FROST & SULLIVAN

(ISC)²

CENTER FOR CYBER SAFETY AND EDUCATION

International Consortium of Minority CYBERSECURITY PROFESSIONALS

Innovation Through Inclusion: The Multicultural Cybersecurity Workforce

An 2017 Global Information Security Workforce Study

A Frost & Sullivan White Paper

by Jason Reed, Consulting Analyst, Digital Transformation, Frost & Sullivan and Jonathan Acosta-Rubio, Market Research Analyst, (ISC)²

INTRODUCTION

For the first time, the Global Information Security Workforce Study features a deeper dive into the diverse composition of the U.S. cybersecurity workforce to encompass not only gender, age and tenure, but ethnicity and race as well. This is the 8th edition of the study. The Center for Cyber Safety and Education partnered with (ISC)[2] , Booz Allen Hamilton (Presenting sponsor), Alta Associates (Gold sponsor), and Frost & Sullivan to examine the state of the response to these developing risks in the 2017 Global Information Security Workforce Study (GISWS).

Key findings from the report indicate that minority representation within the cybersecurity profession (26%) is slightly higher than the overall U.S. minority workforce (21%)[1]. Employment among cybersecurity professionals who identify as a racial or ethnic minority tends to be concentrated in non-management positions, with fewer occupying leadership roles, despite being highly educated.

Among minority cybersecurity professionals, 23% hold a role of director or above, 7% below the U.S. average. Interestingly, minorities who have advanced into leadership roles often hold higher degrees of academic education than their Caucasian peers who occupy similar positions; of minorities in cybersecurity, 62% have obtained a master's degree or higher, compared to 50% of professionals who identified as White or Caucasian. Wh ile it's been noted that academic degrees do not necessarily imply a more advanced level of skill, it has typically been considered a hiring prerequisite for most employers[2]. Additional research has revealed that higher levels of education among leaders can contribute to the greater overall success of an organization.

Multiple studies have pointed out that diversity in leadership has a positive impact on an organization's overall profitability. In a comprehensive review of 180 publicly traded companies, McKinsey & Company noted:

> *"The findings were startlingly consistent: for companies ranking in the top quartile of executive-board diversity, Returns on Equity were 53 percent higher, on average, than they were for those in the bottom quartile. At the same time, Earnings Before Tax and Interest margins at the most diverse companies were 14 percent higher, on average, than those of the least diverse companies."*

McKinsey & Company's study shows that the benefits of a diverse leadership team are multifaceted; thus creating a culture that inspires workers to approach problems and challenges from different perspectives that ultimately help an organization excel. Diversity is not only important for driving company growth and profit, it is vital in the cybersecurity profession that depends on unique approaches to problems and challenges to protect an organization. Moreover, hiring a more diverse workforce is essential to addressing the ever-widening projected workforce gap.[3]

1 Source: Labor force characteristics by race and ethnicity, 2015, U.S. Bureau of Labor Statistics

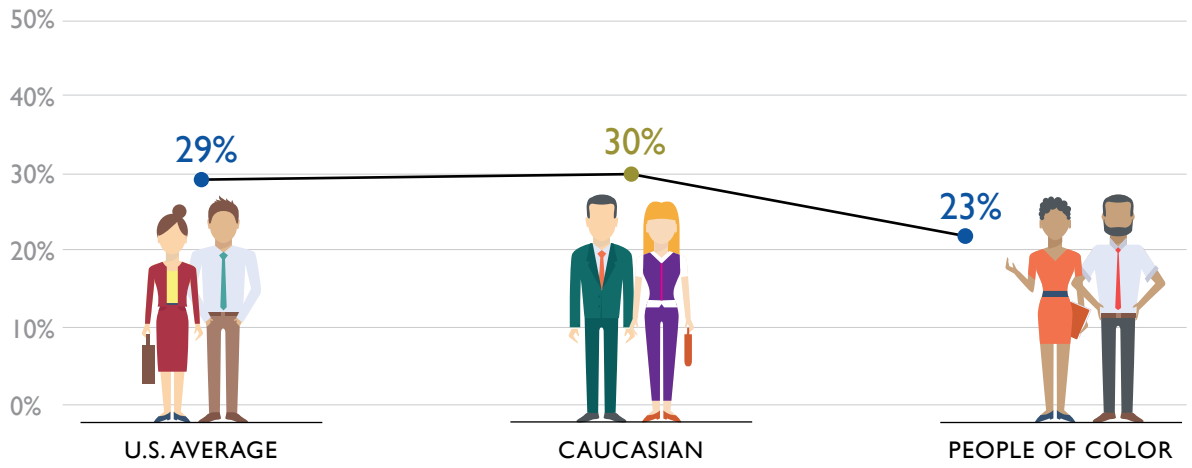
2 Source: 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk

3 Source: Thomas Barta, Markus Kleiner, and Tilo Neumann. "Is There a Payoff from Top-Team Diversity?" McKinsey & Company

REPRESENTATION WITHIN ORGANIZATIONS

While there are a number of ways to define diversity, this particular study focused on race and ethnicity and defines minorities and people of color as those who do not self-identify as White or Caucasian. This group makes up 26% of the U.S. cybersecurity workforce, which is roughly in line with the 28% of the general U.S. population[4]. In the U.S. cybersecurity industry, 9% of workers self-identified as African American or Black, 4% as Hispanic, 8% as Asian, 1% as American Indian or Alaskan Native and Native Hawaiian/Pacific Islander, and 4% self-identifying as "Other."

Exhibit 1: Proportion of Workers in Leadership Roles (Director Level or Above)



Source: 2017 Global Information Security Workforce Study, (n = 2,771)

In the U.S., 17% of the cybersecurity workforce who identify as a minority are female, proportionally exceeding overall female representation (14%) by a margin of 3%. This demonstrates that the presence of women of color positively impacts workforce numbers and not by simply increasing the quantity of females within the profession. It is worthy to note that North America leads the world in female participation rates in cybersecurity at 14%[5].

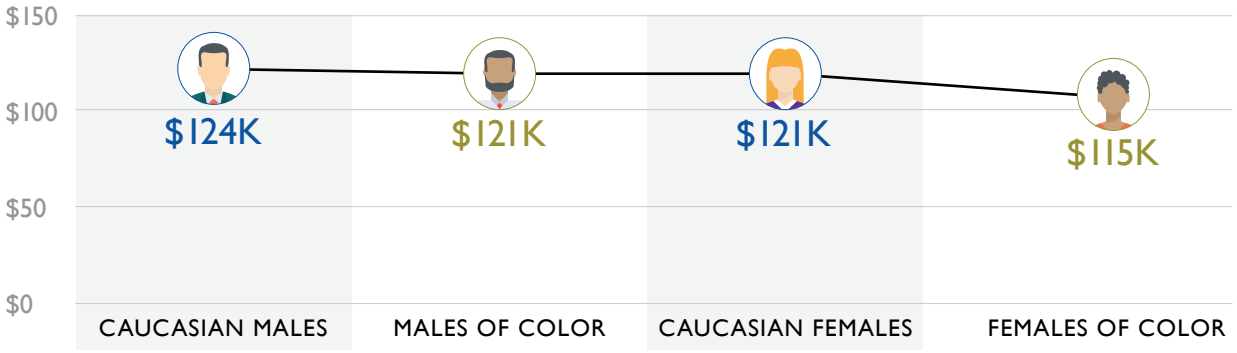
4 Source: https://www.census.gov/newsroom/releases/archives/2010_census/cb11-cn125.html

5 Source: 2017 Global Information Security Workforce Study: Women in Cybersecurity

SALARY DISCREPANCIES

While the average salary of a cybersecurity professional of color is $115,000 USD, research does show that there is still room for them to earn even more. On average a cybersecurity professional of color earns less than the overall U.S. cybersecurity workforce average of $122,000 USD. Salary figures within the profession indicate that Caucasian males earn on average $124,000 USD, and males who do not identify as Caucasian earn $121,000 USD, while females of color earn nearly $10,000 USD less, at $115,000 USD.

Exhibit 2: Average Salary by Minority Group (In $1,000 USD)

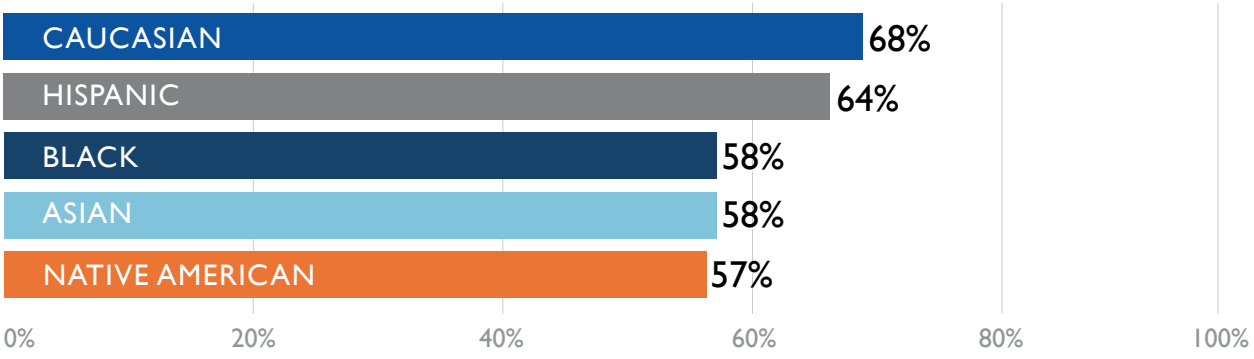


Source: 2017 Global Information Security Workforce Study (n = 9,311)

Lower wages among females who identified as Black, Hispanic, Asian or of Native origin are of particular note, as it reveals a significant intersection of race and gender, where the sum of two diverse personal attributes yield lower wages.

In addition to a higher average salary, Caucasian workers were more likely to receive a salary increase within the past year, as compared to other races and ethnicities.

Exhibit 3: Percentage Who Received a Raise in the Past Year



Source: 2017 Global Information Security Workforce Study (n = 9,311)

Minority underrepresentation in leadership roles, coupled with lower average compensation and fewer reported instances of salary increases, seem to create a trifecta of obstacles for minorities pursuing a career in cybersecurity. Beyond lower salaries and fewer holding leadership roles, minorities in cybersecurity are disproportionately affected by other, less tangible barriers to entry and advancement.

DISENFRANCHISEMENT AND DISCRIMINATION

The 2017 Global Information Security Workforce Study examined, for the first time, both conscious and unconscious forms of discrimination in the workplace. For the purposes of this study, discrimination can take the form of unfair treatment based on gender, age, ethnicity or an employee's cultural group. The results of the survey reveal that discrimination is most prevalent along two intersecting axes, ethnicity and gender.

Overall, 32% of cybersecurity professionals of color who participated in the survey report that they have experienced some form of discrimination in the workplace. Across all races and ethnicities, women experience greater rates of discrimination in the workplace than men, reporting discrimination in much greater proportions than men when viewed as a total U.S. population. Women who identify as Black, Hispanic, Asian or of Native American descent, report the highest numbers of discrimination.

Exhibit 4: Discrimination Reporting by Gender

	Overt discrimination	Unconscious discrimination	Unexplained denial or delay in career advancement	Exaggerated highlighting of mistakes, errors or occurrences	Tokenism
ALL WOMEN	10%	45%	27%	15%	11%
ALL MEN	1%	6%	4%	2%	3%
CAUCASIAN WOMEN	1%	7%	4%	2%	2%
CAUCASIAN MEN	0%	1%	1%	1%	1%
HISPANIC WOMEN	17%	35%	19%	19%	18%
HISPANIC MEN	9%	9%	7%	3%	3%
BLACK WOMEN	10%	44%	35%	19%	16%
BLACK MEN	0%	4%	2%	1%	0%
ASIAN WOMEN	10%	28%	26%	15%	18%
ASIAN MEN	1%	1%	1%	1%	1%
NATIVE WOMEN	17%	44%	33%	17%	17%
NATIVE MEN	9%	53%	22%	22%	25%

Source: 2017 Global Information Security Workforce Study (n = 1,895)

When examining the responses of women across all races and ethnicities, those who identified as a minority, report discrimination in even higher numbers across every category, presenting an enormous barrier to entry and advancement for minority women in cybersecurity.

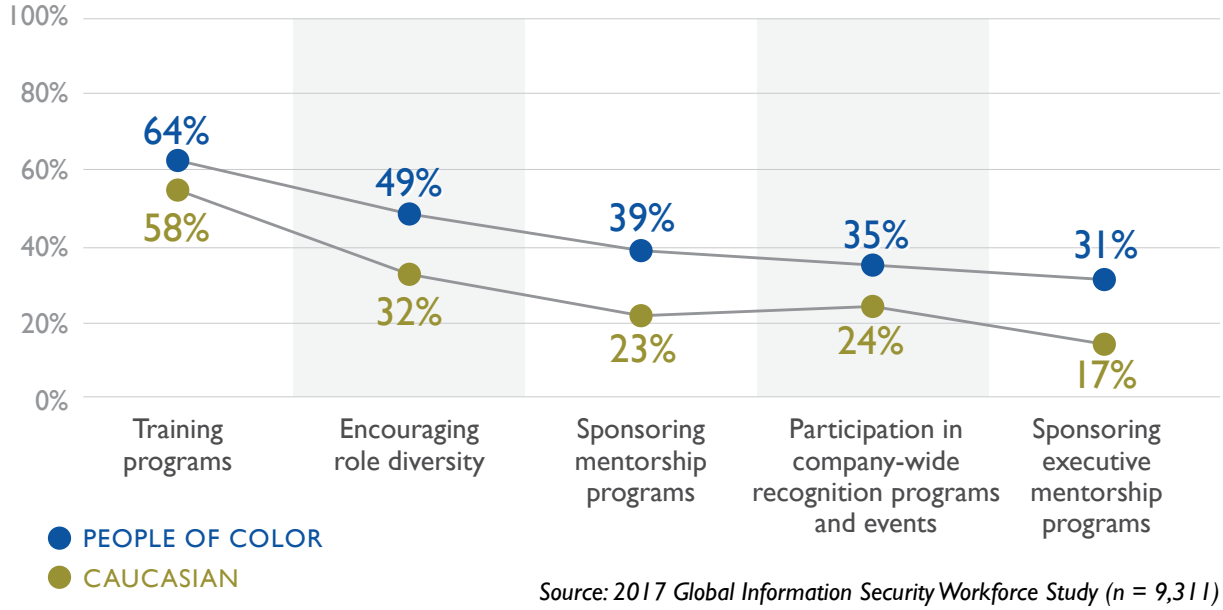
ADDRESSING THE BARRIERS

Among the ethnically and racially diverse professionals that help compose the cybersecurity workforce, optimism is strong despite the unique obstacles they face. This group of professionals report almost equal levels of job satisfaction when compared to the U.S. average; (75% are satisfied in their current position, compared to the U.S. average of 78%) and also feel that they are not only valued, but contribute to their organizations' success at a similar rate of the overall U.S. average (70% vs. the U.S. average of 76%).

This diverse and confident group represents a significant portion of the cybersecurity workforce, but remain underrepresented in senior roles. Diversity at the leadership level has been shown to positively impact both organizational culture and bottom line. Employers should be encouraging the growth and development of a skilled cybersecurity organization by looking at its own ranks.

This study also examined the significance this group of professionals places on various initiatives central to attracting, hiring and retaining top-notch employees.

Exhibit 5: Importance of Programs by Ethnicity (% Very Important)



Source: 2017 Global Information Security Workforce Study (n = 9,311)

In each case, these professionals are more likely to place value on mentorship and training programs that support professional development and career advancement, a trend seen across various diverse groups, including millennials[6], women[7] and racial and ethnic minorities. Implementing and encouraging participation in programs designed to address the unique challenges faced by these diverse groups not only has the potential to advance, embolden and elevate individuals, but support and stimulate progress and growth within the cybersecurity workforce.

6 Source: 2017 Global Information Security Workforce Study: Meet the Millennials

7 Source: 2017 Global Information Security Workforce Study: Women in Cybersecurity

IN CONCLUSION

1. Minority professionals make up a significant portion of the cybersecurity workforce, but are underrepresented across senior roles within their organizations.
2. Studies show that organizations with racially and ethnically diverse leadership teams benefit both company culture and bottom line revenues, while also adding to the overall confidence of an organization's security posture.
3. Measures that can be taken by organizations to help foster, promote and nurture the success of this group include:
    - Mentorship and training programs
    - Executive leadership programs to promote the advancement of the multicultural workforce
    - Company-wide recognition programs and events

ABOUT CENTER FOR CYBER SAFETY AND EDUCATION

The Center for Cyber Safety and Education (the Center), is a non-profit charitable trust committed to making the cyber world a safer place for everyone. The Center works to ensure that people across the globe have a positive and safe experience online through their educational programs, scholarships, and research. Visit www.iamcybersafe.org.

ABOUT (ISC)²

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, over 130,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry.

Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – the Center for Cyber Safety and Education™. For more information on (ISC)², visit www.isc2.org, follow us on Twitter or connect with us on Facebook.

ABOUT ICMCP

The International Consortium of Minority Cybersecurity Professionals (ICMCP) is a 501(c)(3) non-profit organization. It began official operations in September 2014 and is organized exclusively for charitable purposes, to provide members with educational/technical scholarships, mentoring opportunities, professional development, and networking opportunities. For more information or to become a sponsor, please visit https://icmcp.org/, follow @ICMCP_ORG on Twitter or visit the ICMCP LinkedIn page.

ABOUT THE GLOBAL INFORMATION SECURITY WORKFORCE STUDY

The Global Information Security Workforce Study (GISWS), is conducted every two years by (ISC)² and its Center for Cyber Safety and Education. The latest worldwide study was conducted from June 22 through September 11, 2016. This online survey gauged the opinions of 19,641 information security professionals from 170 countries regarding trends and issues affecting their profession and careers. It was designed to capture expansive viewpoints and produce statistically significant findings. The Center has conducted similar surveys since 2004 and has made results available to private, governmental and nonprofit organizations as a means for these organizations to plan, assess and implement workforce policies. The study was conducted by Frost and Sullivan and sponsored by (ISC)² and Booz Allen Hamilton and Alta Associates. The findings from this massive study have been released in a series of dedicated reports.

2017 FEATURED REPORTS

WOMEN IN CYBERSECURITY

Co-authored by the Executive Women's Forum on Information Security, Risk Management & Privacy and (ISC)². Presented by PricewaterhouseCoopers. Sponsored by Alta Associates, IBM and Veracode. This report takes a new and unique look into the vital role women play in cybersecurity today and in the future.

MILLENNIALS IN SECURITY

Presented by (ISC)² and Booz Allen Hamilton. This online, interactive infographic takes a look into the future information security workforce. What makes them tick? How do I attract and retain these vital employees?

U.S. GOVERNMENT SECURITY WORKFORCE

Presented by (ISC)². Government security has always been in the forefront of the news, but now more than ever, the general has public paid attention. Take a look at the people who work behind the scenes with our national secrets and security.

GLOBAL / REGIONAL REPORTS

Presented by (ISC)² and Booz Allen Hamilton. This series of reports focuses on the global workforce as a whole, but also takes a closer look at data through a regional lense (EMEA, APAC, LATAM and North America).

These reports (and past reports) are found at www.isc2.org/research or www.IAmCyberSafe.org/gisws.

FROST & SULLIVAN

SILICON VALLEY
3211 Scott Blvd
Santa Clara, CA 95054
Tel 650.475.4500
Fax 650.475.1571

SAN ANTONIO
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

LONDON
Floor 3 - Building 5,
Chiswick Business Park,
566 Chiswick High Road,
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
3211 Scott Blvd
Santa Clara, CA 95054