Chapter 9
Opinions of the Software and Supply Chain Assurance Forum on Education, Training, and Certifications

Beatrix Boyens
Adaptive Management Concepts, USA

ABSTRACT

This article provides an overview of discussions held at the Software and Supply Chain Assurance (SSCA) forum held May 1-2, 2018, in McLean, Virginia. The two-day event focused on education and training for software assurance (SwA) and Cyber-Supply Chain Risk Management (C-SCRM). Attendees discussed questions such as "What are some challenges facing industry, academia, and government organizations in this area?" "Who needs education or training?" "What needs to be taught?" and "What strategies do or do not work?" Discussions related to the current environment, hiring and retaining qualified employees, defining roles and responsibilities, and the knowledge, skills, and abilities (KSAs) that are most in-demand.

1. INTRODUCTION

On May 1-2, 2018, 118 persons representing industry (64), government (45), and academia (12)[1] gathered in McLean, Virginia, to discuss education, training, and certifications for software assurance (SwA) and Cyber-Supply Chain Risk Management (C-SCRM). Because the events are held under Chatham House rule (Chatham House, N.D.), no attributions are made in this paper.

The event was part of a regular series titled the Software and Supply Chain Assurance (SSCA) Forums, held 2-3 times/year, as a venue for participants from around the world to learn about and discuss software and supply chain risks, mitigation strategies, tools, and any gaps related to the people, processes, or technologies involved. These forums are co-led by the U.S. National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Department of Defense (DoD),

DOI: 10.4018/978-1-6684-3554-0.ch009

and the Government Services Agency (GSA). The Software Engineering Institute based in Pittsburgh, Pennsylvania, helped co-lead the May 2018 event.

The goal of the event was to identify what knowledge, skills, and abilities (KSAs) should be taught in formal education and training programs and relevant opportunities or roadblocks. This paper contains an overview of the event to provide information useful for the design or use of education, training, or certifications, as well as to provide insight into the opinions of SwA and C-SCRM experts. Portions of the event which did not directly tie into education and training, while valuable, are out of scope of this paper. This paper is intended to provide an overview of the discussions from the forum; any opinions, recommendations, or suggestions included in this paper are based on attendees' comments and do not necessarily reflect the opinions of the authors or the sponsoring organizations.

2. BACKGROUND

The Online Trust Alliance (2018) found that the number of cybersecurity incidents doubled from 82,000 in 2016 to nearly 160,000 in 2017. Many of these incidents highlighted risks associated with software and/or supply chain management. High-profile incidents have helped highlight the importance of software assurance (SwA) and cyber-supply chain risk management (C-SCRM).

For this paper, C-SCRM is loosely defined as a discipline located at the intersection of supply chain management and cybersecurity. It covers the entire life cycle of information or operations technology (IT/OT) and often overlaps or includes disciplines like third-party risk management, logistics, and quality control. SwA is a closely related, more focused, and mature discipline concentrated on ensuring a level of confidence that software is free from vulnerabilities. Cybersecurity generally denotes the protection of technologies and processes related to the creation, transmission, modification, analysis, and control of data or information. For the purposes of this paper, the term cybersecurity is inclusive of C-SCRM and SwA.

Along with the steady increase of cybersecurity-related incidents, there has been steady growth in the reported cybersecurity skills gap. In 2015, it was estimated that there would be a global shortage of 1.5 million workers by 2020; in 2017, the shortage estimate increased to 1.8 million by 2022 (Frost & Sullivan, 2017, p. 3). Specializations such as SwA and C-SCRM have an even greater shortage. A study by Burning Glass Technologies (2015) found that cybersecurity-related job postings increased 91 percent from 2010 to 2014 (p.3) and that hybrid jobs (such as cyber-supply chain risk management) took roughly 17 percent longer to fill than other cybersecurity job openings (p. 11). The main reasons for the shortage were reported as qualified personnel were difficult to find and job requirements were not understood by leadership (Frost & Sullivan, 2017, p. 4).

3. WHY THERE IS A SWA/C-SCRM PROBLEM

More than one attendee commented that software has evolved significantly since the 1960s. According to one participant, the Orange Book, one of the first cybersecurity guidelines, never looked at software. Software was viewed as simple logic that was added on to hardware. Today, software is ubiquitous. As a result, society is moving from an area of information-only risk to more severe impacts, including direct physical harm to people.