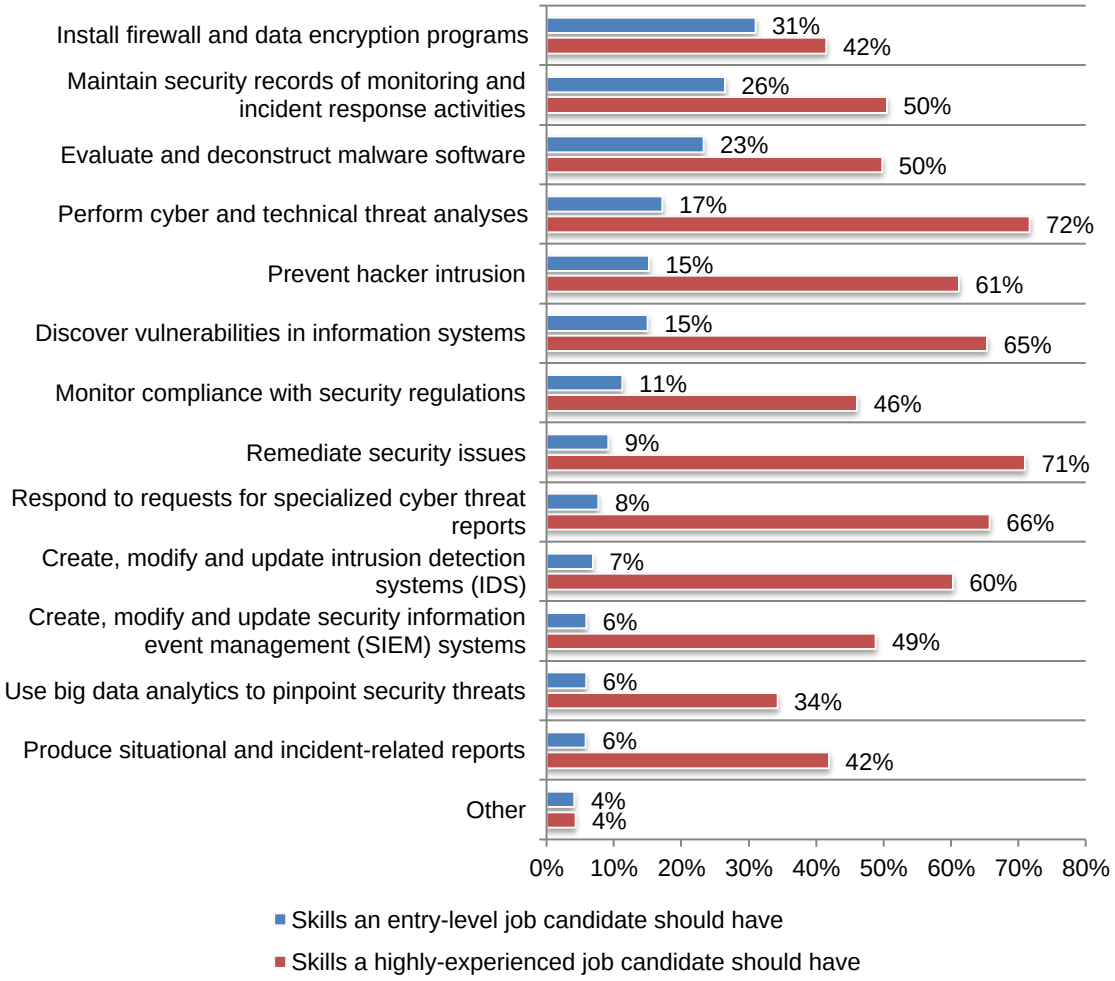
Figure 17. What knowledge should entry-level and highly experienced job candidates have?
More than one response permitted



[1] "Staffing the IT Security Function in the Age of Automation: A Study of Organizations in the US, UK and APAC", conducted by Ponemon Institute and sponsored by Domain Tools, 2019.

Figure 18 shows that entry-level job candidates are expected to have more tactical technical skills, such as installing firewall and data encryption programs and maintaining security records of monitoring and incident response activities. Highly experienced job candidates, on the other hand, are mostly expected to have the skills to perform cyber and technical threat analyses, remediate security issues, and respond to requests for specialized cyber threat reports.

Figure 18. What IT security technical skills should entry-level and highly experienced job candidates have?
More than one response permitted



Appendix: Organizational characteristics

Organizations represented in this study are either buyers of technologies and outsourced services or sellers or vendors.

Figure 19. Cybersecurity function in the organization

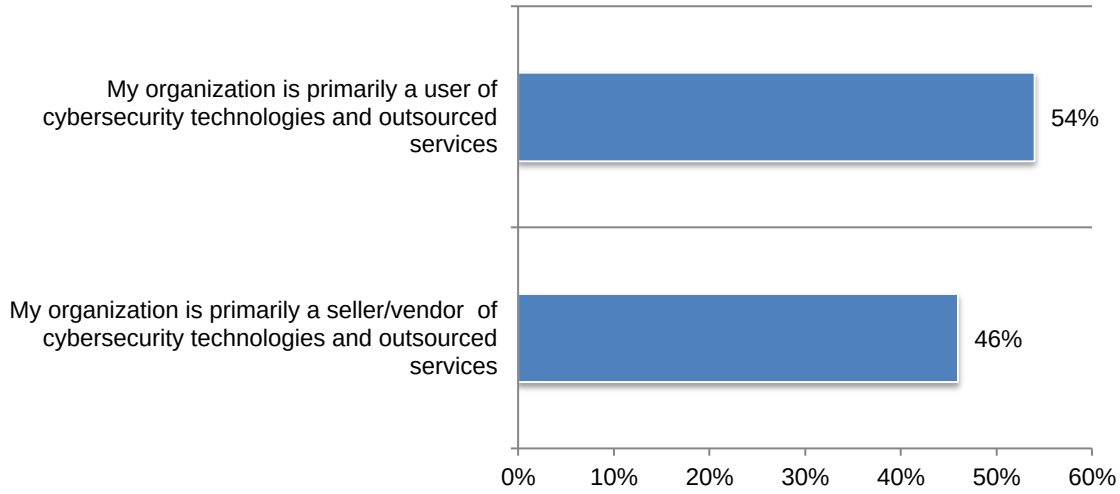
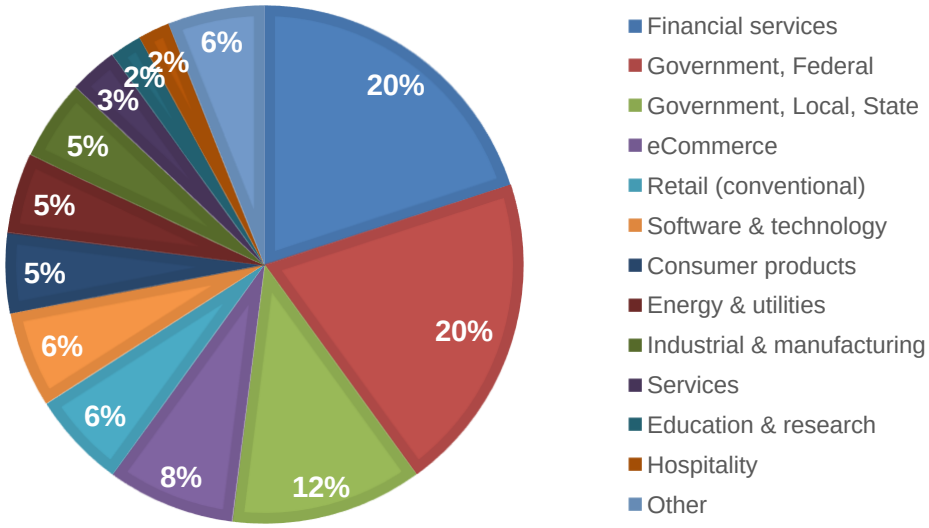


Figure 20 provides the list of the verticals represented in this study.
Financial services and the federal government are the largest sectors in the study.

Figure 20. Industry sector



The following table summarizes our sampling plan, which consists of five independent studies that we use to derive key demographics that relate to diversity among the cybersecurity workforce. All studies were launched in the Fall of 2021. The sum of these statistically valid sampling plans is 96,035 qualified cybersecurity professionals. The consolidated final sample is 3,870 individuals – or a response rate of 4.0 percent. In summary, the estimated total population (size) of the U.S. cybersecurity workforce is 2,383,132. Using a 95 percent confidence interval, we compute an upper bound at 2,740,602 and lower bound at 2,025,662.

Survey response (U.S. Sample)	Month launched	Freq	Samples
Sampling frame 1	9/10/21	17,450	668
Sampling frame 2	9/25/21	19,072	802
Sampling frame 3	10/21/21	21,334	855
Sampling frame 4	11/6/21	18,619	763
Sampling frame 5	11/17/21	19,560	782
Totals		96,035	3,870

Appendix: Detailed Survey Results

Demographics

Q1. Age range of workforce:	Pct%
Less than 20 years	1%
20 to 25 years	11%
26 to 30 years	25%
31 to 40 years	23%
41 to 50 years	19%
51 to 60 years	13%
More than 60 years	8%
Total	100%
Extrapolated value (age)	38.2

Q2. Gender of workforce:	Pct%
Female	18%
Male	77%
Other (Not Disclosed)	5%
Total	100%

Q3. Race of workforce:	Pct%
White alone	78.5%
Black or African American alone	12.1%
American Indian and Alaska Native alone	1%
Asian alone	8.0%
Total	100%

Q4. Hispanic or Latino Status (ethnic code)	Pct%
Not a member of the Hispanic or Latino community	77%
Member of the Hispanic or Latino community	23%
Total	100%

Q5. U.S. Veteran Status of workforce	Pct%
Served (or presently served) in the U.S. military	5.3%
Did not serve in the U.S. military	94.7%
Total	100.0%

Cybersecurity Expertise of Respondents

Q6. Please select the job title that best describes your role or function within the cybersecurity industry today? Please select all that apply..	Pct%
Security Engineering	18%
Chief Information Officer (CIO)	18%
Security Network Engineering	17%
Security Help Desk	16%
Chief Information Security Officer (CISO)	15%
Security Education & Training	11%
Security / Cloud Administrator	11%
DevSecOps Team	11%
Chief Security Architect	9%
Information Security Auditor	8%
Information Assurances	8%
Chief Security Officer (CSO)	6%
Chief Data Protection Officer (DPO)	4%
Security Staff Recruitment & Retention	4%
Data Center Management	3%
Threat Hunting Team	3%
Security Products Testing	3%
Legal Counsel/Security	3%
Chief Privacy Officer (CPO)	2%
Security by design (SbD)	2%
Security Intelligence	2%
Cybersecurity Certification	2%
Security Operation Center (SOC)	1%
Other	1%

Q7. Please select your current position level in your organization?	Pct%
C-Level Executive	7%
Vice President	8%
Director	16%
Manager	19%
Supervisor	15%
Staff/Associate/Technician	30%
Contractor	5%
None of the above	0%
Total	100%

Q8. How long have you held this position?	Pct%
Less than 1 year	10%
1 to 2 years	15%
3 to 4 years	23%
5 to 6 years	21%
7 to 8 years	11%
9 to 10 years	12%
More than 10 years	8%
Total	100%
Extrapolated value (years)	5.2

Q9. How many professional certifications relating to cybersecurity do you hold? (E.g., CISSP, CISA, CISM, GiAC,, CEH, and more)	Pct%
0	25%
1	31%
2	17%
3	10%
4	9%
Extrapolated value (number of certifications)	8%
Total	100%
Extrapolated value (number of certifications)	1.7

Q10. What best describes your highest level of education attained?	Pct%
No formal education	4%
High school diploma, certificate or equivalent	16%
Earned two-year degree or equivalent	18%
Attended college or university (but did not earn a degree)	25%
Attended college or university (and earned a four-year degree)	23%
Earned graduate degree	14%
Total	100%

Q11. What best describes the cybersecurity function within your organization?	Pct%
My organization is primarily a user of cybersecurity technologies and outsourced services	54%
My organization is primarily a seller/vendor of cybersecurity technologies and outsourced services	46%
Total	100%

Q12. What best describes your organization's primary industry sector? Please select only one best choice	Pct%
Agriculture & food services	1%
Communications	1%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
eCommerce	8%
Energy & utilities	5%
Entertainment & media	1%
Financial services	20%
Health & pharma	1%
Hospitality	2%
Industrial & manufacturing	5%
Government, Federal	20%
Government, Local, State	12%
Retail (conventional)	6%
Services	3%
Software & technology	6%
Transportation	1%

Q13. What best describes the U.S. regional location where you are located?	Pct%
Northeast	20%
Mid-Atlantic	18%
Midwest	17%
Southeast	13%
Southwest	12%
Pacific West	20%
Total	100%

Q14. Do you plan to remain in the cybersecurity profession (or another related field) over the next two-to-four years?	Pct%
Very likely	40%
Likely	34%
Not likely	21%
No chance	5%
Total	100%

Q15. What describes the percentage of your job role dedicated to cybersecurity?	Pct%
< 20%	15%
21 to 40%	13%
41 to 60%	23%
61 to 80%	27%
81 to 100%	22%
Total	100%
Extrapolated value	56.4%

Q16. In the context of your job, what best describes the adequacy of compensation (salary and benefits)	Pct%
More than adequate	30%
Adequate (fair)	53%
Inadequate	17%
Total	100%

State of Diversity

Q17. Do you believe the "diversity gap" among qualified cybersecurity staff and available job openings will close over the next two-to- four years?	Pct%
Very likely	19%
Likely	22%
Not likely	34%
No chance	25%
Total	100%

Please rate the following statement using the scale provided below each item.

Q18. How would you characterize the diversity of your cybersecurity staff? Please use the following scale from 1 = not diverse to 10 = highly diverse	Pct%
1 or 2	13%
3 or 4	25%
5 or 6	23%
7 or 8	21%
9 or 10	18%
Total	100%
Extrapolated value	5.62

Q19. How important is a diverse cybersecurity staff? Please use the following scale from 1 = not important to 10 = highly important.	Pct%
1 or 2	8%
3 or 4	7%
5 or 6	16%
7 or 8	31%
9 or 10	38%
Total	100%
Extrapolated value	7.18

Q20. What are the most significant barriers to achieving a diverse cybersecurity workforce? Please select all that apply.	Pct%
Lack of senior leadership support	35%
Limited budgets for hiring	49%
Inability to retain a diverse cybersecurity personnel	63%
Other (please specify)	3%
Total	150%

Q21. What are the benefits of a diverse cybersecurity workforce? Please select all that apply.	Pct%
Different perspectives on achieving a strong cybersecurity posture	46%
Providing opportunities to different ethnic and gender groups	67%
Ability to achieve the staffing and expertise needed	65%
Other (please specify)	2%
Total	180%

Q22. What are the ideal characteristics of a diverse workforce? Please select all that apply.	Pct%
Level of education	56%
Certifications	61%
Past history in cybersecurity	55%
Evidence of ability to be a team player	37%
Other (please specify)	3%
Total	212%

Thank you for your participation. All responses are completely confidential.
Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.