
# Cybersecurity & Diversity

Dr. Kevin Harris

# Presentation

- Intro
- Tech Sector
- Global Cybersecurity shortage
- 2019 Breaches
- Diversity as a way to increase pipeline
- How organizations can assist
- Input

# Background

- Roles – Support, Infrastructure, DBA, Networking, System Analyst, CIO
- Industries – Government, Not for Profit, Higher Ed, Private, Consulting
- Academic - Information Security, Cybersecurity, Networking, Forensics

# Techs Impact

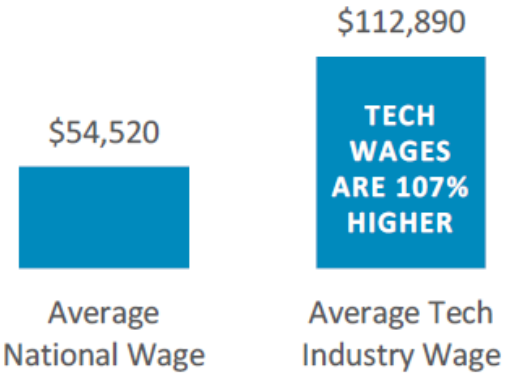
## ECONOMIC IMPACT

**9.2%**

Estimated direct contribution of the tech sector to the U.S. economy: $1.6 trillion

Primary data sources: EMSI | U.S. Bureau of Labor Statistics | U.S. Bureau of Economic Analysis | Burning Glass Technologies Labor Insights. All data are estimates covering the 2017 time period, unless specified as earlier | See Appendix for full methodology and data tables

## TECH INDUSTRY WAGES





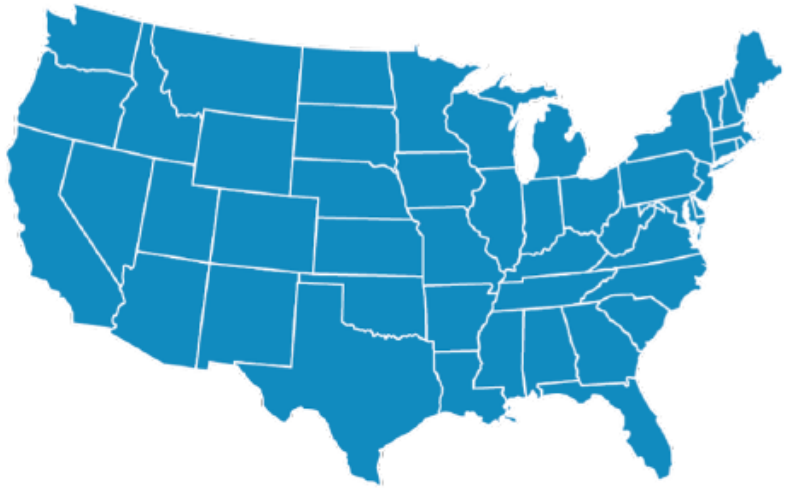
 

# US Tech Sector

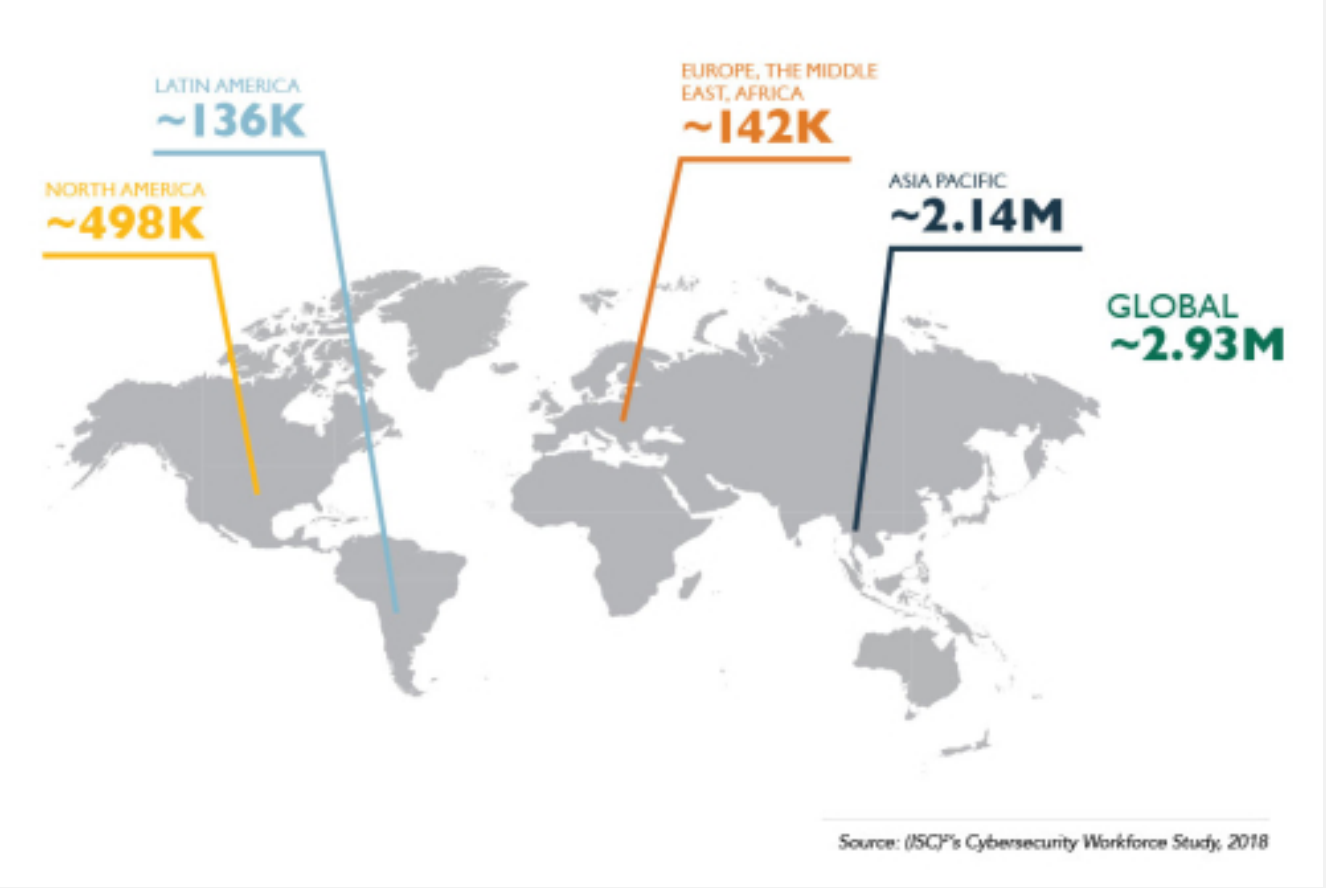
## United States

### STATE OF TECHNOLOGY SUMMARY

| | |
|---|---|
| 11,504,000 | NET TECH EMPLOYMENT[1] |
| 194,000 | NET TECH JOB GAINS [2017 vs. 2016] |
| 7.2% | NET EMPLOYMENT AS A % OF OVERALL WORKFORCE |
| 502,989 | TECH BUSINESS ESTABLISHMENTS [firms with payroll] |
| 2,835,250 | TECH OCCUPATION JOB POSTINGS [2017 total] |
| 27.0% | EMERGING TECH JOB POSTINGS % CHANGE [2017 vs. 2016] |



# Global Cybersecurity Shortage




CYBERSECURITY SKILLS SHORTAGE SOARS, NEARING 3 MILLION

# Breaches (Identity Force)

- **Blur**
- **January 2, 2019:** It didn't take long for the first major breach announcement of 2019. Blur announced a breachafter an unsecured server exposed a file containing 2.4 million user names, email addresses, password hints, IP addresses, and encrypted passwords. The password management company urged their users to change their Blur login credentials and enable two-factor authentication

- **DiscountMugs.com**
- **January 4, 2019:** Online retailer of custom mugs and apparel, DiscountMugs.com was hacked for a four-month period in the latter half of 2018. The company announced that it had discovered malicious card skimming code placed on its payment website. Hackers were able to steal full payment card details (number, security code, and expiration date), names, addresses, phone numbers, email addresses, and postal codes.

- **Alaska Department of Health & Social Services (DHSS)**
- **January 23, 2019:** A cyberattack targeting Alaska's Division of Public Assistance has exposed data on at least 100,000 people. The attacker was able to access the names, Social Security numbers, dates of birth, addresses, health information, and income of people who applied for government programs.

- **Critical Care, Pulmonary & Sleep Associates (CCPSA)**
- **January 31, 2019:** Patients of the Colorado-based healthcare facility had their personal health information exposed after CCPSA employees fell for a phishing attack. Approximately 23,000 people have been notified of the breach, which included names, medical information, dates of birth, addresses, Social Security numbers, and driver's licenses

- **UW Medicine**
- **February 20, 2019:** Nearly 1 million patients have been notified of a UW Medicine data breach, which was discovered December 26, 2018. A vulnerability on the health network's website server exposed protected health information including names, medical record numbers, and a description of each individual's information

- **Georgia Tech**
- **April 2, 2019:** Personal information of current and former faculty, students, staff and student applicants of Georgia Tech were accessed by a hacker through a central database. The database affected by the breach includes names, addresses, Social Security Numbers and birth dates of 1.3 million individuals. This is the university's second breach in less than a year.

- **U.S. Customs and Border Protection**
- **June 10, 2019:** Images of travelers' faces and license plates were compromised in a cyberattack on a contractor for U.S. Customs and Border Protection. The agency said that fewer than 100,000 people were impacted while entering and exiting a border entry point.

- **Dealer Leader, LLC.**
- **September 16, 2019:** The personal information of 198 million protective car buyers was left exposed in an unsecured database belonging to Dealer Leader, a digital marketing company for car dealerships. The information exposed included names, email addresses, phone numbers, home addresses and IP addresses.

# Diversity as means to increase the pipeline to the cyber field.

# Women

- The 2019 (ISC)² Cybersecurity Workforce Study: Women in Cybersecurity found that women are still underrepresented in the field.  Using a more inclusive methodology to define cybersecurity professionals, the survey concluded that the number of women in the field is now 24% (as opposed to the previous number of 11%).
- The problem is anticipated to grow. “Employment of information security analysts is projected to grow 28 percent from 2016 to 2026, much faster than the average for all occupations,”

# Minorities in Cybersecurity

- In the U.S. cybersecurity industry
  - 9% of workers self-identified as African American or Black
  - 8% as Asian
  - 4% as Hispanic
  - 4% self-identifying as “Other.”
  - 1% as American Indian or Alaskan Native and Native Hawaiian/Pacific Islander,

# Impacts of limited women/minorities

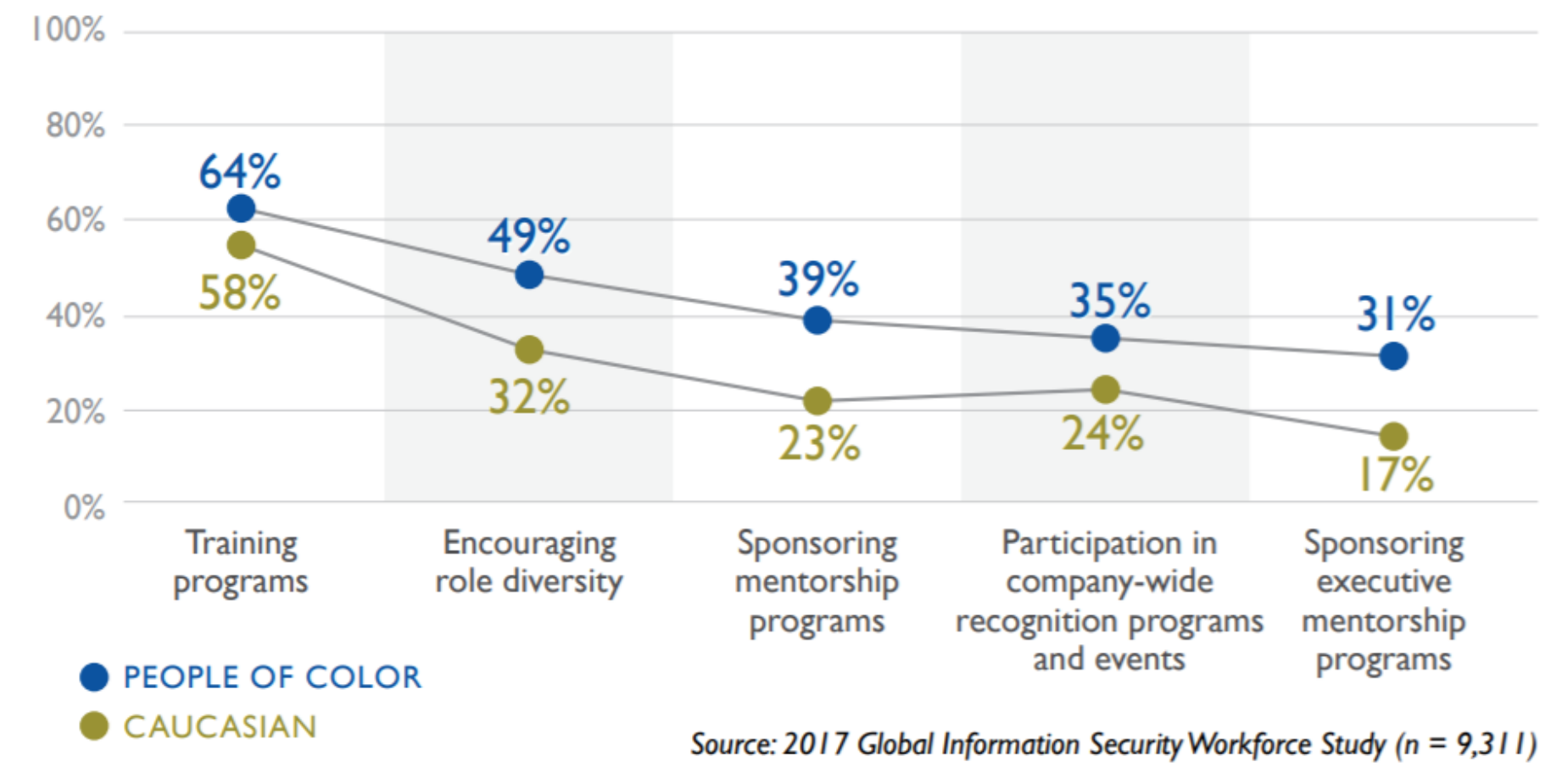
- Fewer workers available to protect vital digital assets
- Introduction on unintentional biases in AI
- Global interactions require diversity
- Group think
- Recruitment
- Legislation (GDPR/CCPA)

# Other Areas of focus

- Rural locations
- Veterans
- Disabilities

# How organizations can help

# Views of program importance's



# Academic Programs

- Diversity in Students & Faculty Members
- Various types of programs
  - Highly technical
  - Managerial
  - Breadth of knowledge
- Programs at Minority Serving Institutions
  - Stillman University Cybercore
  - HBCU/Hispanic Serving Institution


# Business Community Support

- Training Programs for leadership
- Board level
- Ethical implications
- Awareness

# Questions
# &
# Collaboration

# Reasons women and minorities may not pursue cyber fields

# Ideas to encourage women and minorities to pursue cyber fields

# Thank You!

Dr. Kevin Harris
American Public University Systems
Cybersecurity Program Director
kharris@apus.edu
Twitter: @KevinHarrisTech
Linkedin: https://www.linkedin.com/in/harris-kevin/

# Resources

- https://www.identityforce.com/blog/2019-data-breaches
- https://fcw.com/articles/2019/05/02/cyber-trump-exec-order.aspx
- https://sera-brynn.com/cybersecuritys-3-million-person-workforce-shortage-is-now-a-risk-management-problem/
- https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx
- https://blog.isc2.org/isc2_blog/2018/10/cybersecurity-skills-shortage-soars-nearing-3-million.html