CS4A: A New Approach for Cybersecurity Workforce Development

Yong Wang
Beacom College of Computer and Cyber Sciences
Dakota State University
Madison, SD
yong.wang@dsu.edu

Abstract

The paper proposes a new approach, Cybersecurity for All (CS4A), to resolve the cybersecurity workforce shortage challenge. CS4A aims to establish new pathways for nontraditional computer and information sciences and lifelong learners to become cybersecurity professionals through continuing education. CS4A addresses the challenge in three steps: identify cybersecurity skills needed to succeed in cybersecurity, create cybersecurity skill stacks to establish pathways to cybersecurity career, and develop flexible and accessible cybersecurity programs for people of all ages. In addition to the current endeavors from government, academia, and industry, CS4A reaches, recruits, and prepares a new talent pool of candidates for cybersecurity workforce and thus help resolve the cybersecurity workforce shortage challenge.

I. Introduction

The cyber threat landscape has changed over in the last 20 years. Cyberattacks are surging and becoming more organized and structured. The technology and tactics used by cyber criminals also become more complicated. The sophistication has outpaced the ability of IT and security professionals to address the threats (Cisco 2015). As a result, data breaches are getting bigger. In a recent data breach in Equifax in 2017, 143 million Americans' sensitive personal information was exposed (FTC 2017). Cybersecurity is a national priority (The White House 2017). However, finding qualified people to help drive successful cybersecurity programs has become a nontrivial task. Cybersecurity skills shortage has become a top challenge for organizations in the world (Suby & Dickson 2015). The 2017 Global Information Workforce Study estimates that the cybersecurity workforce gap will reach 1.8 million by 2022 (Center for Cyber Safety and Education 2017). While government, academia, and industry have worked together to address the cybersecurity skills shortage, it is apparent that more efforts are needed to fill the gap as the data reveals that the cybersecurity skills gap is getting worse (Oltsik 2017).

This paper propose a new approach, Cybersecurity for All (CS4A), to resolve the cybersecurity workforce shortage. An overview of the approach is shown in Figure 1. CS4A aims to establish new pathways for nontraditional computer and information sciences and lifelong learners to become cybersecurity professionals through continuing education.

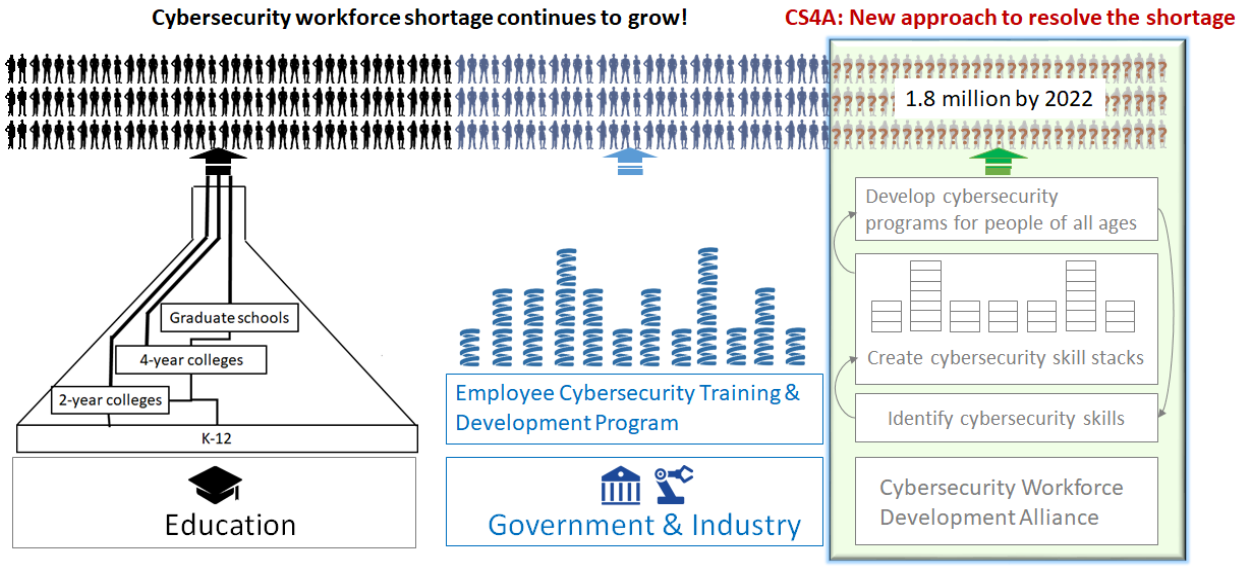

Figure 1. CS4A Overview

II. CS4A: A New Approach for Cybersecurity Workforce Development

A. CS4A Overview

Many initiatives have been put in place to develop cybersecurity workforce. Higher education are adapting curriculums to support cybersecurity program needs. Colleges are taking actions to partner with K-12 and post-secondary schools to engage more students in cybersecurity education. Extra efforts are also being made to attract minority students (e.g., women students) to cybersecurity (A Frost & Sullivan White Paper 2017). In private sectors, many companies and organizations have developed their own on-the-job training programs to train employees to meet their needs in cybersecurity. These endeavors are clearly important and will continue to help build cybersecurity workforce. However, they are far more than enough (Oltsik 2017).

In addition to the traditional academic programs and on-the-job training, the paper proposes a new approach, Cybersecurity for All (CS4A), for cybersecurity workforce development. CS4A targets to a new pool of candidates who are nontraditional computer and information sciences

and lifelong learners. These learners will be most likely declined from any academic cybersecurity programs due to lack of required background. Their daily jobs typically do not involve any cybersecurity duties and will not be able to participate in any on-the-job cybersecurity training. However, they would like to develop their cybersecurity skills through continuing education and prepare them for cybersecurity career in the future. CS4A aims to help this new pool of candidates and help them develop the desired cybersecurity skills. CS4A achieves the goal in three steps: i) identify cybersecurity skills needed to succeed in cybersecurity, create cybersecurity skill stacks to establish pathways to cybersecurity career, and develop flexible and accessible cybersecurity programs for people of all ages.

B. Identify Cybersecurity Skills

The fast changing and sophisticated attacks indicate that the cybersecurity skills needed to prevent those attacks must also be adapted over time. In addition to the skills taught in computer and information sciences, skills such as data analysis and an understanding of risks are also important. To address the cybersecurity skills shortage, it is important to clearly identify what cybersecurity skills are needed to succeed in cybersecurity. This is an important issue for all parties including government, academia, and industry. The paper proposes to form a Cybersecurity Workforce Development Alliance (CSWDA) to lead the efforts. The Alliance includes companies and organizations from both the public and the private sectors.

C. Create Cybersecurity Skill Stacks

Based on the cybersecurity skills identified, the Alliance will create cybersecurity skill stacks which will establish pathways leading to cybersecurity career. Cyberseek (www.cyberseek.org) divides cybersecurity career into three levels: entry-level, mid-level, and advanced-level. The common cybersecurity feeder roles which lead to cybersecurity career includes networking, software development, system engineering, financial and risk analysis, and security intelligence. The cybersecurity skill stacks will establish new pathways for participants to become one of feeder roles as identified by Cyberseek.

The cybersecurity skill stacks will be based on the cybersecurity skills identified in Section II.B. Each stack specifies prerequisite skills required, skills to be developed, and the career path which it may lead to. The cybersecurity skill stacks could be cascaded together horizontally and

vertically. The stacks cascaded horizontally aim to help participants to extend breadth of skills in cybersecurity. The stacks cascaded vertically aim to help participants to develop cybersecurity skills in depth. The stacks will be modulated and can be grouped together based on needs. Certificates can be created for stacks as incentives to participants.

D. Develop Cybersecurity Programs for People of All Ages

Most of the current endeavors of cybersecurity workforce development programs are closed loop. The academic cybersecurity programs are very competitive and selective. Companies and organizations develop training programs to meet their own needs. These programs are generally not available for public. To resolve the cybersecurity workforce shortage challenge, we need to target to a much larger pool of candidates and prepare them to become cybersecurity professionals. CS4A targets a new pool of candidates which are nontraditional computer and information science and lifelong learners. New programs will be developed based on the cybersecurity skill stacks. These programs will be accessible to these learners and also flexible for participants. These new programs may include online programs, vocational schools, certificate programs, etc. The new programs can be sustained with the support from government agencies, academia, and industry.

III. Summary

This paper proposes a new approach, CS4A, to resolve the cybersecurity workforce shortage challenge. Unlike the academic cybersecurity programs and the on-the-job training, CS4A targets to a new pool of talent candidates which are nontraditional computer and information sciences and lifelong learners. CS4A creates new pathways for these leaners to become cybersecurity professionals and thus help resolve the cybersecurity workforce shortage challenge. CS4A can also be used as training programs for students in colleges and continuous training programs for cyber professionals.

References

A Frost & Sullivan White Paper, 2017. *The 2017 Global Information Security Workforce Study : Women in Cybersecurity*, Available at: https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf.

Center for Cyber Safety and Education, 2017. The 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk. *Frost & Sullivan in partnership with Booz Allen Hamilton for ISC2*.

Cisco, 2015. *The Internet of Things : Reduce Security Risks with Automated Policies*, Available at: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/security-risks.pdf.

FTC, 2017. The Equifax Data Breach. Available at: https://www.ftc.gov/equifax-data-breach.

Oltsik, J., 2017. The Life and Times of Cybersecurity Professionals: A Cooperative Research Project by ESG and ISSA. , (November), p.9. Available at: http://www.esg-global.com/.

Suby, M. & Dickson, F., 2015. *The 2015 (ISC)2 Global Information Security Workforce Study*, Available at: http://www.csoonline.com/article/2922381/infosec-careers/confronting-the-widening-infosec-skills-gap.html.

The White House, 2017. President Trump Protects America's Cyber Infrastructure.

Dr. Yong Wang is an Associate Professor in the Beacom College of Computer and Cyber Sciences at Dakota State University. He received his B.S. and M.S.E degrees in Computer Science from Wuhan University (China) in 1995 and 1998, respectively. He received his Ph.D. degree in Computer Science from University of Nebraska-Lincoln in 2007. Before he joined DSU in 2012, he had spent 10 years in telecommunication industry as a senior software engineer and a team leader. His research focuses on network security and privacy issues. His current research projects include mobile, cloud, IoT, and big data. He has published 50+ peer-reviewed papers in prestigious journals/conferences. He is a co-author of three books. He also severs as Technical Program Committee (TPC) members and reviewers for many international conferences in Computer Science. Dr. Wang received four awards from National Science Foundation between 2012 and 2017. He is currently leading the NSF CyberTraining project at DSU.