7-15-2019

Securing the Human: Broadening Diversity in Cybersecurity

Mohammad Azhar

Sajal Bhatia
Sared Heart University

Greg Gagne

Chadi Kari

Joseph Maguire

See next page for additional authors

Recommended Citation

Azhar, M., Bhatia, S., Gagne, G., Kari, C., Maguire, J., Mountrouidou, X., Tudor, L., Vosen, D.& Yuen, T. T. (2019). Securing the human: Broadening diversity in cybersecurity. Proceedings from *2019 ACM Conference on Innovation and Technology in Computer Science Education.* Scotland: Aberdeen. July 15. Doi: 10.1145/3304221.3325537

Securing the Human: Broadening Diversity in Cybersecurity

Mohammad Azhar
Borough Of Manhattan Community College
United States
MAZHAR@bmcc.cuny.edu

Sajal Bhatia
Sacred Heart University
United States
bhatias@sacredheart.edu

Greg Gagne
Westminster College
United States
ggagne@westminstercollege.edu

Chadi Kari*
University of the Pacific
United States
celkari@pacific.edu

Joseph Maguire
University of Glasgow
United Kingdom
Joseph.Maguire@glasgow.ac.uk

Xenia Mountrouidou†
College of Charleston
United States
mountrouidoux@cofc.edu

Liviana Tudor
Politehnica University of Bucharest, Petroleum-Gas University of Ploiesti
Romania
liviana.tudor@cs.pub.ro

David Vosen‡
College of St. Scholastica
United States
DVosen@css.edu

Timothy T. Yuen
The University of Texas at San Antonio
United States
Timothy.Yuen@utsa.edu

ABSTRACT

Recent global demand for cybersecurity professionals is promising, with the U.S. job growth rate at 28%, three times the national average [1]. Lacking qualified applicants, many organizations struggle to fill open positions [2]. In a global survey, 2,300 security managers reported that 59% of their security positions were unfilled, although 82% anticipated cyberattacks to their systems [3]. At the same time, the cybersecurity field is broadening, not only in technical concepts but also in human factors, business processes, and international law. The field has not become culturally diversified, however. Professionals hired in 2018 included only 24.9% women, 12.3% African Americans, and 6.8% Latinos [4]. These facts create an opportunity for higher education: diversify the profession while increasing the numbers of skilled computer scientists. New and integrated methods of attracting student populations in the field of cybersecurity are needed. The working group goal is to evaluate the effectiveness of approaches used in higher education to diversify the cybersecurity field through literature review, analysis of the findings, and a survey on techniques used for diversification of the cybersecurity field.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Social aspects of security and privacy**; • **Social and professional topics → Computing education**;

KEYWORDS

Cybersecurity; Diversification; Education

ACM Reference format:
Mohammad Azhar, Sajal Bhatia, Greg Gagne, Chadi Kari, Joseph Maguire, Xenia Mountrouidou, Liviana Tudor, David Vosen, and Timothy T. Yuen. 2019. Securing the Human: Broadening Diversity in Cybersecurity. In *Proceedings of Innovation and Technology in Computer Science Education, Aberdeen, Scotland, UK, July 15–17, 2019 (ITiCSE '19),* 2 pages.
https://doi.org/10.1145/3304221.3325537

1 INTRODUCTION

Data breaches, social engineering, and cybercrime are continuously escalating [5]. Furthermore, pervasive adoption of the Internet of Things (IoT) smart devices, cloud storage, and mobile technologies expand into every economic sector and compound these security flaws by increasing the attack surface [6]. Thus, cybersecurity is no longer just about data and technology; it is about life and property with the the annual cost of global cybercrime is now estimated to be 600 billion USD, up more than a 100 billion from four years ago [5].

Global job demands for cybersecurity professionals reveals a long term workforce gap with a 3.5 million deficit of workers predicted by 2021 [2]. However, current Computer Science (CS) and Cybersecurity education programs neither are able to meet the demand nor provide the modern empirical training techniques needed especially in information technology security areas of social engineering, spear phishing, and ransomware attacks. Several questions arise for CS educators, industry, and governmental sectors: how effective is cybersecurity education if the knowledge is siloed or only expanded to CS majors? How effective are the solutions that are

*Working Group co-leader.
†Working Group leader.
‡Working Group co-leader.

ITiCSE '19, July 15–17, 2019, Aberdeen, Scotland, UK

ACM ISBN 978-1-4503-6301-3/19/07.
https://doi.org/10.1145/3304221.3325537

given by a non-diverse population of CS students that constitute the majority of cybersecurity professionals? Diversification of global security threats demands a diversification in the student population and educational approaches in computer science education. Our working group will address these issues regarding diversification of the cybersecurity field through analysis and evaluation of existing techniques.

2 WORKING GROUP OBJECTIVES

This working group will build upon ITiCSE cybersecurity endeavors from 2010, 2011, and 2018 [7, 8, 9] in expanding cybersecurity development to engage diverse undergraduate programs and interest. The goals of this working group are to:

(1) A detailed literature review of current methods used to attract additional students in the field, such as general education, gamification, active learning, pre-college education, conferences, summer camps, and peer instruction.
(2) An analysis of outcomes of these active learning techniques.
(3) A survey for educators that explores their formal and informal methods for diversifying the field of cybersecurity.
(4) An exploratory analysis of the interdisciplinary cybersecurity studies and the connection to the Internet of Things (IoT) systems. Smart devices are of interest regarding privacy implications and education opportunities that they may offer, such as hands on projects and experimentation [10].

The group will explore these issues in cybersecurity through a global perspective, investigating the approaches to, challenges of, and issues in broadening diversity around the world.

3 ACKNOWLEDGMENTS

The team acknowledges support provided by the US National Science Foundation under Award No. DUE-1700254. The team also acknowledges the support of ACM.

REFERENCES

[1] Bureau of Labor Statistics. 2019. *Occupational Outlook Handbook, Bureau of Labor Statistics.* https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.
[2] Steve Morgan. 2017. *Cybersecurity jobs report 2018-2021.* https://cybersecurityventures.com/jobs/.
[3] ISACA. 2018. *State Of Cybersecurity Study: Security Budgets Increasing, But Qualified Cybertalent Remains Hard To Find.* http://www.isaca.org/About-ISACA/Press-room/News-Releases/2018/Pages/State-of-Cybersecurity-Study-Security-Budgets-Increasing-But-Qualified-Cybertalent-Remains-Hard-to-Find.aspx.
[4] Bureau of Labor Statistics. 2019. *Labor Force Statistics from the current population survey, Bureau of Labor Statistics.* https://www.bls.gov/cps/cpsaat11.htm.
[5] James Lewis. 2018. *Economic Impact of Cybercrime, No Slowing Down.* McAfee. https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf.
[6] Michael J Covington and Rush Carskadden. 2013. Threat implications of the internet of things. In *2013 5th International Conference on Cyber Conflict (CYCON 2013).* IEEE, 1–12.
[7] Stephen Cooper, Christine Nickell, Lance C. Pérez, Brenda Oldfield, Joel Brynielsson, As Gencer Gökce, Elizabeth K. Hawthorne, Karl J. Klee, Andrea Lawrence, and Susanne Wetzel. 2010. Towards information assurance (ia) curricular guidelines. In *Proceedings of the 2010 ITiCSE Working Group Reports* (ITiCSE-WGR '10). ACM, Ankara, Turkey, 49–64. ISBN: 978-1-4503-0677-5. DOI: 10.1145/1971681.1971686. http://doi.acm.org/10.1145/1971681.1971686.
[8] Lance C. Pérez, Stephen Cooper, Elizabeth K. Hawthorne, Susanne Wetzel, Joel Brynielsson, Asim Gencer Gökce, John Impagliazzo, Youry Khmelevsky, Karl Klee, Margaret Leary, Amelia Philips, Norbert Pohlmann, Blair Taylor, and Shambhu Upadhyaya. 2011. Information assurance education in two- and four-year institutions. In *Proceedings of the 16th Annual Conference Reports on Innovation and Technology in Computer Science Education - Working Group Reports* (ITiCSE-WGR '11). ACM, Darmstadt, Germany, 39–53. ISBN: 978-1-4503-1122-9. DOI: 10.1145/2078856.2078860. http://doi.acm.org/10.1145/2078856.2078860.
[9] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (ITiCSE 2018 Companion). ACM, Larnaca, Cyprus, 36–54. ISBN: 978-1-4503-6223-8. DOI: 10.1145/3293881.3295778. http://doi.acm.org/10.1145/3293881.3295778.
[10] Barry Burd, Lecia Barker, Felix Armando Fermin Perez, Ingrid Russell, Bill Siever, Nicoleta Tudor, Michael McCarthy, and Ian Pollock. 2018. The internet of things in undergraduate computer and information science education: exploring curricula and pedagogy. In *2018 ITiCSE Working Group Reports.* ACM. (November 2018).