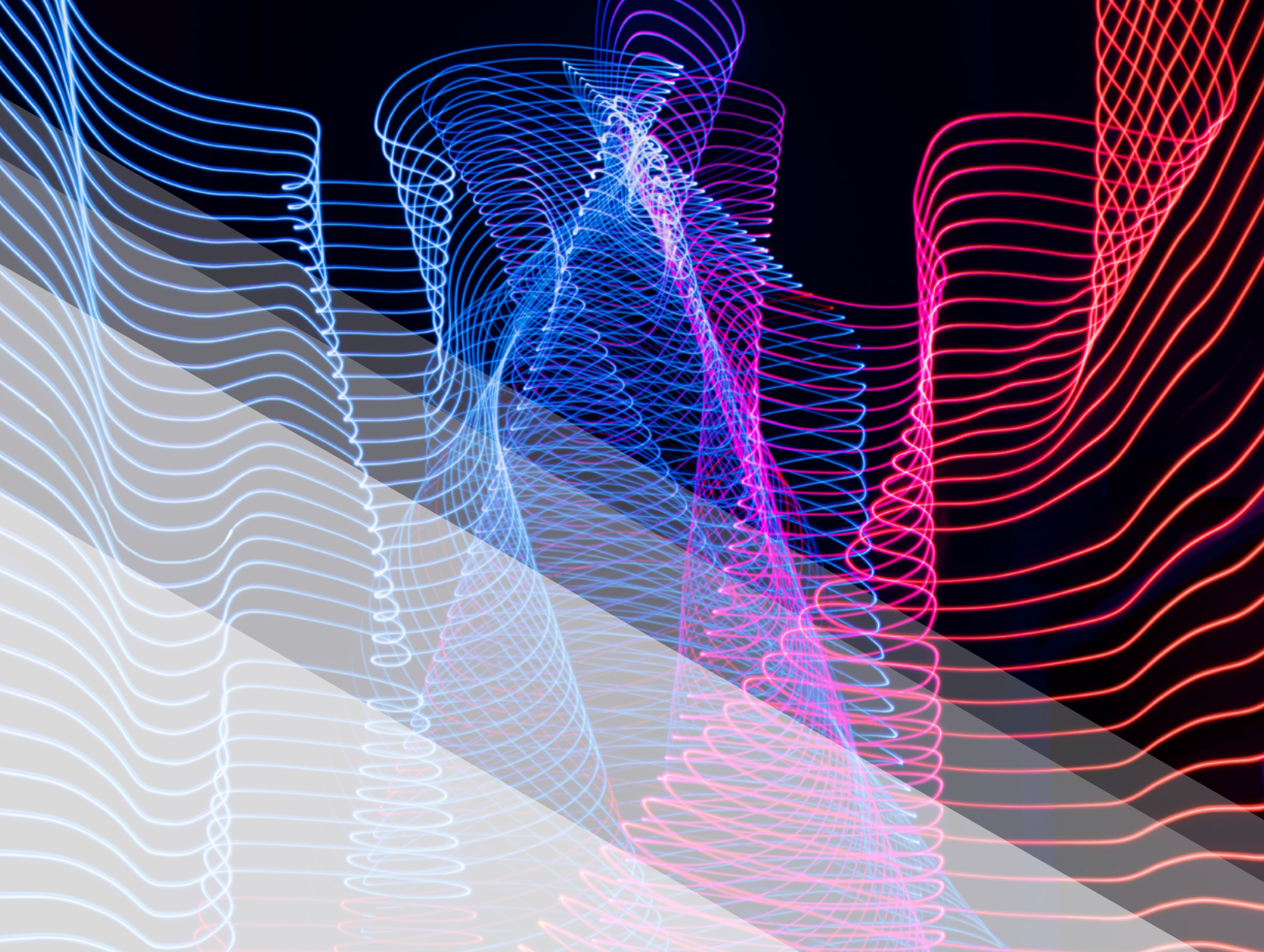


Diversity, Equity, and Inclusion in Cybersecurity

SEPTEMBER 2021

ASPEN DIGITAL
aspen institute

ASPEN TECH POLICY HUB
aspen institute

Following two workshops on diversity, equity, and inclusion (DEI), an intergenerational, multidisciplinary, and multicultural group of cybersecurity professionals from across the private and public sectors proposed the following priority approaches for achieving better DEI in cybersecurity:

- Organize a coalition to assess the value of certifications in developing quality candidates for cybersecurity jobs;
- Survey participants in cybersecurity apprenticeship programs to better support diverse candidates;
- Collect and share anonymous data about characteristics that prove useful for successful hiring for cybersecurity jobs;
- Establish a group of pro bono experts to help cybersecurity employers rewrite their job descriptions without jargon and focus on the skills required;
- Reconsider whether the current criminal background check process is appropriate, fair, and equitable;
- Establish a task force to track C-suite executives' commitments to DEI initiatives related to cybersecurity professionals within their companies;
- Develop a coalition to identify best practices for mentoring diverse cybersecurity practitioners and create shared resources; and
- Cultivate brand, advertiser, and media influencer partnerships and develop a campaign to reshape narratives around cybersecurity professionals.

These recommendations need to be supported by accountability and incentive structures that enable the private and public sector to adopt them.

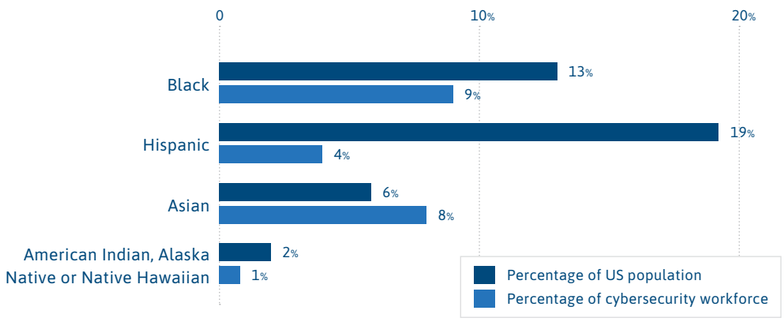
Cover image by Tim Mossholder (unsplash)

Image by Gerd Altmann (Pixabay)

Introduction

Following the national reckoning on racial justice in mid-2020 prompted by the murders of George Floyd, Breonna Taylor, and other Black Americans, it became clear that current diversity, equity, and inclusion (DEI) efforts, however well-meaning, have not addressed the overwhelming white-ness and male-ness of the cybersecurity field. The field remains remarkably homogeneous, both among technical practitioners and policy thinkers, and there are few model programs or initiatives that have demonstrated real progress in building diverse and inclusive teams. It is estimated that only 4% of cybersecurity workers self-identify as Hispanic, 9% as Black, and 24% as women.[1] Moreover, many conversations about the lack of diversity in cybersecurity have fallen flat; they often include participants from similar occupational backgrounds and positions, have need of measurable deliverables and executive leadership buy-in, and lack the specificity and funding needed to make progress. Additionally, individual and institutional commitments are often not supported by formal structures to ensure accountability and provide incentives for change.

Racial and Ethnic Diversity in the Cybersecurity Workforce



Sources: Jason Reed and Jonathan Acosta-Rubio, "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce," Frost & Sullivan, 2019, https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx; United States Population Estimates, 2019," US Census Bureau, accessed July 18, 2021, https://www.census.gov/quickfacts/fact/table/US/SB0050212.

Women in Cybersecurity

Sources: "Women in Cybersecurity: Young, Educated and Ready to Take Charge," (ISC)², accessed August 20, 2021, https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx-?la=en&hash=4C3B33AABFBEAFDDA211856CB274EBDDF9DBEB38; "United States Population Estimates, 2019," US Census Bureau, accessed July 18, 2021, https://www.census.gov/quickfacts/fact/table/US/SB0050212.

One key gap in the ecosystem was that no organization had convened an intergenerational and cross-disciplinary group of cybersecurity professionals to develop a concrete, impact-oriented set of commitments focused on improving DEI in cybersecurity. With the support of the Hewlett Foundation and consultant Camille Stewart, Aspen Digital convened a series of roundtable discussions in October 2020 and February 2021 that brought together leading cybersecurity professionals with representatives from affinity groups and other diverse bodies. The first meeting established concrete, actionable commitments to be made across the cybersecurity ecosystem, and the second reviewed progress made toward those commitments and refined plans. Over

60 attendees participated, representing academia, cybersecurity firms, government agencies, multinational corporations, nonprofits, and startups. The meetings were convened under the Chatham House Rule, protecting the identities of individual participants.[2]

At the meetings, participants were divided into groups based on five subtopics:

- Education;
- Recruiting and Hiring;
- Retention;
- Mentorship; and
- Shifting the Narrative.

This report summarizes each group's recommendations along two dimensions:

1. Actions that single actors (companies, executives, nonprofits, etc.) can take right now with existing resources, and
2. Actions that would require additional support (funding, staff time, etc.) to get off the ground. In section II, we summarize priority recommendations where additional investment from industry or philanthropy is required. In section III, we review each of the five subtopic themes and detail the recommendations developed by our participants.

Aspen Digital would like to thank the following:

- Camille Stewart and #ShareTheMicInCyber for their leadership in this space and outstanding organization of the roundtables;
- Kelly Born, Monica Ruiz, and Eli Sugarman for the support of the William and Flora Hewlett Foundation;
- Meha Ahluwalia and Mai Sistla of the Aspen Tech Policy Hub for serving as lead authors of this report, and Vivian Schiller, Zaki Barzinji, and Betsy Cooper for their contributions;
- Chuck Kapelke for excellent editorial advice, and CCM.design for laying out this report; and
- All the participants of the roundtables who contributed their time and ideas to advancing this work.

This report is dedicated to Savilla Pitt, who led this work until her untimely passing from pancreatic cancer in January 2021. We know Savilla would very much hope that this work will grow to have a significant impact.

Photo by ThisisEngineering RAEng (Unsplash)

Image by Christina (wocintechchat.com)

EXECUTIVE SUMMARY

Key Recommendations Requiring Additional Institutional Investment

Throughout the two workshops, participants agreed that making meaningful progress on DEI requires further investment from industry or philanthropy, through funding, staff time, leadership, and technology. Many of the organizations represented at the workshop have been developing their own individual DEI plans, but most agreed that real progress will require gathering further evidence about best practices, and establishing broader goals that individual companies and organizations can work toward.

Workshop attendees identified the following priority needs that would require additional investment:

Education

- **Organize a coalition to assess the value of certifications in developing quality candidates for cybersecurity jobs.** Over the past decade, numerous cybersecurity certification programs have emerged in an effort to close the cybersecurity skills gap and increase the number of non-traditional candidates entering the field. However, there is little evidence about whether these programs have been effective. Moreover, the costs associated with these programs may present additional barriers. A coalition of cybersecurity managers and human resource professionals should invest in research to assess the efficacy of these certification programs across the field, and use the findings to advise the industry about its use of certifications to evaluate candidates.
- **Survey participants in cybersecurity apprenticeship programs to better support diverse candidates.** While apprenticeships allow students to develop practical skills through hands-on experience at cybersecurity workplaces, they are not always best equipped to support students of diverse backgrounds. Conducting a survey of past apprenticeship participants, applicants, and employers — with specific attention to the experiences and outcomes of diverse participants — will help determine weaknesses in existing apprenticeship programs. Such a survey would likely identify additional opportunities to improve the success of diverse candidates.

Recruitment and Hiring

- **Collect and share anonymous data about the characteristics that prove useful for successful hiring of cybersecurity jobs.** It is often difficult to identify what characteristics of candidates are most likely to lead to successful job hires, which makes it difficult to replicate success in future hiring. A data repository containing sample profiles of successful hires from a wide diversity of experiential, educational, and cultural backgrounds could help hiring managers adjust job requirements and focus on the skills new hires actually need.
- **Establish a group of pro bono experts to help cybersecurity employers rewrite their job descriptions without jargon and focus on the skills required.** Currently, many cybersecurity job descriptions are filled with industry-specific terms that can be confusing even to professionals within the field. Moreover, existing job descriptions rarely include broader skill sets, like problem-solving and critical thinking, that are essential for success in the field. In order to recruit a more diverse workforce, a group of cybersecurity and human resources experts should be enlisted to provide pro bono guidance to help cybersecurity employers write more clear, effective job descriptions. These experts could also publish best-practice guides for writing job descriptions and recruiting diverse talent.
- **Reconsider whether the current criminal background check process is appropriate, fair, and equitable.** Cybersecurity jobs are often subject to strenuous background checks, which can discourage many candidates from completing the hiring process. A task force should be convened to assess whether background check requirements can be eliminated or streamlined, as well as how such changes could reduce biases in the hiring process caused by the disparate impacts of law enforcement and the criminal justice system on persons of color.[3]

Retention

- **Establish a task force to track C-suite executives' commitments to DEI initiatives related to cybersecurity professionals within their companies.** Over the past year, numerous technology and cybersecurity CEOs have made public statements about improving DEI within their organizations. Yet there are no mechanisms currently available to hold CEOs accountable for their commitments. A publicly available tracking system would enhance accountability and may incentivize companies to make progress on their specific DEI goals. A task force of DEI experts could help track C-suite executives' commitments to improving diversity and inclusion within their companies and monitor whether their companies achieve their stated DEI goals over time.

Mentorship

- **Develop a coalition to determine DEI mentorship models for cybersecurity organizations of all types.** Mentorship programs are a common tool for fostering DEI in organizations. However, there is little data on what types of mentorship models work in the cybersecurity space, and whether mentorship programs need to be tailored to different types of organizations. A coalition of experts from across industry, academia, non-profit organizations, and government could publish a "best practices" guide to determine the most effective DEI mentorship models for different types of organizations.

Shifting the Narrative

- **Cultivate brand, advertiser, and media influencer partnerships and develop a campaign to reshape narratives around cybersecurity professionals.** As many of the most visible faces in cybersecurity are White and male, diverse candidates and students may not see themselves as future cybersecurity experts and leaders. A public awareness campaign should be established — largely, but not exclusively, targeting middle- and high-school students — that features diverse cybersecurity employees sharing their positive experiences in the field, and that highlights the the benefits of diversity in the field. Such a campaign would send the message: "Cybersecurity needs professionals like you and the communities you represent, and you belong in this field as much as anyone."

Image by Christina (wocintechchat.com)

Detailed Review of Workshop Findings

The below section reviews lessons from each of the five subtopics covered during the workshops: Education, Recruiting and Hiring, Retention, Mentorship, and Shifting the Narrative. For each subtopic, we review actions requiring additional institutional support (highlighting those the group emphasized as deserving priority) and those that organizations can pursue today with existing resources.

Education

To get a job in the cybersecurity field, candidates are typically expected to have a roster of technical certifications.[4] However, these credentials are expensive to attain and renew, which can present a barrier for diverse candidates. To even the playing field for applicants of all backgrounds, employers should consider subsidizing certification costs for diverse candidates. At the same time, organizations should evaluate whether certifications should be a necessary prerequisite to cybersecurity jobs, and whether apprenticeship programs could be an alternate pathway into the field.

Actions Requiring Additional Institutional Support

Recommendation 1

A coalition of cybersecurity managers and human resource professionals should assess the value of certifications in developing quality candidates for cybersecurity jobs.

When hiring managers were asked in a survey what skills they value most in cybersecurity practitioners, they emphasized communication and analytical skills over a range of technical certifications.[5] A new coalition of cybersecurity managers and human resource professionals should be convened to evaluate whether technical certifications actually make candidates better prepared for cybersecurity roles, or whether they are only marginally helpful and unnecessarily discourage candidates who cannot afford to acquire them.

If the coalition determines that certifications are useful, it should also investigate how to better support candidates of diverse backgrounds through the certification process. For example, the coalition might assess:

- Whether diverse candidates are applying to certification programs;
- How many diverse candidates are accepted into certification programs, but do not matriculate; and
- How many diverse candidates begin certification programs, but do not complete them.

By determining where along the certification pipeline diverse candidates are falling off, the coalition can direct initiatives to support these candidates. For the coalition's work and recommendations to ultimately succeed, unified commitment by industry leaders to jointly revise their certification standards will be essential.

Photo by Afsal CMK

Recommendation 2
A task force should survey participants in cybersecurity apprenticeship programs to better support diverse candidates.

Apprenticeships allow students to develop practical skills through hands-on experience at a cybersecurity workplace. As cybersecurity organizations explore and expand apprenticeship programs, however, they should make sure they understand the needs of diverse students and are able to support them through the experience. A new task force could survey diverse alumni of apprenticeship programs — from the cybersecurity industry and other fields — and use the results to outline best practices for organizations to consider.

Actions That Can Be Taken Now

Participants identified a number of activities that organizations can take without additional investment to support better outcomes in cybersecurity education for diverse participants.

Organizations can:

- Take over the burden of certification costs from candidates. Instead of requiring candidates to front expensive certification fees, employers can pay for new hires to complete certifications. At a minimum, employers could commit to subsidizing these costs for candidates with diverse backgrounds.
- Embrace apprenticeships as a common training practice within the cybersecurity industry. Organizations should especially:
  - Foster apprenticeship programs for students in programs that generate diverse talent, such as historically Black colleges and universities (HBCUs); and
  - Pay apprentices competitive and fair wages.

Academic institutions can:

- Consider creating cybersecurity bridge programs to create new structured pathways into the field. Such programs could, for example, support students as they transition from community colleges and universities into apprenticeships, and later on to professional careers.

Recruitment and Hiring

Cybersecurity organizations will continue to have difficulty attracting diverse talent if their hiring practices are biased toward candidates with elite educations and social capital. To ensure candidates from diverse backgrounds have equal opportunities, organizations should target programs that generate diverse talent; evaluate whether existing job applicant criteria are appropriate; reform their hiring practices to eliminate bias; and reevaluate security clearance processes.

Actions Requiring Additional Institutional Support

Recommendation 3
Cybersecurity organizations that succeed at hiring diverse talent should collect and share anonymous data about which characteristics prove useful for successful hiring.

Within individual organizations, sample sizes may be too small to see overarching trends in what factors lead to success for employees from diverse backgrounds. By combining their data with other organizations, however, cybersecurity organizations can gain insight into what helps employees excel and, equally importantly, which credentials are not important. With that knowledge, hiring managers can adjust job requirements and hone in on the skills new hires will actually need.

Cybersecurity hiring managers could contribute to and analyze anonymous profiles of successful employees to find patterns in what education, background, and skills enable them to succeed. This data can inform what qualifications hiring managers should actually be searching for in new hires, rather than focusing on arbitrary credentials.

To make sure the repository's data is usable, an oversight group should mandate consistent data collection practices across organizations. The repository might also use standardized skill metrics — similar to sports metrics of agility, speed, and power — to further streamline comparisons. Care should be taken to ensure anonymity of the user profiles; the focus instead should be on identifying diverse experiences, educational backgrounds, and skills, and on building teams with complementary skill sets.

Recommendation 4

A group of pro bono experts should help cybersecurity employers rewrite their job descriptions without jargon and focus on the skills required.

Most cybersecurity job descriptions are full of technical jargon that even cybersecurity practitioners can have trouble deciphering. This has a doubly defeating effect: potential applicants cannot figure out whether they are qualified for the positions, and students are intimidated by the jargon, and by extension, are intimidated by cybersecurity work.

A new group of cybersecurity and human resource experts could help organizations make their cybersecurity work more understandable. With institutional support, the experts could offer their services on a pro bono basis to help as many organizations as possible to move away from jargon in their job descriptions. The experts might use the NICE framework, a set of simple descriptions of the tasks and knowledge required for cybersecurity work developed by the National Initiative for Cybersecurity Careers and Studies, as a starting point for creating a robust cybersecurity communications library.

One condition of the experts' free services could be that organizations would agree to share the original and updated job descriptions publicly. These examples could help others make similar changes for their own organizations.

Ideally, the experts would also create resources and models that can be shared widely and complemented with recorded and live trainings for hiring managers and HR teams. Key organizations in the cybersecurity ecosystem — for instance, the Department of Homeland Security, the National Institute of Standards and Technology, and civil society organizations — could help disseminate these training materials.

Photo by Tim Gouw on Unsplash

Recommendation 5

A task force should consider whether the current criminal background check process is appropriate, fair, and equitable.

When candidates are hired by cybersecurity organizations, especially in government but also in the private sector, they are often subjected to extensive background checks that delve into many areas of their lives, including their criminal, credit, and health histories. In light of current reckonings on bias in the criminal justice system, it is worth considering whether background checks perpetuate similar biases.

A new task force might consider:

- What goals background checks are intended to achieve;
- Whether exclusions based on mental health, arrests, and marijuana use are sound;
- What background experience makes someone a poor fit for a cybersecurity position, and whether that criteria contains implicit biases;
- Whether companies administering security clearance interviews have the right cultural competency training; and
- Whether the cybersecurity industry should create a uniform screening system so candidates are not unduly burdened with redundant checks each time they change jobs.

Actions That Can Be Taken Now

Beyond the interventions above, cybersecurity organizations and individuals can take a variety of actions to encourage diversity in hiring and recruitment.

Organizations can:

- Consult with DEI training experts to review and support recruitment and hiring efforts;
- Reset workplace norms to encourage conversations about race and diversity;
- Establish partnerships with programs and schools that generate diverse talent, such as HBCUs and Latinx-serving institutions.
- Assess whether they are disproportionately marketing job opportunities to students at elite universities and, if so, adjust their advertising strategy;
- Use artificial intelligence tools to parse job postings for implicitly biased language and use findings to guide further review and revising;
- Keep job postings open until a diverse slate of candidates have applied.

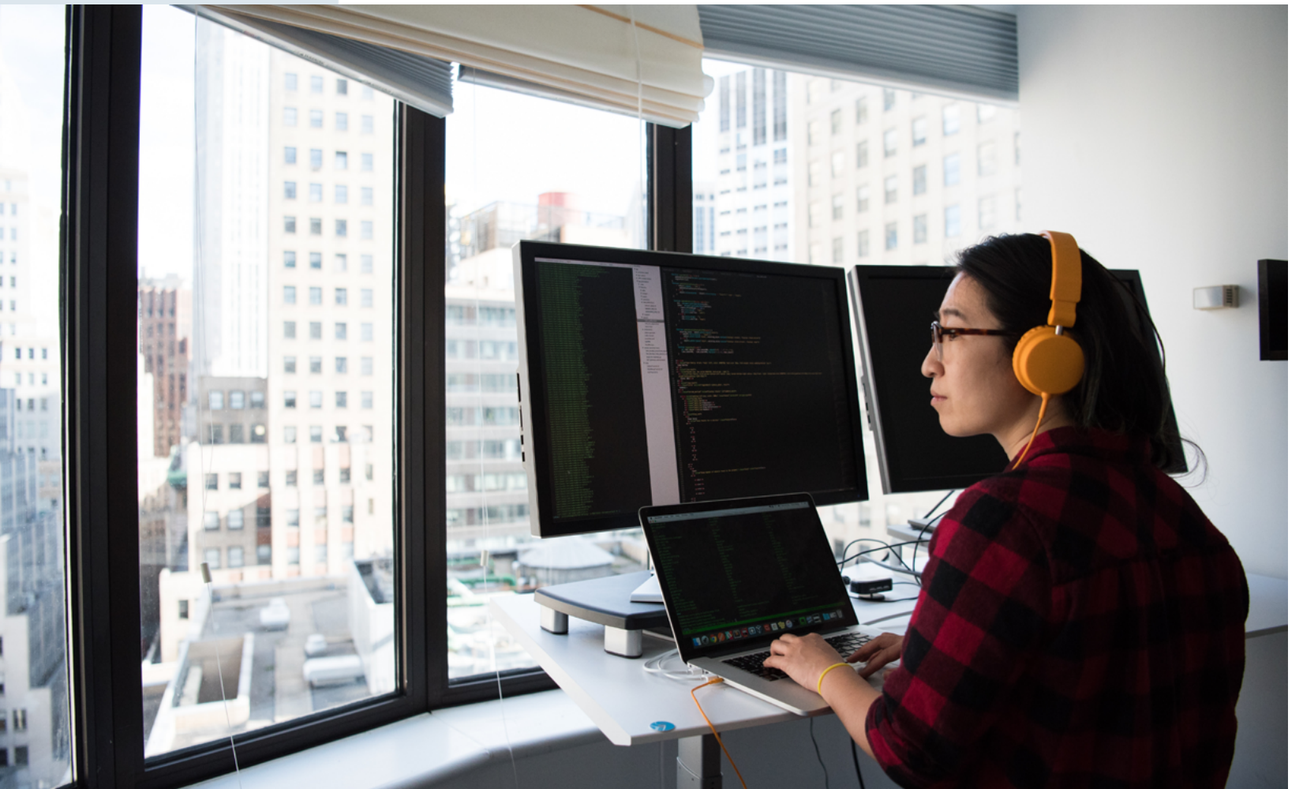
Companies might, for instance, implement a modified version of the Rooney Rule by committing to interview a certain number of candidates of color and/or non-male candidates before making a hiring decision;[6]

- Ban referrals in the hiring process, or only consider referrals in final stages of review; and
- Apply the same standards to intern recruitment and hiring. Organizations should also provide career advancement opportunities for interns after their internships conclude and make return offers as often as possible.

Hiring managers can:

- Undergo training about unconscious bias before assessing candidates;
- Compare candidates' skills based upon anonymous skills practicums, rather than on resumes alone;
- Hold recruiting staff accountable for identifying a diverse slate of candidates; and
- Take time to walk recruiting staff through position requirements beyond the job description. This extra insight may equip them to search beyond certifications and legacy candidate profiles.

Photo by Christina Morillo from Pexels



Retention

Recruiting and hiring diverse employees is just a first step; organizations should also support employees of diverse backgrounds once they are onboarded and enable them to rise within leadership hierarchies. While many organizations offer programs specifically for employees with underrepresented backgrounds, these initiatives are often deprioritized in favor of other goals that may be perceived to have a more direct impact on the bottom line.[7] For DEI initiatives to get full support, C-suite level executives must be held personally accountable for their success.

Actions Requiring Additional Institutional Support

Recommendation 6
A task force should track C-suite executives' commitments to DEI initiatives within their companies.

A key piece missing from many cybersecurity organizations' DEI efforts is a mechanism to hold executives publicly accountable for their commitments. While there have been many diversity pledges circulated over the last several years, these statements of commitment have typically lacked a system for regular follow up. Executives thus can add their names to a pledge and garner good press, but never follow through on their words.

To remedy this, a new task force might:[8]

- Present cybersecurity executives with a list of DEI goals and actions to accomplish these goals with defined success metrics;
- Collect pledges from executives who understand that they will be assessed periodically against the success metrics; and
- Maintain a website that is accessible to the public, where cybersecurity executives' progress is tracked against the success metrics. The task force might use a stoplight color-coding system to categorize whether organizations are meeting their goals, on track to meet their goals, or failing to meet their goals.

The public accountability component of this task force is crucial; within their own organizations, cybersecurity executives are often insulated from criticism. Creating an objective, third-party task force to enforce executives' commitments is key to long-term organizational change.[9]

Actions That Can Be Taken Now

Even without a public set of commitments to DEI and retention, there are a number of actions cybersecurity organizations and individuals can take immediately to improve the likelihood of retaining diverse talent.

Organizations can:

- Embed executives' participation in DEI initiatives in their performance reviews;
- Carve out a certain percentage of staff time for projects related to DEI, with achievements rewarded in performance reviews or through compensation;
- Encourage partnerships between diverse employee resource groups and other affinity groups;
- Track retention and attrition rates for diverse candidates, in addition to tracking broader employee retention; and
- Practice information-sharing when determining DEI strategies. Before settling on any particular policy, DEI committees should engage staff at all levels, from junior staff to executives, to ensure policies are well-received all levels.

Executives can:

- Individually sponsor a certain number of diverse employees' professional development each quarter or year. For example, executives might invite junior employees to sit in on leadership huddles, participate in client meetings, or practice work presentations together;
- Highlight a DEI accomplishment at each major company- or division-level meeting, emphasizing how the accomplishment has contributed to the company's financial success;
- Be directly involved in setting up diverse employee resource groups and joining them as appropriate;
- Encourage employees to dedicate time to DEI projects and contribute to DEI projects themselves, ensuring they are rewarded for this additional work;
- Make the business case for diversity, including why diversity is a business imperative and not just a moral one;[10]
- Join the boards of inclusion-focused nonprofits; and
- Require diverse representation for events and speaking engagements.

Employees can:

- Hold executives accountable when they fall short on the above goals; and
- Review their company's annual reports to understand the company's current priorities and future plans. Employees can then incorporate these priorities into DEI pitches to underscore how diversity fits into the company's broader goals.

Mentorship

Research has shown that engaged mentors are highly valuable resources for diverse professionals.[11] In the cybersecurity industry, long-term mentorship programs can help diverse students get through the entire cybersecurity pipeline, from discovering the field and getting an education to career advancement. But for relationships to flourish, mentorship programs must be set up thoughtfully to support both mentors and mentees.

Actions Requiring Additional Institutional Support

Recommendation 7

A coalition of cybersecurity experts should identify best practices for mentoring diverse cybersecurity practitioners and create a repository of shared resources.

To prevent cybersecurity organizations from designing their mentorship programs from scratch, a coalition of experts from across industry, academia, non-profit organizations, and government could create a set of mentorship program resources. The coalition might start by surveying diverse cybersecurity students and professionals to probe where they would benefit from added support. Based on these results, the coalition could develop professional development resources, reading materials for mentors, and other resources that could be shared publicly.

This new coalition could also facilitate collaborations among organizations by creating a broader mentorship network. For example, a school counselor who is trying to advise a student on cybersecurity careers might draw on the network to find a cybersecurity practitioner whom the student can shadow. A mentor whose mentee is interested in a specific niche of cybersecurity similarly could use the network to find an additional mentor in that niche area. The network could also establish shared connection spaces online, for example by setting up relevant Facebook groups or Slack channels.

Actions That Can Be Taken Now

There are a number of steps that organizations and individuals can take prior to the establishment of a cybersecurity mentorship network.

Cybersecurity workplaces can:

- Create formal mentorship programs with special consideration for diverse employees, and:
  - Ensure these programs are well-funded;
  - Design programming to foster long-term relationships;
  - Discuss the importance of allyship;
  - Ease allies' fears of "saying the wrong thing" and emphasize a culture of assuming good intentions and willingness to learn;
  - Acknowledge that meaningful mentorship requires time and energy; and
  - Market these programs widely so that employees know how to participate in them.

Academic institutions can:

- Add special programming for students of diverse backgrounds at technology and cybersecurity career fairs; and
- Include conversations about diversity and allyship in the cybersecurity curriculum.

Shifting the Narrative

Unlike careers in law and medicine that are already well-defined, careers in cybersecurity can be technical and hard to conceptualize. At the same time, the demographics of the cybersecurity industry remains overwhelmingly male and White, especially in leadership positions,[12] making it difficult for students of diverse backgrounds to envision themselves working in the field. To create a more inclusive cybersecurity workforce, the field must collaborate to redefine the narrative around cybersecurity work and professionals.

Actions Requiring Additional Institutional Support

Recommendation 8
Brands, advertisers, and media influencers should cultivate partnerships to reimagine narratives around the field of cybersecurity.

Put simply, students cannot be what they cannot see. For diverse students to overcome imposter syndrome and feel empowered to pursue careers in cybersecurity, they must believe that there is space for them in the field. A public, multi-platform campaign, largely targeted at middle- and high-school students, could help shift attitudes by featuring diverse cybersecurity employees discussing their positive experiences in the field, as well as honest accounts about the challenges they faced. Such a campaign — building off of the success of existing work, such as #ShareTheMicInCyber, but targeting a younger generation — would show students that the cybersecurity field welcomes practitioners who come from diverse backgrounds and are proud of the work they do.

Students may also be inspired by messages emphasizing not only that there is a place for them, but also that cybersecurity as a whole needs them and the communities they represent at every level, to ensure the evolution of the industry truly centers and protects all. Armed with these new images, students will better be able to envision themselves pursuing careers in cybersecurity and related fields.

Actions That Can Be Taken Now

Beyond a public campaign, a number of approaches can help shift the narrative and raise the profile of diverse practitioners in cybersecurity.

Educators can:

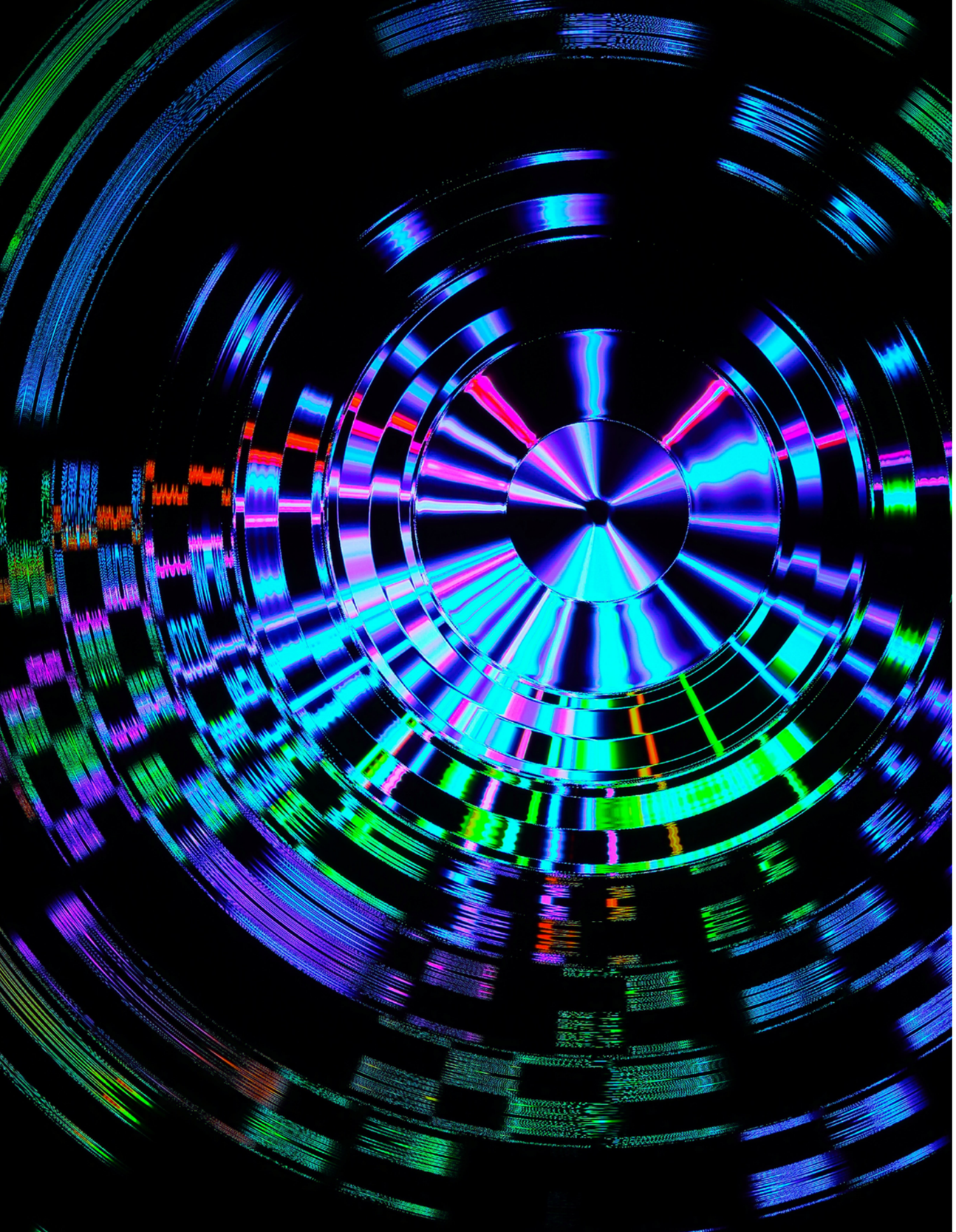
- Introduce their students to cybersecurity as an interdisciplinary field that combines information and social sciences.

Organizations can:

- Financially sponsor and otherwise support initiatives that uplift underrepresented communities in cybersecurity, especially those programs that are led by diverse founders;
- Make select, non-sensitive cybersecurity projects available for educators and students to learn from for free; and
- Encourage employee participation in school career fairs.

Individuals can:

- Participate in movements that amplify underrepresented profiles in the cybersecurity industry. For instance, the #ShareTheMicInCyber campaign pairs Black cyber practitioners with prominent allies in the field; allies lend their social media accounts for the day to elevate their Black practitioner partners' voices and stories.



Conclusion

The participants in the DEI in cybersecurity workshop series coalesced around a few key themes. First, organizations should take a hard look at their internal policies to evaluate how they can better recruit, retain, and support diverse cybersecurity practitioners. There are a wide range of simple steps, requiring minimal intervention, that can lead to better outcomes for diversity in cybersecurity. However, organizations do not have to go about these efforts alone. A handful of new, shared resources could make a big difference in helping organizations learn from each other, understand best practices, and foster a cybersecurity ecosystem that is welcoming and inclusive to all.

Photo by FLY:D on Unsplash

SUMMARY

Key Report Recommendations

Education

Actions That Can Be Taken Now

- Organizations can take over the burden of certification costs from candidates and embrace apprenticeships as a common training practice within the industry.
- Academic institutions can consider creating new cybersecurity bridge programs to give students structured pathways from cybersecurity education to employment.

Actions Requiring Additional Institutional Support

- A coalition should assess the value of certifications in developing quality cybersecurity candidates.
- A task force should survey diverse participants in apprenticeship programs to better support diverse candidates.

Recruitment and Hiring

Actions That Can Be Taken Now

- Companies should establish partnerships with programs that provide pathways for diverse talent and work to remove bias from their hiring practices.

Actions Requiring Additional Institutional Support

- Cybersecurity organizations that succeed at hiring diverse talent should collect and share anonymous data about the diversity of characteristics that prove successful in hiring for cybersecurity jobs.
- A group of pro bono experts should help cybersecurity employers rewrite their job descriptions without jargon and focus on the skills required.
- A task force should consider whether the current criminal background check process is appropriate, fair, and equitable.

Retention

Actions That Can Be Taken Now

- Organizations can tie executives' participation in DEI initiatives to their performance evaluations, carve out a certain percentage of staff time for projects related to DEI, and track retention and attrition rates for diverse candidates.
- Executives can get involved in DEI work, directly sponsor diverse employees' professional development, and highlight how diversity is a business asset.

Actions Requiring Additional Institutional Support

- A task force should track C-suite executives' commitments to initiatives related to cybersecurity professionals within their companies.

Mentorship

Actions That Can Be Taken Now

- Cybersecurity workplaces can create diversity-focused mentorship programs that are well-resourced and emphasize the importance of allyship.
- Academic institutions can add programming for students of diverse backgrounds at technology and cybersecurity career fairs, and include diversity and allyship in the cybersecurity curriculum.

Actions Requiring Additional Institutional Support

- A coalition of cybersecurity experts should identify best practices for mentoring diverse cybersecurity practitioners and create a platform of shared resources.

Shifting the Narrative

Actions That Can Be Taken Now

- Educators can introduce students to cybersecurity as an interdisciplinary field that combines information and social sciences.
- Organizations can support initiatives that uplift underrepresented profiles in cybersecurity, make select, non-sensitive cybersecurity projects available for educators and students to learn from for free, and encourage employee participation in school career fairs.
- Individuals can participate in #ShareTheMicInCyber and other movements that amplify the profiles of underrepresented communities in the cybersecurity industry.

Actions Requiring Additional Institutional Support

- Brands, advertisers, and media influencers should cultivate partnerships to reimagine narratives around the cybersecurity field.

Endnotes

1 Jason Reed and Jonathan Acosta-Rubio, "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce," *Frost & Sullivan*, 2018, https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx; "Women in Cybersecurity: Young, Educated and Ready to Take Charge," (*ISC*)², accessed August 20, 2021. https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBEAFDDA211856C-B274EBDDF9DBEB38.

2 "Chatham House Rule," *Chatham House*, accessed June 12, 2021, www.chathamhouse.org/about-us/chatham-house-rule.

3 Elizabeth Hinton, LeShea Henderson, and Cindy Reed, "An Unjust Burden: The Disparate Treatment of Black Americans in the Criminal Justice System," *Vera Institute of Justice*, May 2018, www.vera.org/downloads/publications/for-the-record-unjust-burden-racial-disparities.pdf; "Report to the United Nations on Racial Disparities in the U.S. Criminal Justice System," *The Sentencing Project*, April 19, 2018, www.sentencingproject.org/publications/un-report-on-racial-disparities/.

4 Henry Kenyon, "Cybersecurity Certifications – What You Need to Know: A U.S. News Guide," *U.S. News & World Report*, December 15, 2020, www.usnews.com/education/learn-cybersecurity-certifications.

5 "2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk," *Frost & Sullivan*, 2017, www.isc2.org/-/media/B7E003F79E1D-4043A0E74A57D5B6F33E.ashx.

6 The Rooney Rule is a National Football League policy requiring teams to interview at least one diverse candidate for any head coaching or front office vacancy. See "NFL Expands Rooney Rule Requirements to Strengthen Diversity," *NFL Communications*, 2018, https://nflcommunications.com/Pages/NFL-EXPANDS-ROONEY-RULE-REQUIREMENTS-TO-STRENGTHEN-DIVERSITY.aspx.

7 Aiko Bethea, "What Black Employee Resource Groups Need Right Now," *Harvard Business Review*, June 29, 2020, hbr.org/2020/06/what-black-employee-resource-groups-need-right-now.

8 Two examples of pledges designed for accountability and impact are Mekong Club's Business Pledge and Mariah Lichtenstern's Opportunity Pledge. See "The Business Pledge: A New Roadmap for The Private Sector to Address Modern Slavery," *Mekong Club*, May 2019, https://themekong-club.org/wp-content/uploads/2019/07/THE-BUSINESS-PLEDGE_final.pdf and Mariah Lichtenstern, "The Opportunity Pledge: Accelerating Equity in Startup Opportunities," *Aspen Tech Policy Hub*, accessed June 12, 2021, https://www.aspentechpolicyhub.org/wp-content/uploads/2020/08/TFE-White-Paper.pdf.

9 Aspen Digital took a first step in this direction by establishing an Anti-racism pledge tracker, identifying organizational commitments to anti-racism activities. To be successful, such a tracker would need to be continuously updated and contain accountability mechanisms, as noted above. Such an effort might also be based upon a tech executive tracker, such as that developed by Sherrell Dorsey, Grace McFadden, and Ashley Stewart of tpinsights.com, but with a specific focus on cybersecurity. See "The Aspen Digital Anti-racism Pledge Tracker," *Aspen Digital*, June 25, 2020, https://www.aspeninstitute.org/blog-posts/aspen-digital-anti-racism-pledge-tracker/ and Sherrell Dorsey, Grace McFadden, and Ashley Stewart, "Tech Statements: Statements Made by Top Tech Companies on Racial Justice, BLM, and George Floyd," *The Plug*, accessed June 12, 2021, https://docs.google.com/spreadsheets/d/1OZx-_tm3PPyx6-ZJAST1xxOJRfn7KfYDjDT-6JedrTfs/edit#gid=0.

10 McKinsey & Company's report "Diversity Wins: How Inclusion Matters" and the Massachusetts Institute of Technology's study "Workplace Diversity Can Help the Bottom Line" are two helpful resources. See Sundiatu Dixon-Fyle, et al., "Diversity Wins: How Inclusion Matters," *McKinsey & Company*, May 19, 2020, https://www.mckinsey.com/featured-insights/diversity-and-inclusion/diversity-wins-how-inclusion-matters and Peter Dizikes, "Study: Workplace Diversity Can Help the Bottom Line," *Massachusetts Institute of Technology*, October 7, 2014, https://news.mit.edu/2014/workplace-diversity-can-help-bottom-line-1007.

11 David Thomas, "Race Matters," *Harvard Business Review Magazine*, April 2001, hbr.org/2001/04/race-matters.

12 Reed and Acosta-Rubio, *supra* note 1.

We thank the William and Flora Hewlett Foundation for funding this work.

For inquiries about this report, please contact:

The Aspen Institute
Aspen Digital
2300 N Street, NW
Suite 700
Washington, DC 20037

Published by The Aspen Institute. We encourage others to share and cite this report using the following citation: Aspen Digital, "Diversity, Equity and Inclusion in Cybersecurity." The Aspen Institute, Washington, DC. August 2021.


ASPEN
DIGITAL
ASPEN TECH
POLICY HUB