

January 2020



THE BUSINESS VALUE OF A DIVERSE INFOSEC TEAM

**A Discussion on How Gender, Racial,
Cognitive, and LGBTQ Diversity Improves
Cybersecurity Outcomes**

Authored By:

Parham Eftekhari, Executive Director, ICIT
Drew Spaniel, Lead Researcher, ICIT

ICIT | Institute for Critical
Infrastructure Technology
The Cybersecurity Think Tank

The Business Value of a Diverse InfoSec Team

A Discussion on How Gender, Racial, Cognitive, and LGBTQ Diversity Improves Cybersecurity Outcomes

January 2020

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

- Devon Bryan, Former CISO, The Federal Reserve
- Teddra Thomas Burgess, CRO, Micro Focus Government Solutions
- Jerry Davis, ICIT Fellow & Former CIO, NASA Ames Research Center
- Joyce Hunter, ICIT Fellow & CEO, Vulcan Enterprises LLC
- Don Maclean, ICIT Fellow & Chief Cybersecurity Technologist, DLT

Copyright 2020 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) certain 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

Introduction	3
Diversity in Cybersecurity is a Matter of National Security	3
Focusing on Business Value Will Accelerate Diversity	4
Despite Awareness, Systemic Problems Remain	5
Diversity Comes in Many Forms	7
Minorities in Cybersecurity	7
Women in Cybersecurity	8
Neurodiversity in Cybersecurity	9
LGBTQ+ In Cybersecurity	10
Conclusion: Progress is Happening, but the Acceptance of Diversity Must Accelerate	11
Sources	13

Introduction

National security and critical infrastructure resiliency depend on the success of the cybersecurity community's diversity efforts. Reducing risk to an organization requires cross-functional stakeholder engagement within the business and its supply chain to balance business objectives with security needs. Security teams that bring diversity of thought and perspective to the decision-making process are best equipped to navigate this complex ecosystem of players, technologies, and cultures.

The last several years have seen cybersecurity workforce discussions mature to include diversity as both a competitive advantage and a [solution to the growing talent shortage](#). Leaders increasingly understand that to prepare for the broadest variety of vulnerabilities we need people who are attuned to *all* types of risks participating at *all* levels of the discussion. This evolving mindset can be partially attributed to conversations such as WeLiveSecurity's series [Adventures in cybersecurity research: Risk, cultural theory, and the white male effect](#). This study revealed that relative levels of perceived risk for security-related problems were assessed differently depending on a respondent's age, income, gender, ethnicity, and cultural alignment.

A diverse cybersecurity team maximizes an organization's ability to bring innovation into its efforts and acts as a force multiplier for a company's capacity to combat digital threats. While it is encouraging that increasing diversity has become a widely accepted business value with measurable benefits for corporations, more significant action is required to transform the security workforce. For diversity initiatives to yield maximum results, they must never be implemented due to HR trends, government regulation, or the buzz-worthiness of the term itself. Focusing on diversity is not merely about creating opportunities for marginalized groups; it is about proactively leveraging human variations to ensure that teams are more productive, innovative, and efficient than the homogeneous teams of the past [1].

Diversity in Cybersecurity is a Matter of National Security

In ICIT's August 2019 Bright Minds Q&A Series, "Diversity in Cybersecurity," Devon Bryan, Founder of the International Consortium for Professionals in Cybersecurity and former Federal Reserve CISO said, "Cybersecurity has been identified as one of the most serious economic and national security challenges we face worldwide. Sadly, there is a global underrepresentation of women and other major minority groups in the fast-growing discipline of cybersecurity. Yet, their perspective is essential if we are to protect sensitive networks, systems, applications, and data in public and private sectors critical to our nation's economic health and national security."

Cybersecurity breaches are widely acknowledged by our defense and intelligence agencies as a top national security concern, with the cost of a public sector breach or commercial sector breach averaging \$2.3 million or \$3.92 million, respectively [2] [3]. Overall, it is estimated that cybercrime costs the global economy over \$600B per year, a number expected to grow to \$1 trillion by 2021 [4] [5]. Compounding the threat, the US is expected to suffer a cybersecurity workforce talent shortage of 500,000 employees by 2021, with the global deficit estimated at 3.4 million [6] [7].

Our current workforce challenges have been well documented for over a decade. In 2010, the Center for Strategic and International Studies' (CSIS) report, *A Human Capital Crisis in Cybersecurity*, found that the United States "not only [has] a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer code and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts" [8]. By 2019, CSIS found that the prospects of hiring qualified technical talent had not improved; information technology professionals still consider technical skills such as secure software development the most difficult to find among cybersecurity candidates. By excluding minority groups from the cybersecurity workforce, organizations are limiting their access to qualified talent and creating artificial scarcity through imposed barriers to entry [9].

"Cybersecurity has been identified as one of the most serious economic and national security challenges we face worldwide. Sadly, there is a global underrepresentation of women and other major minority groups in the fast-growing discipline of cybersecurity. Yet, their perspective is essential if we are to protect sensitive networks, systems, applications, and data in public and private sectors critical to our nation's economic health and national security."

- Devon Bryan, Founder of the International Consortium for Professionals in Cybersecurity & Former Federal Reserve CISO

Therefore, a more diverse cybersecurity workforce has become critically important in addressing the risks to our economic and national security as well as addressing the human talent gap in cybersecurity. By failing to identify, hire, train, and promote diverse candidates, we are inadvertently and artificially narrowing our human talent pool. According to Devon Bryan, we are also "excluding possible collective creativity that could be instrumental in helping us solve the problems we continue to face, year over year, in the field."

Focusing on Business Value Will Accelerate Diversity

Teddra Thomas Burgess, Chief Revenue Officer at Micro Focus Government Solutions, asserts that, "The customers our industry serves are an increasingly diverse population with increasingly complex needs. Yet, diversity of thought and cultural experience are underestimated or entirely absent from consideration in workforce planning. Often, diversity

initiatives are only launched when we see the negative impact caused by a lack of diverse representation. Until we first seek to acknowledge and understand the need for increased diversity in cybersecurity, we cannot properly execute on any initiative or achieve the outcomes we seek.”

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.

“The customers our industry serves are an increasingly diverse population with increasingly complex needs. Yet, diversity of thought and cultural experience are underestimated or entirely absent from consideration in workforce planning. Often, diversity initiatives are only launched when we see the negative impact caused by a lack of diverse representation. Until we first seek to acknowledge and understand the need for increased diversity in cybersecurity, we cannot properly execute on any initiative or achieve the outcomes we seek.”

- Teddra Thomas Burgess,
Chief Revenue Officer at
Micro Focus Government
Solutions

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.

Studies have also shown that diversity in leadership improves the bottom line for businesses. A recent McKinsey & Co. study of 180 publicly traded companies found that companies in the top quartile of executive-board diversity had returns on equity 53% higher, on average, than those in the bottom quartile. At the same time, the most diverse companies had earnings before tax and interest margins that were 14% higher, on average, than those of the least diverse companies [10].

Despite Awareness, Systemic Problems Remain

The past decade has seen a sharp increase in the technology community’s focus on diversity. At a January 2019 AFCEA event in Augusta, Georgia, Senior Cybersecurity Advisor to the NSA, Director Rob Joyce, emphasized the need for formal and informal education, diversity in cybersecurity, and continuous learning, stating, “[In 2019] Less than 65,000 people will graduate with undergraduate degrees in the computer and information science fields. That’s

not cybersecurity. That includes all [information technology] and computer science students across the country. That's a scary figure when we say we have more than 300,000 open jobs."

Of the estimated 65,000 graduates in information science and computer science fields in 2019, only an estimated 12,000 are women. Joyce continued, "I think if you are looking for a strategic lever that the nation has to pull, the first thing we have to do is balance that pipeline out to represent our population. If we can get women into the computer science/cybersecurity field at the same level as men, we will see a substantial increase in that pipeline. It's the same for minorities. If the computer science outlook looked like the demographics of our country, we would up those numbers [in the pipeline] significantly" [11].

The [\(ISC\)² Cybersecurity Workforce Study: Women in Cybersecurity](#) found that while men currently outnumber women in cybersecurity by about three to one overall, women in the field are advancing to leadership positions. According to survey respondents, higher percentages of women than men are attaining senior leadership and decision making positions:

- Chief Technology Officer – 7% of women vs. 2% of men
- Vice President of IT – 9% of women vs. 5% of men
- IT Director – 18% of women vs. 14% of men
- C-level/Executive – 28% of women vs. 19% of men

Despite this progress, pay inequities persist. According to the report, 17% of women reported annual salaries between \$50,000 – \$90,000, as compared to 29% of men, and 15% of women earned between \$100,000 – \$499,999, compared to 20% men.

"The world is made up of people from many different backgrounds, and yet, our cybersecurity workforce does not reflect this diversity. Across the board, Latino and Black employees are massively underrepresented, accounting for less than 10% of the workforce across many large organizations, including Facebook, Microsoft and Salesforce."

- Joyce Hunter, CEO of
Vulcan Enterprises

ICIT Fellow Joyce Hunter, who is the CEO of Vulcan Enterprises, explains that, "The world is made up of people from many different backgrounds, and yet, our cybersecurity workforce does not reflect this diversity. Across the board, Latino and Black employees are massively underrepresented, accounting for less than 10% of the workforce across many large organizations, including Facebook, Microsoft, and Salesforce." Recent studies underscore this lack of diversity in many organizations. For instance, the recent the [\(ISC\)² Innovation Through Inclusion Report](#) showed that, in the US, cybersecurity professionals from minorities generally hold higher academic degrees than their Caucasian counterparts, yet make less money and hold fewer managerial and leadership positions. The same study found that women of color in cybersecurity make nearly 10% less than their white, male counterparts in the same starting position. The Fortinet report, [Exploring the Benefits of Gender Diversity in Cybersecurity](#), found

that 32% of minorities say they have experienced discrimination at work despite organizational efforts to combat conscious and unconscious biases [10]. These metrics, and others, show that while progress is being made, inequality and underrepresentation are still prevalent.

Diversity Comes in Many Forms

The projected shortage of cybersecurity talent is expected to increase to 1.8 million by 2022, according to the Center for Cyber Safety and Education. Diversity initiatives could address this threat to our nation's resiliency while improving cybersecurity innovation and problem solving.

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 [1]. 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 [1].

Ultimately, it is up to cybersecurity leaders to recognize the benefits of each type of diversity and to determine how to effectively incorporate it into the workforce [12]. The following is a summary of some underrepresented communities in the cybersecurity community.

Minorities in Cybersecurity

In the 2018 release of McKinsey's [Delivering Through Diversity](#) study, 39% of the US population classifies as a minority. However, only 12% of minorities occupied executive positions and 15% were part of the board of directors [13].

There is a clear diversity problem within cybersecurity. According to the [\(ISC\)² Innovation Through Inclusion Report](#), minority representation in the cybersecurity field is slightly higher than the overall US minority workforce, at 26% compared to 21%. However, the study also revealed that racial and ethnic minorities tend to hold non-managerial positions and that pay discrepancies exist, particularly for minority women. In addition to these inequities, the technology community faces challenges in retaining personnel from underrepresented groups once they enter the workforce.

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.

To address these issues, ethnic diversity must go well beyond meeting a quota. According to Devon Bryan, “You might be meeting the spirit, but are you really meeting the intent? The simplest recipe for success is leading high-performing teams. Everyone wants to feel valued, irrespective of race, gender, religion, sexual affiliation, and age.” He explained that organizations must embody the various dimensions of the diversity spectrum, ensuring that the opinions and perspectives of everyone matters by making their voices heard.

It is critically important for leaders to ensure that women and 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 [14].

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](#).

Women in Cybersecurity

The United States is not efficiently recruiting women, who comprise approximately half the population, into cybersecurity roles [15]. According to a 2018 (ISC)² study, there are even fewer women in US government cybersecurity than there are proportionally in cybersecurity globally. The US 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

According to a project between Fortinet and Datalere, some systemic bias against women and minorities 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 [10]:

- Of the top 20 skills employers list as a requirement in their job descriptions for CISO placements, 17 are considered soft skills.
- On resumes, females 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 in Cybersecurity

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 has 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 [16].

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 [16].

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 providing 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.

Conclusion: Progress is Happening, but the Acceptance of Diversity Must Accelerate

While diversity efforts have produced measurable results, more must be done to ensure diverse cybersecurity teams are the norm, not an exception.

To have a balanced discussion on diversity, it is important to highlight signs of progress, which include:

- The announcement of new Girl Scout Cybersecurity Badges in January 2017
- The Obama Administration Cybersecurity Grants to historically black colleges and universities (HBCUs) and community colleges
- An increasing number of female speakers at major cybersecurity conferences
- The growth of organizations that focus on minorities in cybersecurity, including:
 - Girls Who Code
 - Black Girls Code
 - Executive Women's Forum
 - Women in Cybersecurity
 - Women Cyberjutsu

"Diversity isn't just a philosophical issue; the US cybersecurity workforce desperately needs more talented technical staff to fill a surfeit of open positions. For the sake of our nation, we must draw from every resource pool by making the profession both attractive and equitable."

- Don Maclean, Chief
Cybersecurity Technologist
at DLT

As we look toward the next decade, the business and technology community must rapidly come together to build on these successes. This can only begin when it is widely understood and accepted that organizations that prohibit discrimination in all forms and embrace structures that empower diverse thinking will have an enormous competitive advantage over rival businesses and emerging threats alike [12].

Some among us may erroneously argue that including diverse employees subjects the organization to undue constraints or imposes a burden of accommodation upon the company. That view is cloistered and unreflective of the agile thought necessary to evolve with the cyber threat landscape. Often, organizations will find that accommodating one employee actually improves the work environment for many personnel. For instance, designating a quiet area for noise-sensitive employees can also benefit employees who prefer conversation or music by

creating conflict-free work areas that empower personnel to work in whichever environment they find most productive [12].

The greatest challenge to increasing diversity may actually lie in the recruitment strategies currently implemented. IT leaders need to overhaul their strategies to encourage diverse people to apply for mission-critical positions. This may include wording job adverts constructively to prevent inherent biases, increasing the emphasis on skills over degrees, or by phasing out boiler-plate interview questions with skills-based challenges, samples of work, and aptitude assessments [12]. According to ICIT Fellow and DLT's Chief Cybersecurity Technologist, Don Maclean, "Diversity isn't just a philosophical issue; the US cybersecurity workforce desperately needs more talented technical staff to fill a surfeit of open positions. For the sake of our nation, we must draw from every resource pool by making the profession both attractive and equitable"

Sources

- [1] J. Frankland, "#2018 In Review Women and Diversity in Cybersecurity", *Infosecurity Magazine*, 2018. [Online]. Available: <https://www.infosecurity-magazine.com/opinions/2018-women-diversity/>. [Accessed: 07- Jan- 2020].
- [2] M. McCarter, "State and Local Governments Face High Costs from Data Breaches", *StateTech*, 2019. [Online]. Available: <https://statetechmagazine.com/article/2018/09/state-and-local-governments-face-high-costs-data-breaches>. [Accessed: 07- Jan- 2020].
- [3] L. Ponemon, "What's New in the 2019 Cost of a Data Breach Report", *Security Intelligence*, 2019. [Online]. Available: <https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/>. [Accessed: 07- Jan- 2020].
- [4] D. Palmer, "Cybercrime drains \$600 billion a year from the global economy, says report", *ZDNet*, 2018. [Online]. Available: <https://www.zdnet.com/article/cybercrime-drains-600-billion-a-year-from-the-global-economy-says-report/>. [Accessed: 07- Jan- 2020].
- [5] S. Morgan, "Cybercrime Damages \$6 Trillion by 2021", *Cybercrime Magazine*, 2019. [Online]. Available: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. [Accessed: 07- Jan- 2020].
- [6] J. Stone, "How much of the cybersecurity talent shortage is self-inflicted? - CyberScoop", *CyberScoop*, 2018. [Online]. Available: <https://www.cyberscoop.com/cybersecurity-talent-shortage-self-inflicted-problem/>. [Accessed: 07- Jan- 2020].
- [7] D. Barton, "The Cybersecurity Talent Gap = an Industry Crisis", *Securitymagazine.com*, 2019. [Online]. Available: <https://www.securitymagazine.com/articles/90182-the-cybersecurity-talent-gap-an-industry-crisis>. [Accessed: 07- Jan- 2020].
- [8] K. Evans and F. Reeder, "A Human Capital Crisis in Cybersecurity", *Csis.org*, 2010. [Online]. Available: <https://www.csis.org/analysis/human-capital-crisis-cybersecurity>. [Accessed: 07- Jan- 2020].
- [9] W. Crumpler, "The Cybersecurity Workforce Gap", *Csis.org*, 2019. [Online]. Available: <https://www.csis.org/analysis/cybersecurity-workforce-gap>. [Accessed: 07- Jan- 2020].
- [10] "Exploring the Benefits of Gender Diversity in Cybersecurity", *Fortinet Blog*, 2019. [Online]. Available: <https://www.fortinet.com/blog/business-and-technology/exploring-benefits-gender-diversity-cybersecurity.html>. [Accessed: 07- Jan- 2020].

[11] J. Simpson, "Urgent Need for Cybersecurity Professionals Grows", *SIGNAL Magazine*, 2019. [Online]. Available: <https://www.afcea.org/content/urgent-need-cybersecurity-professionals-grows>. [Accessed: 07- Jan- 2020].

[12] K. O'Flaherty, "How diversity can help fight cyber-attacks", *Information Age*, 2018. [Online]. Available: <https://www.information-age.com/how-diversity-can-cyber-123477494/>. [Accessed: 07- Jan- 2020].

[13] J. Orr, "The Need For Diversity In A Cyber Security Workforce", *Cyber Security Hub*, 2019. [Online]. Available: <https://www.cshub.com/interviews/interviews/the-need-for-diversity-in-a-cyber-security-workforce>. [Accessed: 07- Jan- 2020].

[14] D. Bryan, "ICIT Bright Minds: Diversity in Cyber with Devon Bryan, CISO, Federal Reserve - Institute for Critical Infrastructure Technology", *Institute for Critical Infrastructure Technology*, 2019. [Online]. Available: <https://icitech.org/icit-bright-minds-diversity-in-cyber-with-devon-bryan-ciso-federal-reserve/>. [Accessed: 07- Jan- 2020].

[15] J. Marks, "The Cybersecurity 202: There are even fewer women in U.S. government cybersecurity than there are globally", *The Washington Post*, 2019. [Online]. Available: <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/04/10/the-cybersecurity-202-there-are-even-fewer-women-in-u-s-government-cybersecurity-than-there-are-globally/5cad44531ad2e567949ec115/?noredirect=on>. [Accessed: 07- Jan- 2020].

[16] N. Thacker, "Supporting neurodiversity in cybersecurity", *ITProPortal*, 2019. [Online]. Available: <https://www.itproportal.com/features/supporting-neurodiversity-in-cybersecurity/>. [Accessed: 07- Jan- 2020].