



FEBRUARY 2022

SHIELDED BY THE MELTING POT

How Diversity and Inclusion Improve U.S. National Security and Resilience

Authored By:

Drew Spaniel, Lead Researcher, ICIT

Contributors Include:

Dr. Lenora Peters Gant, National Security Fellow & Senior Executive Advisor at Howard University

Stan Mierzwa, Director, Center for Cybersecurity, Kean University

Don Maclean, ICIT Fellow & Chief Cybersecurity Technologist, DLT

Dr. Barry C. West, ICIT Fellow & Former Acting CIO, DHS

Joyce Hunter, Executive Director, ICIT

Malcolm Harkins, ICIT Fellow & Chief Security and Trust Officer, Epiphany Systems

Jim Routh, ICIT Fellow & Advisor, Board Member, & Former CSO

Don Heckman, ICIT Fellow & Defense Cyber Solutions Leader & Director, Cybersecurity Solutions, Guidehouse

M.K. Palmore, Director, Office of the CISO, Google Cloud

Itzik Kotler, ICIT Fellow & Co-Founder & CTO, SafeBreach

Teddra Burgess, ICIT Fellow & Senior Vice President Public Sector, Tanium

Shielded by the Melting Pot

How Diversity and Inclusion Improve U.S. National Security and Resilience

February 2022

ICIT would like to thank the following experts for their contributions to this paper:

- Dr. Lenora Peters Gant, National Security Fellow & Senior Executive Advisor at Howard University
- Stan Mierzwa, ICIT Fellow & Director and Adjunct Professor, Center for Cybersecurity, Kean University & CTO, Vennue Foundation
- Don Maclean, ICIT Fellow & Chief Cybersecurity Strategist, DLT
- Dr. Barry C. West, ICIT Fellow & Former Acting CIO, DHS
- Joyce Hunter, ICIT Executive Director & Former Interim CIO and Deputy CIO, USDA
- Malcolm Harkins, ICIT Fellow & Chief Security and Trust Officer, Epiphany Systems
- Jim Routh, ICIT Fellow & Chief Security Advisor, Virsec
- Don Heckman, ICIT Fellow & Defense Cyber Solutions Leader & Director, Cybersecurity Solutions, Guidehouse
- M.K. Palmore, Director, Office of the CISO, Google Cloud
- Itzik Kotler, ICIT Fellow & Co-Founder and CTO, SafeBreach
- Teddra Burgess, ICIT Fellow & Senior Vice President Public Sector, Tanium

Copyright 2022, The Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

Contents

Abstract	3
Introduction	3
How can adopting, increasing, and improving the Diversity, Equity, and Inclusion posture combat the cyber talent shortage?	4
How are Diversity, Equity, and Inclusion Lacking in the Public and Private Sector?	5
How would a diverse set of people, processes, and technology improve national cybersecurity?	6
Types of Diversity	7
Racial and Ethnic Diversity	7
Diversity of Background	8
Gender Diversity	9
Neurodiversity	10
LGBTQ+ In Cybersecurity	11
Ideological Diversity	12
Technological Diversity	13
How Can Leaders Address Diversity and Inclusion Adoption Hesitancy or Dismissal?	14
Ten Ways to Better Incorporate Diversity and Inclusion	14
Conclusion	16

Abstract

America was built through the union of diverse people and the development of a shared culture and national identity. While a discussion of the philosophy of “what is a nation” is outside the scope of this publication, we can agree without dispute that the United States is globally recognized as a “melting pot” that draws its strengths, innovations, growth, and evolutions from the complex topic of diversity and inclusion. The internet is borderless and innumerable adversaries of all levels of technological sophistication intermingle and collaborate to evolve, mutate, and threaten U.S. critical infrastructure. Worse, cyberwarfare is asymmetric and U.S. organizations are already at a significant detriment. If we are to continue to secure the nation against domestic and international threats, U.S. critical infrastructure organizations must improve their diversity and inclusion efforts to better retain and feature the varied peoples that built our nation and to advance the whole-of-nation approach essential to combatting the rapidly evolving threat landscape.

This publication features research from ICIT and the support, expertise, and valued perspectives of eleven distinguished thought leaders.

Introduction

The American Melting Pot is a monocultural metaphor that has been used since the early twentieth century to describe the nation as a heterogeneous society that combines different cultures, traditions, and heritage into an evolving homogeneous culture. In some nations, multiculturalism, the coexistence of different cultures remains the norm, but the United States has defined itself from its shared and dynamic national identity. The term “melting pot” derives from the crucible of a forge in which a variety of metals are melted, refined, and combined to fuse a stronger alloy—the increased tensile strength and cohesion of alloys allowed for military dominance and technological innovation throughout history. Higher quality weapons, technology, and tools allowed some nations to thrive while those who failed to adapt faded into the annals of history.

In a similar fashion, America is a country that was built from the culture, labor, suffering, and achievement of many diverse peoples. Every U.S. critical infrastructure was built on the innovations of our diverse population and is still dependent on that diversity today. For instance, the U.S. military is considered the largest and most powerful force on the planet. It is a microcosm of American society and relies on people from diverse backgrounds to defend a country whose nation they each proudly call their own. Even in terms of modern national security, diversity and inclusion remain a national imperative. Last year, in response to questions about efforts to improve diversity and inclusion in the armed forces, Jack Kirby, Press Secretary to DoD Sec. Austin commented, “It is important for the force to look like the country it serves — absolutely. But [Sec. Austin] strongly believes diversity is a readiness issue because it allows different perspectives, additional context, different lived experiences to inform the way we make decisions, the policies that we craft, the operations that we lead”. In short, since the founding of our America, our national stability, security, and resiliency have depended on the tools, swords, and shields that we forged from diversity into a stronger national identity.

American history is often tinted by the lens of our national ability to overcome domestic threats, international conflicts, and national turmoil. Our history is neither spotless nor pristine, but it is

characterized by perseverance. We overcome trials and tribulations as a nation by drawing from the lessons, perspectives, and ideologies of the workers, soldiers, and leaders who choose America as their home. However, conflict is no longer solely confined to the physical realm, and we have a severe shortage of cyber-talent in the public and private sectors. We are now past the point where we need to realize that our security in cyberspace and at cyber-physical boundaries likewise depends on our diverse population. America's diversity defines its strength and makes it unique in the great-power competition of the global stage. We need to better leverage diversity and inclusion to elevate our citizens, improve critical infrastructure resiliency, and ensure national security.

How can adopting, increasing, and improving the Diversity, Equity, and Inclusion posture combat the cyber talent shortage?

Media coverage and vendor materials all-too-often frame cybersecurity as an issue of incongruent technologies, nefarious code, and Machiavellian nation-states. While elements of that depiction are certainly accurate, many cybersecurity practitioners would be the first to confirm that cybersecurity is as much about people as it is about tools, policies, and governance. People are diverse. Our cybersecurity workforce needs to better adapt to, accommodate, and embrace those diversities of person, background, and thought.

At the time of this writing, the American cybersecurity workforce numbers at around 1,053,468 according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology in the U.S. Department of Commerce. While that may seem impressive for a nation of around 330 million, the U.S. actually has an additional 597,767 cybersecurity job openings that remain unfilled. More simply, based on just the numbers at the time of this writing, only 68% of U.S. cybersecurity positions are filled. Teddra Burgess, ICIT Fellow & Senior Vice President Public Sector, Tanium adds, "There are currently half a million cyber vacancies across the country. We know that it is critical to invest in how we protect and secure the nation, and in doing so, we must work to prevent future shortages that threaten our ability to meet cyber threats head-on. The inclusion of diverse populations in cyber defense and threat response allows for a diversity of thought and approach; reduces groupthink, allowing for the differences in the way people assess and problem-solve to positively impact business outcomes."

Estimates for how many additional cyber professionals will be needed by 2025 vary, but most predictions lie in the range of one to three million additional positions. Worse, many of those currently employed in U.S. cybersecurity may be considering retirement within the next decade. The nation might be in desperate need of cyber-defenders during the pinnacle of digital warfare. The worst time to need fresh cyber talent is after attackers are already digitally assaulting your infrastructure. Don Maclean, ICIT Fellow & Chief Cybersecurity Strategist, DLT, observes, "Cybersecurity talent is present in every ethnic group and every socioeconomic stratum. America's security rests on finding the best talent to protect our critical infrastructure. "So why does the U.S. still have a dearth of cyber talent despite years of increased recruitment? M.K. Palmore, Director, Office of the CISO, Google Cloud, explains, "As an industry, we do a poor job of outlining the requirements for bringing new talent to the table, and

because of this, we essentially see recycling of existing talent. This is not scalable and requires us to broaden the scope of the potential entrant to this growing and exciting field. Among those new entrants should be people of color as they are not appropriately represented in this exciting industry." Ms. Burgess elaborates, "To combat talent shortages, we must be intentional about recruiting strategies and diversify how we source candidates if we want to continue building more resilient cyber teams."

How are Diversity, Equity, and Inclusion Lacking in the Public and Private Sector?

For the sake of soliciting honest observations and feedback, ICIT has anonymized this section of feedback and it should be noted by the reader that a specific observation expressed here should not be directly or indirectly attributed to a specific contributor. Based on the recommendations and experience of our contributors, ICIT has inferred that diversity, equity, and inclusion efforts in the federal government and in some private sector organizations are still lacking in the following critical areas:

1. Leaders' require greater commitment and "will" to take on DEI issues and need to address their fear of failure and lack of other leaders' genuine support.
2. Lack of clear DEI Strategy that includes real accountability among managers and leaders at all levels of the organization, no concrete relevant measures and metrics.
3. Organizations in both sectors need leaders aware and educated with the necessary skills in inclusiveness to change practices for talent development.
4. Despite years of articulation and published reputable research on the need for DEI programs and the benefits of adoption, progress has been slow and public and private sector leadership still does not proportionally reflect the diverse workforce.
5. It takes decades to improve diversity and shift organizational culture to be more inclusive and equitable. Organizations are not proactively adapting and are setting themselves further behind.
6. DEI also needs to be improved within the STEM and multi-disciplinary fields from which cybersecurity draws talent. It behooves the government, organizations, and academic institutions to collaborate to improve DEI within higher education and training programs. Inner city and after school programs help from the grassroots, but more must be done (years in advance) by resourced organizations to better support these programs and foster interest in the cybersecurity field. We will not reduce the cyber talent shortage if we do not guide students now.
7. Attackers evolve from a diversity of experiences, thought, and tactics. Organizations need to likewise embrace DEI as a proactive and concerted security effort.
8. Much like how cybersecurity is plagued with "checkbox compliance" frameworks and self-assessment, DEI efforts sometimes lack objectives metrics, holistic accountability, and leadership commitment.
9. A formal and purposeful diversity developmental workforce strategy must include all personnel and employees to shift organizational culture and build a diverse long-term pipeline of qualified talent.

Leaders must do better at championing DEI efforts, listening to concerns, and articulating the benefits of DEI and the need to respect the dignity, experiences, and identity of every member of the organization.

10. The public and private sector need to understand that DEI is not a “politically correct” or partisan topic. The rhetoric and perception need to be discharged, deescalated, and reframed so that they can appreciate it as a cybersecurity topic and as a business enabler.

How would a diverse set of people, processes, and technology improve national cybersecurity?

Cyberwarfare is an asymmetric conflict that benefits the attackers. Teddra Burgess describes, "As threat actors continuously advance, modify and expand their tactics, it's imperative that cyber teams stay ahead through creative problem-solving and diverse ideas and tactics that meet these emerging threats. Limited viewpoints create a barrier to cyber teams' ability to mitigate and respond to attacks comprehensively. Our teams are stronger when we can leverage the collective power of our similarities as well as our differences to diversify and strengthen our cybersecurity posture. Problem-solving, strategic planning, and innovation all benefit from diversity and inclusion." In addition to requiring fewer resources for offensive operations than defenders, adversaries also benefit from collaboration with diverse communities of other attackers to develop malware, exchange materials, and resources, or coordinate attack campaigns. Don Maclean emphasizes, “cybersecurity is fundamentally a problem of human behavior -- or misbehavior. To anticipate threats and fight them effectively, we need insight into the culture, psychology, and motives of all potential adversaries."

With diversity and inclusion comes organizational strength, cohesion, and agility. Homogeneous experiences and perspectives yield less success compared to problem-solving done by teams with varied backgrounds. One of the most significant ways that diversity augments cybersecurity is in the added ability of the organization to draw from the views of people with different experiences in life, education, and skill. Aggregating a multitude of perspectives is invaluable when developing proactive cybersecurity strategies and responding to attacks because innovation, problem-solving, and consensus-building all benefit from diversity. Don Heckman notes, "Successful cybersecurity programs depend on people, processes, and technology to deliver a defense-in-depth approach. It has been proven that a team whose members have diversity (e.g., culture, age, education, work experiences) delivers superior results. This diversity can allow the team to approach problems differently and come up with innovative solutions. With respect to processes and technology, having diversity in both leads to a more secure and robust environment. If you take a layered approach with both processes and technologies, a vulnerability or weakness in one layer can be mitigated and contained, whereas if you have a uniform homogenous solution, a single vulnerability can comprise the entire system." Strengthening diversity initiatives can improve National Security and critical infrastructure resiliency by:

- a) by intentionally attracting and sustaining a flow of new talent with current and updated skill sets;
- b) promoting inclusion of fresh perspectives from new talent into workgroups and brainstorming sessions to ensure they belong, and their ideas are "listened" to and considered in the final decision process.

Moreover, according to Dr. Lenora Peters Gant, "The inclusion of non-technical insights, perspectives and ideas can make for more cyber-resilient systems in the decision-making process. Inviting multiple SMEs from across business lines (including Human Resources) can be a 'win-win' in the final analysis since cybersecurity risks are continuously growing and evolving. "

Types of Diversity

A diverse workforce brings a deeper understanding of our enemies' mindset. Diversity comes in many forms, including race, gender, sexual orientation, age, physical abilities, neurodiversity, and religious beliefs. In the context of the cybersecurity workforce, one way to raise the profile of diversity initiatives is to focus on the value variety brings to the mission of a cybersecurity team and improve our articulation of the correlation between diversity and desired business outcomes. This message is a valuable complement to other essential diversity efforts, including eliminating hiring biases, preventing discrimination, and improving equality in the workplace. Diverse teams are stronger because they can harness different viewpoints when assessing a threat or solution, interpreting the narrative of an attack, and evaluating risk. For instance, some studies have found that women are more risk-averse than men. Different studies have found that those with atypical thought processes, such as those on the autistic spectrum and people with dyslexia or dyspraxia, may be better at identifying patterns within large data sets. By incorporating diversity into the cybersecurity workforce, an organization can limit cognitive blind spots, groupthink, and other forms of stagnation that may have limited performance in the past. Jim Routh, ICIT Fellow & Chief Security Advisor, Virsec, contributes, "More diversity in employees translates into higher performance, increased talent development opportunities and teaching existing leaders how to increase inclusive behaviors and neuter institutional and systemic racism." Dr. Barry West, ICIT Fellow & former Acting CIO, DHS, adds, "Any organization benefits by having individuals who are diverse with different skill sets and talents. This is also very true for cybersecurity, where you need professionals who are talented at disciplines within cyber such as policy, technology, management, and so on. This is when you create high-performing organizations but having this great skillset mix."

Racial and Ethnic Diversity

In the 2018 release of McKinsey's Delivering Through Diversity study, 39% of the U.S. population classifies as a minority. However, only 12% of minorities occupied executive positions, and 15% were part of the board of directors.

Joyce Hunter, ICIT Executive Director & Former Interim CIO and Deputy CIO, USDA, explains, "Organizations must analyze and understand the current workforce composition. Minorities comprise 26% of the cybersecurity workforce and only 21% of the overall workforce. This is a key demographic

that warrants further research to develop methods to recruit more minorities into the field. Much of the existing body of research also fails to explore the effective sources of cybersecurity personnel or what skills other than technical are good indicators of success. The U.S. workforce does not mirror the adult population at large, as diverse U.S. citizens are underrepresented in the workforce and, specifically, in cybersecurity." A study entitled Tech Leavers by the Kapor Center for Social Impact found that unfairness-based turnover costs the technology industry \$16B a year. Further, it concluded that almost 25% of underrepresented minorities and women of color experienced stereotyping and that 40% of Black, Hispanic, and Native American men left their jobs due to discrimination and racism in the workplace. Disenfranchisement discourages personnel from remaining in their positions, and it dissuades new talent from pursuing education and careers in cybersecurity and other technology fields. It is critically important for leaders to ensure that minorities are not just invited to the table but are active participants and equal stakeholders. Cybersecurity leaders need to demonstrate that minority employees are valued and that they are empowered to actively participate in supporting the mission, driving the organization forward, and helping the organization grow top-line revenue.

Several organizations exist today whose aim is to improve minority underrepresentation in cybersecurity through access to training, scholarships, and education. This includes [the International Consortium of Minority Cybersecurity Professionals](#), the [Hispanic I.T. and I.T. Security Professionals Network](#), and [Blak Cyber](#).

Dr. Lenora Peters Gant, National Security Fellow & Senior Executive Advisor at Howard University, provides that according to DEI research studies by Forbes (2020), McKinsey (2020), and Harvard Business Review (2016), by adopting and increasing Diversity, Equity, and Inclusion (DEI) in an organization, the benefits include, but are not limited to:

- (1) The ability to acquire a variety of perspectives and data sets from different cultural backgrounds that inform decisions and triangulate issues to promote an improved course of action;
- (2) Improve innovation and the diversity of thought in working groups;
- (3) Influence the acceleration of positive change;
- (4) Provide insights that could positively challenge and impact the "status quo"; and
- (5) The capacity to attract, recruit, hire and possibly retain high-quality, diverse talent from a variety of cultural backgrounds.

Dr. Barry West suggests, "Most of the historically black colleges and universities (HBCUs) now offer college curriculums that offer degrees focused on cybersecurity. Bringing these individuals into the workforce will only help organizations improve not only diversity and inclusion posture but help with the cyber talent shortage."

Diversity of Background

Don Heckman, ICIT Fellow & Defense Cyber Solutions Leader & Director, Cybersecurity Solutions, Guidehouse, notes, "As more and more aspects of our society (e.g., government services, healthcare, e-commerce, entertainments) move online, cybersecurity is becoming critical to delivering these in a safe and secure manner. The demand for cybersecurity professionals globally is outpacing the supply, with

significant shortages predicted in the near future. It is time the industry looks to attract underrepresented groups of our populations to attract to the cyber security field. I also think we need to think about looking outside our traditional educational norms (e.g., four-year STEM degree) to expand our workforce. We should identify individuals with the correct aptitudes to include critical thinking problem-solving and then have them work through a combination of on-the-job training and development/certification program."

Malcolm Harkins, ICIT Fellow & Chief Security and Trust Officer, Epiphany Systems, observes, "With the skills and talent shortage, we need to make sure we are looking at all pools of potential talent. We need to be grooming earlier in the educational process to gear people towards careers in cyber security. Collaborating with colleges, inner-city school programs, nonprofits, etc., will not only lift people out of economic uncertainty but also improve our long-term pool of talent." Itzik Kotler, ICIT Fellow & Co-Founder and CTO, SafeBreach, expands, "In order to combat the shortage in cyber security talent, organizations must be willing to expand the pool from which they look to draw candidates. Shifting hiring efforts to focus more on diversity, equity, and inclusion can help organizations overcome ingrained assumptions about who should be in the cybersecurity space and what qualifies them to be there. Qualities like specific diplomas, universities, or career paths are outdated (and often inaccurate) measures of a candidate's real value. Looking beyond these traditional qualifiers—and focusing instead on current capabilities and future potential—can dramatically expand an organization's talent pool to include candidates with more diverse but equally valuable backgrounds."

Dr. Lenora Peters Gant agrees, "A diverse set of individuals from a variety of backgrounds, innovative processes, and emerging technologies can improve cybersecurity risks by challenging traditional and status quo educational requirements of cybersecurity professionals. As the cybersecurity profession evolves, it appears that a multi-disciplinary approach to training new talent and workforce engagement via 'on-demand' learning tools/modules to update skill sets are essential. Further, it's important to re-imagine and intentionally employ a variety of 'talent acquisition' strategies that could improve outdated methods and processes over the longer-term of cybersecurity posture in organizations."

Gender Diversity

The United States is not efficiently recruiting women, who comprise approximately half the population, into cybersecurity roles. According to a 2018 (ISC)² study, there are even fewer women in U.S. government cybersecurity than there are proportionally in cybersecurity globally. The U.S. cybersecurity workforce within the federal, state, and local governments is about 11% female, whereas about 24% of cybersecurity practitioners globally are women.

Despite accounting for half the overall population within the cybersecurity field, women are significantly overshadowed by their male counterparts. For instance, The (ISC)² Cybersecurity Workforce Study: Women in Cybersecurity report found that men are:

- Four times more likely to hold executive roles than their female counterparts
- Nine times more likely to hold managerial positions than women
- Paid 6% more than women

- Experience 240% less discriminatory treatment than women

Trans women, trans men, and non-binary individual often face discriminatory practices that their cisgender co-workers do and may also be subject to dead-naming, misgendering, or denials in advancement.

To mitigate this bias, organizations' leadership, management, and HR teams need to work together to foster an inclusive and welcoming environment that empowers all employees with the equal opportunities based on their work. To be clear and address common rebukes, no one is asking for additional advantages or special treatment; the misconception and perceived injustice of "special privileges" or inconveniences derives from a conflation of equality and equity. Equality and equity are similar concepts, but their differences matter. Equality is treating all people the same and providing equal access to opportunity. Equity refers to proportional representation based on circumstance (e.g., class, race, gender). Diversity, equity, and inclusion are not about special treatment and diverse groups are not asking to be treated differently than their peers; in fact, all they are asking is to be treated without implicit biases against their diversity. People are asking to be treated like humans, afforded human decency and dignity, and to not have their self-identification or preferences impact their treatment in the workplace since it has no objective bearing on their job performance.

According to a project between Fortinet and Datalere, some systemic bias can be eliminated by reevaluating the language and structure used to construct job listings. They applied natural language processing algorithms to thousands of job ads and resumes for job types ranging from Incident Response Specialist to CISO. Next, they analyzed the presence of hard and soft skills as well as a range of demographics, including job-hopping, tenure, and gender diversity. They found that:

- Of the top 20 skills employers list as a requirement in their job descriptions for CISO placements, 17 are considered soft skills.
- On resumes, women cited:
 - Soft skills 52.5% more frequently than men
 - Analytical skills 150% more frequently than men
 - Leadership skills 46% more frequently than men
 - Gender-diverse teams made better decisions 73% of the time versus 58% of the time for all-male teams.
- Venture capitalist funded, women-led teams, bring in 12% higher revenue for their organizations than their male-dominated counterparts do, while venture capitalist firms with at least one woman in a leadership position outperform all-male peer organizations by 63%.

Neurodiversity

Stan Mierzwa, ICIT Fellow & Director and Adjunct Professor, Center for Cybersecurity, Kean University & CTO, Vennue Foundation, argues, "The varied roles in cybersecurity require different kinds of skills and attention to detail. In some cases, reviewing detailed information, as in the case of a digital forensic investigation, requires more than just technical skill. Such skills include almost an obsession to evaluate all data and options for a possible link or connection to a cybercrime. The area of neurodiversity can be

one segment of the population that may add value to such efforts. Neurodiversity includes the area of considering different ways that brains work in different individuals. For example, these could include individuals on the autistic spectrum other similar neurological conditions. In addition to diversifying the workforce with individuals with neurodivergencies, there is the potential to provide value to the cybersecurity field with their inherent advantageous abilities."

Neurodiversity is the term used to cover a range of differences in brain function and behavioral traits. One study estimated that around 3% of the population exhibits the signs of neuro-atypicalism. This generally includes conditions such as attention deficit disorder, attention deficit hyperactivity disorder, autism spectrum disorders, dyslexia, and dyspraxia. Many of these conditions are stigmatized despite affected individuals often demonstrating an aptitude for the cybersecurity and technology field.

Differences in the way people apprehend and solve problems have a real impact on outcomes. Studies have shown that innovation can be born from distinctive brains. A study of Silicon Valley, considered by many to be the tech-hub of the United States, shows an abnormal number of atypical brains, especially among the founders of start-ups. This phenomenon can also impact innovation and success in cybersecurity and risk management. Incidental proofs are in the number of famous hackers that are believed to exhibit the signs of neuro-atypicalism.

In similar comparisons to early developments in racial and gender diversity in the industry, discussion about neurodiversity within the workforce has so far been driven by those who are personally associated with it. For neurodiversity to be achieved, a broader coalition of stakeholders must identify this gap and work to close it.

Fortunately, we see signs of progress. In September 2019, a pilot program that aimed at finding neuro-diverse adults cybersecurity jobs within the federal government won the Government Effectiveness Advanced Research Center challenge and received a \$300,000 federal grant. The program was a collaboration between the MITRE Corporation, SAP, Specialisterne, the DXC Dandelion Program, George Mason University, Mercyhurst University, Rochester Institute of Technology, University of Maryland, and Drexel University.

LGBTQ+ In Cybersecurity

A University of Michigan study of 330,000 employees (11,000 who identified as LGBT) in 28 different federal agencies with LGBT-inclusive policies found that "Lesbian, gay, bisexual and transgender employees in federal workplaces report worse job experiences than their colleagues, leading to higher intentions to leave their job." Unsurprisingly, when people are not satisfied with their jobs, the study showed they are more likely to seek employment elsewhere.

Members of the LGBTQ+ community bring unique perspectives to the cybersecurity and privacy discussion because of their unique experiences. Many members of the LGBTQ+ community use mobile applications and social networking as safe spaces to express their identity and connect with others. According to statistics from LGBT Tech, The Trevor Project, and a study released by GLSEN (the Gay, Lesbian, and Straight Education Network:).

- 81% of LGBTQ+ youth have searched for health information online, as compared to 46% of non-LGBTQ+ youth
- In the past year, 62% of LGBTQ+ youth have used the internet to connect with other members of the LGBTQ+ community
- More than 1 in 10 said they had first disclosed their LGBTQ+ identity to someone online
- 1 in 4 LGBTQ+ youth said they are more out online than in person

These experiences mean that those in the LGBTQ+ community may have a deeper appreciation of the ramifications of compromised online privacy and how data breaches of personally identifiable information (PII) can impact individuals, particularly those in vulnerable groups.

Organizations, especially those that have been breached in the past, would benefit from the perspective of individuals who place a higher value on privacy and data security because they recognize the potential harm that could be inflicted if data were compromised. To increase hiring, retention, and promotion of LGBTQ+ professionals, organizations can support the creation of LGBTQ+ employee resource groups and provide training to lessen biases that promote favoritism and unfair resource distribution. Collaboration with private sector groups could also be leveraged to increase federal government cybersecurity recruitment. The LGBT Technology Partnership works to provide a centralized, national presence for the many LGBTQ+ groups that are impacted by telecommunications, cable, and technology policies. Queercon, which started as an LGBT meet-up group at Defcon, is an annual cybersecurity and technology convention specifically geared towards the LGBTQ+ community. Its mission is to increase LGBT visibility in the cybersecurity and technology community.

Ideological Diversity

Mitigating ideological bias is a difficult and often overlooked challenge. Malcolm Harkins elaborates, "I have long believed the biggest vulnerability we face today and in the future is the misperception of risk - not only end-users do this and business leaders do this ... security teams also misperceive risk. If you look at the misperceptions, you see biases based on background skills/education, angle of view, as well as things like recency, a bias, or confirmation bias. SO if we treat this misperception as vulnerability - what is the mitigation? - Diversity of perspective. How do you get that diversity of perspective? You get people engaged from different backgrounds, different organizations, and different skills." Itzik Kotler adds, "There is rarely one way to solve a problem in the world of cybersecurity, and solutions are only as good as the opinions in the room. If everyone has the same background, education, and experience, the room quickly becomes an echo chamber of unremarkable ideas. When a more diverse group of people is invited to contribute, we open the door to novel opinions, processes, and applications of technology. As a result, organizations are able to generate more creative solutions to their most challenging cybersecurity problems and, ultimately, enhance their ability to protect themselves within the ever-evolving threat landscape." M.K. Palmore agrees, "It has been researched and clearly noted that diversity in opinions and approaches leads to better results. Because the cybersecurity industry has historically been monolithic, we should expect that our responses and ideas may not take into account the users or stakeholders as the world increasingly grows to be a much more diverse place. Diverse talent means diverse and new outcomes."

Diversity and inclusion empower teams to adapt to new ideas and methodologies beyond their lived experiences. By eschewing diversity or only implementing it as part of hiring quotas, organizations are doing themselves a disservice. Itzik Kotler explains:

"When we look at common cybersecurity adversaries and hacking groups, they have highly motivated individuals working on their behalf with dramatically different backgrounds. Individuals are recruited to join these groups based purely on the skill set they can contribute, so characteristics like gender, race, and educational background are of little consequence. As a result, these groups have been able to bolster their ranks with talented individuals who bring a diversity of thought that has enabled them to increase the creativity and efficacy of their attacks. In order to effectively combat these groups, the cybersecurity industry must do a better job of competing for talent that is as diverse as the opponents they face. Diversity of thought helps us move past assumptions about who adversaries can be, where they come from, what they look like, how they implement attacks, etc. As a result, we are able to develop more creative solutions to the challenges being faced in the areas of national security and critical infrastructure."

In addition, without diversity of thought, innovation and evolution of the field is stifled. Joyce Hunter infers, "A lack of diversity in thinking and experience in the cyber workforce may contribute to the negative outcomes we are all experiencing in the cybersecurity industry." Cybersecurity perhaps more than any other field relies on multidisciplinary skillsets to complex problem-solving. A holistic view of entire sectors, fields of research, and multi-stakeholder and experience approaches are necessary to address an issue and sometimes even to mitigate an attack or limit the impact of an incident. By leveraging a diverse team, organizations can improve outcomes, enhance performance, boost innovation, and focus more keenly on facts.

Technological Diversity

While diversifying the cybersecurity controls and solutions utilized by an organization is important to limit the exploitation of critical vulnerabilities, it is also important to consider the impact that the adoption of a solution may have on diversity and inclusion. Enabling personnel to work remotely may empower those with disabilities, children or those who cannot afford to live in the geographic region of the organization, to enter the workforce. Especially at the time of this writing and in the near future, as cybersecurity talent are at a premium and when it is a "candidate's market," it behooves organizations to expand their pool and offering remote work or compromise solutions where possible. Some of this nation's best talent are underutilized because they are either trapped in systemic conditions out of their control or they are the victim of personal constraints that inhibit their entrance into the cybersecurity field. By understanding or anticipating some of these constraints and offering accommodations, whether they be remote work, flexible hours, and unconventional schedule, etc. employers can both gain devout and high-quality talent and diversify themselves from every other employer that is competing for the same talent. One method to address implicit and explicit biases in the talent acquisition process is to adopt "blind" hiring solutions that allow leaders to evaluate talent based solely on their merits and skills. However, "blind" evaluation may be further improved if talent are evaluated in parallel according to

their lived experiences. Through this parallel evaluation, employers can assess skills with lessened bias but also without dismissing the lived experiences of candidates.

The converse can also be true and should not be understated. For instance, biometrics, machine learning, and behavioral analytics, are all promising and evolving technologies in the cybersecurity field; however, each can be predisposed to biases that disproportionate impact members of diverse communities. Leaders should evaluate new technologies for their potential impact on inclusion as much as their impact on security. One potential lens through which to consider is that we emphasize assessing security as measures of risk, threats, and potential impacts. Failing to consider the positive and negative effects of a control, policy, or technology on your organization's diverse workforce increases the risk that talent will leave, threatens the organization's ability to innovate and adapt, and impacts internal and external reputation.

How Can Leaders Address Diversity and Inclusion Adoption Hesitancy or Dismissal?

We need to confront the reality that diversity is not being effectively leveraged or implemented in some areas of cybersecurity and we need to begin to proactively confront dismissals of the discussion in a nonpartisan and objective way. In short, ignoring diversity, believing we are past the problem, not actively considering inclusion, and quota hiring can all contribute to underperformance or can further entrench staunch critics.

It is the responsibility of leaders to listen to all perspectives, but it is also their responsibility to provide a voice to the underrepresented, embrace the advantages diversity provides to the organization, and articulate the nuances to reticent stakeholders. Leaders should respond to diversity hesitance or dismissal by asking the objector to explain what negatives they anticipate inclusion would bring and the leader should ask them to explain how those perceived negatives somehow outweigh the measurable and humane benefits available from diversity and inclusion efforts.

Ten Ways to Better Incorporate Diversity and Inclusion

According to ICIT Executive Director Joyce Hunter, "Organizations must strive to hear different voices to improve continually. When an issue arises, a meaningful response begins with listening. Diversity, equity & inclusion initiatives must be ongoing and institutionalized. Establishing key performance indicators and holding ourselves accountable to them is the only way forward." To improve diversity and inclusion efforts, our contributors recommend:

1. Listen - What makes the best people in any organization are those who meaningfully add to your culture by challenging the status quo. They ask hard questions on what's working and what isn't and aren't afraid to lead for a change. The best thing leaders can do is to listen from the ground up. And demonstrate a bias for action based on the feedback and be held accountable.

2. Capture decision-makers' attention - Without C-suite buy-in, these DEI programs do not have a chance of survival and impact. There has to be a high-level commitment and accountability from the C-Suite all the way to mid-level management. They need to publicly and proactively support diversity initiatives. They should prioritize diversity, inclusion, and equity with their organization by establishing a diverse C-suite position as well as a diversity program that includes encouraging and allowing time for employees to participate in the program and its multiple groups.
3. Make the C-Suite "Own" the Effort - C-suite level leaders must take on the responsibility to "own and champion" DEI at every opportunity. Equally important, DEI needs to be a CEO-level priority in order to make any measurable difference. However, leaders must ensure and reward accountability, collection of relevant data sets (promotions, awards, bonuses, selection protocols, EEO complaints via each business unit), measures, metrics, and organizational reporting across all business lines. If these are not a key function of any organization, DEI initiatives are pointless! The C-level leaders must be visibly intentional when it comes to DEI. What really matters, get measured!
4. Frame Diversity and Inclusion as a Security Necessity – If leadership considers diversity as a requirement to mitigation misperceptions and bias that occur, then the entire organizational culture will always look for that diversity as a requirement to strengthen the team, improve their decision making, and improve/accelerate their ability to get results. Stress that diversity and inclusion efforts are business enablers and not just altruistic.
5. Leading by example - In order to truly alter the landscape of an organization, leaders must proactively engage and be leaders in diversity and inclusion initiatives - from recognizing the composition of the C-suite, providing budget and resources, using inclusive language, to attending internal events. Often that starts with checking your own privilege and being willing to acknowledge and embrace it--as a leader, you have an obligation to make your organization more welcoming to others, so learning more about your own perspective and privilege can be a powerful first step. Leaders must also actively engage with hiring managers to ensure diversity plays an integral role in the organization's hiring practices and procedures.
6. Communication - You cannot over-communicate early and often enough the importance of your diversity and inclusion efforts to candidates, employees, customers, and stakeholders. Branding is crucial, and one company that has done a great job to broaden the topic of diversity and inclusion is Pinterest, which was one of the first companies to share its diversity data publicly. From implementing the "Rooney Rule" within their recruiting efforts to partnering with outside organizations, such as /dev/color, a nonprofit that helps black engineers build and grow their careers, Pinterest's work has gone beyond just internal efforts showcasing their leadership and commitment in scaling diversity and inclusion.
7. Cultivate Talent - Organizational leaders have a responsibility to cultivate a work culture that thrives on diverse ideas and perspectives. The path to creating that success is through enabling others within the organization to carry out that mission. I believe that diversity is the outcome of inclusion. Focusing on being inclusive from the inside out sets the stage for building a more diverse workforce.
8. Measuring Progress - Talking about diversity and inclusion is one thing, but walking the walk is the true test. In order to view diversity and inclusion as a business priority, one must measure it

as such. Analyzing and dissecting the progress made is important, but equally as important is approaching the future with humility and identifying the areas that need improvement.

9. Hire Intentionally – Diversity needs to be more than just an HR or PR discussion. It needs to be a proactive and forecasting approach with the organization's future needs in mind. Some talent considerations include:
 - a. hire when you find top talent- not when you need it
 - b. Always recruit and always accept exploratory interviews
 - c. Don't hire into established roles; hire top talent and create roles to enable professional development objectives
 - d. Never use the term "employee retention," always use the term "talent development."
 - e. Become educators as leaders and invest in diverse curriculums for multiple stakeholders
 - f. Stop writing job descriptions with prerequisite credentials, use broad definitions of job opportunities
 - g. Never implement a hiring freeze; if you hire too many employees, encourage low performers to re-tool or move onto other areas to balance out the numbers
 - h. Be vulnerable and seek help on how to communicate inclusive behaviors
 - i. Seek alternative channels to develop a pipeline of early in career and diverse employees
 - j. Always ask what candidates want to learn in an interview and then write down what you heard them say. Use this as a basis for the role definition, giving them an opportunity to learn.
10. Consistently Emphasize the Need for Diversity – Work considerations of team composition, ideological biases, etc., into the regular project planning process. Stress it continuously and show it by making diverse job selections. Draw upon different recruitment techniques where diversity is shown, such as job fairs at HBCUs, working closely with human resources to assemble job selection committees that are diverse when jobs are posted, and keeping an open mind and attitude regarding this topic.

Conclusion

America is not a perfect country, and there remains plenty of room for improvement, especially in areas of diversity and inclusion both in general and in cybersecurity specifically. However, diversity is baked into our national identity, and it is the source of our greatest strength. By better leveraging diversity and inclusion efforts in the future, we can rise to address the cyber talent shortage, better secure critical infrastructure against digital adversaries, and advance our nation into the next stage of the digital era.