Chapter 59
The Need for Higher Education in Cyber Supply Chain Security and Hardware Assurance

Brian Cohen
Institute for Defense Analyses, Alexandria, USA

Michelle G. Albert
Institute for Defense Analyses, Alexandria, USA

Elizabeth A. McDaniel
Institute for Defense Analyses, Alexandria, USA

ABSTRACT

Higher education curricula, specialized degrees, and certificate programs related to cybersecurity are proliferating in response to student demand; faculty interest and expertise; employer demand; government and industry standards and funding; and the expectations of specialized, state, or regional accrediting agencies. These expanding academic programs, however, do not adequately address supply chain threats that affect national security. The authors assert that cyber supply chain risk management (C-SCRM), with a focus on hardware assurance, should be considered a critical aspect of cybersecurity and be included in higher education curricula to prepare the future cyber workforce to face challenges related to supply chain security and hardware assurance.

1. INTRODUCTION

The U.S. government, the nation's critical infrastructure sectors, and industry are increasingly dependent on commercially designed and manufactured components for cyber-physical systems, which are "engineered systems that are built from, and depend on, the seamless integration of computation and physical components" (National Science Foundation [NSF], n.d.). Risks to the supply chains of these components pose a national security threat and can render these systems vulnerable to manipulation

DOI: 10.4018/978-1-7998-2466-4.ch059

or exploitation. These supply chains comprise interconnected webs of people, processes, technology, information, and resources spread around the world. Their complexity provides opportunities for malicious actors to tamper with components or steal information and poses security risks to the performance, integrity, and safety of the hardware components inserted in our systems and networks. To address these risks, the cybersecurity workforce must be well-educated in the latest practices, processes, and technologies related to the cybersecurity aspects of supply chain risk management (SCRM), specifically hardware assurance. Hardware assurance refers to the level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, whether intentionally or unintentionally designed or inserted as part of the system's hardware and/or embedded software and/or intellectual property throughout its life cycle (Defense Acquisition University, 2017).

In 2018 the National Institute for Standards and Technology (NIST) coined the term cyber supply chain risk management (C-SCRM), defined as "the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of [information and operational technology] IT/OT product and service supply chains" (NIST, n.d.). The authors use and endorse the C-SCRM term; however, SCRM is used in some places in the paper when citing earlier work.

2. BACKGROUND: RELATED POLICIES AND GUIDANCE

Efforts to manage the risks associated with the cyber supply chain began in earnest with the Comprehensive National Security Initiative (CNCI), which was launched in 2008 when President George W. Bush signed National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), Cybersecurity Policy (The White House, 2008b). President Barack Obama determined that CNCI and its associated activities should evolve to become key elements of a broader, united national security strategy (The White House, 2008a).

CNCI Initiative #11 ("Develop a multi-pronged approach for global supply chain risk management") states that risks from both the domestic and global supply chains must be managed over the life cycle of a cyber-enabled component. The purpose of this initiative was to enhance the U.S. government's skills, policies, and processes to provide departments and agencies with a robust toolset to manage and mitigate supply chain risk levels commensurate with the criticality of, and risks to, the government's systems and networks (CNCI, 2008). Although CNCI's sunset provisions caused it to expire in 2013, its key elements continue.

The Committee on National Security Systems (CNSS) is responsible for the protection of national security systems belonging to the Department of Defense (DoD), the Intelligence Community, and other government agencies. CNSS's goals support CNCI and NSPD-54/HSPD-23. CNSS Directive 505, *Supply Chain Risk Management*, was published in 2012 in accordance with CNCI Initiative #11. It states that the U.S. Government must address the reality that the global marketplace provides increased opportunities for adversaries to penetrate supply chains by establishing an organizational capability to identify and manage supply chain risk to national security systems. Risks must be assessed early and throughout the acquisition life cycle, and all-source threat information must inform the use of risk mitigations (CNSS, 2017).

In response to CNCI #11 and CNSS Directive 505, NIST published organizational SCRM approaches for the acquisition, development, and operation of information systems and systems of systems. NIST