ICIT'S BRIGHT MINDS Q&A SERIES

Diversity in Cybersecurity

with

DEVON BRYAN

CISO, FEDERAL RESERVE SYSTEM

August 2019

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

ICIT's Bright Minds Q&A Series
Diversity in Cybersecurity
With Devon Bryan, CISO, Federal Reserve System

August 2019

About ICIT's Brightest Mind Series:

In continued support of our mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders, ICIT has embarked on a journey to hold candid interviews with some of the brightest minds in national security, cybersecurity and technology. Our goal is to share their knowledge and insights with our community to shed light on solutions to the technology, policy, and human challenges facing our community. Our hope is that their words will motivate, educate, and inspire you to take on the challenges facing your organizations

About this Bright Mind: Devon Bryan, V.P. & CISO, Federal Reserve System

Devon Bryan is Executive Vice President and Chief Information Security Officer for the Federal Reserve System. As Chief Information Security Officer (CISO), Devon oversees information security, including incident response, for the enterprise, ensuring information security architecture, standards, policies and programs remain effective and efficient. Devon was appointed System CISO in February 2016.

Devon came to the Federal Reserve from Fortune 500 payroll and human resources provider ADP, where he served as Global Chief Information Security Officer (CISO). Devon led ADP's information security strategy, collaborating across the company's geographically dispersed business operations to ensure coordination, consensus, and effective execution across global operations. Prior to joining ADP in 2011, he served as the Deputy Chief Information Security Officer (CISO) for the Internal Revenue Service (IRS) after directing the IRS's FISMA-compliant information security program and leading the IRS's incident response team.

His information security career began in the U.S. Air Force, where he served as a Captain and lead engineer working on systems and programs to protect the critical network and communications tools of the Air Force's Air Combat Command.

Devon is Co-Founder & President of ICMCP (International Consortium of Minority Cybersecurity Professionals), which he launched in an attempt to bridge the 'great minority cyber divide' by providing academic scholarships, innovative outreach, mentoring and networking programs targeting minority cyber security professionals worldwide and by promoting academic and technical excellence in our tradecraft.

Devon received a Bachelor of Science, Applied Mathematics from South Dakota Technological University and a Master of Science, Computer Science from Colorado Technological University, graduating Summa Cum Laude. He holds multiple certifications: CISSP, CIPP/US, CIPP/EU, and CISA and participates in several industry forums and is a sought-after speaker and writer on emerging cyber security trends and issues.

ICIT:

What are the benefits of a diverse workforce, and how can those advantages be emphasized?

Devon Bryan:

According to the latest report McKinsey Report on workforce diversity, "Delivering Through Diversity," the more diverse the leadership team, the better the company's financial performance. The latest study looked at the profits and value built by more than 1,000 companies in 12 nations. Companies ranking in the top quarter for gender diversity were 21 percent more likely to see above-average profitability than those in the bottom quarter. An even more dramatic stat: When it comes to ethnic diversity, companies in the top quartile (specifically among executive positions) were 33 percent more likely to see above-average profitability than those with the least ethnic diversity among executives. Profit-motivation aside, tangible message that "diversity wins" also extends to mission-oriented companies and organizations.

Contrast the positive takeaways from the McKinsey Report with the hard truths from the cybercrime predictions of Internet research firm Cybersecurity Ventures which forecasts that cybercrime will continue rising and cost businesses globally more than $6 trillion annually by 2021. An estimate they based on historical cybercrime figures including recent year-over-year growth, a dramatic increase in hostile nation-state sponsored and organized crime gang hacking activities, a cyber-attack surface which will be an order of magnitude greater than it is today, and the cyber defenses expected to be pitted against hackers and cybercriminals over that time. The cybercrime predictions juxtaposed against ISC2's cybersecurity workforce research which cites a workforce shortage of 498,000 skilled professionals in the United States alone, and 2.93 million globally, does paint a very gloomy picture for our heavily Internet-connected and technology dependent society.

Could the infusion of fresh perspectives from non-traditional and underrepresented channels to help fight cybercrime not only fill the critical staffing needs but also stem turn the tables on bad actors?

ICIT:

How does increasing the diversity of the cyber-workforce improve national security and the resiliency of critical infrastructure networks?

Devon Bryan:

Cybersecurity has been identified as one of the most serious economic and national security challenges we face worldwide. Sadly however, there is global underrepresentation of women and other major minority groups in the fast-growing discipline of cybersecurity. Protecting

sensitive networks, systems, applications and data in the public or private sectors is critical to our Nation's economic health is foundational to our national security. Based on various industry reports reciting the shortage of skilled labor and the harsh realities of an exploding cyber threat landscape, non-traditional approaches must be pursued to cultivate strong, skilled cybersecurity workforce pipelines, not just within the federal government, but throughout the whole of the economy. A more diverse cybersecurity workforce has therefore become critically important in addressing the cybersecurity workforce shortage that has adverse consequences on our national economic security and our national security not only because we are inadvertently and artificially narrowing our hiring pipelines but 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.

ICIT:

ICMCP (International Consortium for Minority Cybersecurity Professionals - https://www.icmcp.org/) was founded in 2015, with the official launch of ICMCP being a Town Hall on Minority Underrepresentation of Women and Minorities held in Congress co-hosted with ICIT.

Since the ICIT/ICMCP Town Hall, do you feel there has been progress with respect to opportunities for women and people of color in the field of cybersecurity, and if so please describe ('opportunities' could mean upward movement, new jobs, c-level roles, education, etc.)?

Devon Bryan:

Since the October 2015, "National Townhall on Underrepresentation of Women and Minorities in Cybersecurity" sponsored by Congresswomen Sheila Jackson-Lee (D-TX) and Judy Chu (D-CA) and hosted by our two non-profits, the Institute for Critical Infrastructure Technology (ICIT) and the International Consortium of Minority Cybersecurity Professionals (ICMCP), both of whom were still in their startup phases back then, I'd have to say much progress has indeed been made across the domestic cybersecurity industry but there still however remains so much more to do as evidenced by the 2018 International Information System Security Certification Consortium (ISC2) workforce research, citing women as representing 22% of the US cybersecurity staff despite being 48% of the US labor force. Although this 22% is still less than ideal, it is a 100% increase from the previous years' reported participation rates of women in the cybersecurity industry which have been averaging between 10% - 11%. A related 2018 study also conducted by ISC and titled "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce," reports that a mere 26% of the US cybersecurity workforce identifies as non-Caucasian according.

The harsh realities of the supporting facts and data notwithstanding, there has also been noteworthy intangible progress that has been made to include the fact that there's hardly a cybersecurity conference anymore where there isn't at least one major keynote on cyber diversity or prominent keynote slots afforded female speakers. As an example, the RSA Conference USA 2019 (the world's largest cybersecurity event with more than 40,000 people and 740 speakers) serves as a compelling measuring stick for representation of women in our field and at this year's Conference a reported 46 percent of all keynote speakers were women, achieving near gender parity this year for keynote speakers at this year's conference…a first for the event. Other more tangible progress includes:

- The January 2017 announcement of new Girl Scout Cybersecurity Badges
- The Obama Administration Cybersecurity Grants to HBCUs and Community Colleges
- DHS Cybersecurity Internships
- Great progress being made by the following organizations
    - Girls Who Code
    - Black Girls Code
    - Executive Women's Forum
    - Women in Cybersecurity
    - Women Cyberjutsu
- The February 2016, the Cybersecurity National Action Plan calling for innovation and investments in cybersecurity education and training to strengthen the talent pipeline

I would also cite the House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection and Innovation hearing held on May 21 highlighting the importance of growing and diversifying the cybersecurity talent pipeline as a sign of progress in that increasingly the legislators are also taking note of the acuteness

ICIT:

Since the ICIT/ICMPC Town Hall, what has ICMCP accomplished to help move the needle forward?

Devon Bryan:

The Founders of ICMCP had no illusion that our tiny grassroots volunteer-led organization would completely solve this massive problem for our industry overnight or even a specific time horizon. What we committed to back in 2014 when we created the 501C3 and what we will continue to be laser focused on, is how do we change the trajectory of young deserving lives one female and minority practitioner at a time and the ripple effect of those life transformation in the families and communities of our female and minority members.

So like most organizations engaged in similar social causes to transform lives, we too can rattle off stats regarding the number of academic/certification award scholarships we've provided, the numbers of mentees completed our mentoring programs, the number of internships we've helped to facilitate or job placements opportunities we've helped broker, but for us, perhaps the most meaningful metric we'd cite is the number of lives we've touched and changed.

Interviewees disclaimer:
The views expressed herein are entirely my own and does not reflect the position of my employer bank the Federal Reserve Bank of Richmond, the Board of Governors of the Federal Reserve System, or the Federal Reserve System in general.