Guest Editorial Preface

Special Issue of Education and Training for Cybersecurity and Supply Chain Risk Management (SCRM)

Carol Woody, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, USA

Cybersecurity and supply chain risk management (SCRM) have not, until recently, been critical concerns for system acquisition and engineering. There is growing awareness that many of the cyber security threats and vulnerabilities we see regularly occurring these days stem from weak cybersecurity practices in acquisition engineering, poor third-party product selection, and insufficient supply chain risk management practices. Systems and products are no longer built for purpose and infrequently implemented in an isolated environment. Instead systems are assembled from a wide range of available hardware and software components such as commercial hardware, open source software, reused legacy components, and commercial off the shelf (COTS) products.

Acquisition and engineering can no longer assume that finely crafted requirements will fully define a delivered product. Nor can they assume that attention to internal system functionality and security controls will establish sufficient operational protection for a highly connected environment. Unfortunately, addressing these growing areas of concern requires specialized knowledge about the ways in which systems and products can be compromised and the potential impact such a compromise can have on operational performance.

There is a noticeable gap in the current acquisition and engineering workforce's knowledge and skills and support resources with the right capabilities are brought in too late, if at all, to help address these challenges. Expanding the knowledge of decision makers and participants in system acquisition and engineering is a critical component in changing this situation, but how can we best prepare them for effectively addressing cyber security and SCRM in the jobs that they already perform? What they need to know and how they should go about learning remains unclear. In addition, how will they demonstrate that they have mastered these new capabilities?

This issue contains four articles that describe various efforts underway to address these challenges. Each show promise in making a contribution to improving the current state of the practice. First, Beatrix Boyens in her paper, "Opinions of the Software and Supply chain Assurance Forum on Education, Training, and Certifications" reports discussions with industry, academia, and government on efforts to clarify what knowledge is needed, who should have it, and how should they obtain it to better address today's cybersecurity and SCRM challenges. The second paper from David A. Bird and John Curry shares efforts underway in the UK to establish cybersecurity as a profession based on a knowledge framework that must span many existing silos in learning and development. The third paper "The Need for Higher Education in Cyber Supply Chain Security and Hardware Assurance" from Brian Cohen and colleagues describes why current academic programs teaching supply chain risk management need to focus more extensively on cyber aspects that emphasize hardware assurance. In the final paper, "Enhancing a SCRM Curriculum with Cybersecurity" from Art Conklin and Chris Bronk, the steps taken to incorporate cybersecurity exemplars into an existing supply chain education program are described.

Carol Woody
Guest Editor
IJSSSP