Chapter 18
Enhancing a SCRM Curriculum With Cybersecurity

Art Conklin
University of Houston, Houston, USA

Chris Bronk
University of Houston, Houston, USA

ABSTRACT

Supply chain-related curricula exist across many universities, with many including risk management as an important or focal element. With the rise of software-driven technology across the supply chain, how can firms manage the inherent risks associated with software as part of a procurement process? This article examines how to provide context appropriate cybersecurity exemplars in a model supply chain education program, bringing to light the issue of embedded risk in software acquisition. Through a series of specifically placed educational elements that provide targeted cybersecurity knowledge to students, the objective is to provide additional skill sets for future supply chain professionals to assist firms in including software related cybersecurity risk as a component in SCRM.

1. INTRODUCTION

In August 2017, Danish shipping conglomerate Møller Maersk reported that it had fallen victim to a catastrophic cyberattack on its enterprise computer systems and network. Months later, in a meeting of the World Economic Forum at Davos, Maersk chairman Jim Hageman Snabe offered gripping details of how the widespread cyber-attack referred to as *notPetya*, impacted the firm. It shut down computer operations at Maersk for at least 10 days at 76 ports around the world, and required remediation covering 45,000 PCs, 4,000 servers and over 2,500 applications (Allen 2018). Total costs associated with this event exceeded $300M US (a figure they cite in lost revenue) and clean-up costs. A similar attack befell Federal Express subsidiary TNT Express. The notPetya attack and its effects on these global logistics firms has cast light on the issues of cybersecurity risk to supply chains (Greenberg, 2018). Supply chain management is not immune to the cybersecurity issues found in other major industry verticals.

DOI: 10.4018/978-1-6684-3554-0.ch018

Supply chains are a ubiquitous attribute of business and their function or disruption can have significant impacts to the goods and services that the firms offer. Professionals in the supply chain field toil to obtain the required elements for business adhering to tight schedules and financial constraints. The field of supply chain risk management acknowledges the potential for disruption in the sourcing of materials, which must be incorporated into the overall business risk of the enterprise. With software now embedded in so many products and information technologies, cybersecurity risk from software must be incorporated into the supply chain risk equation. A significant challenge for the supply chain is how to determine, understand and manage the risk associated with software and information technology elements in the overall supply chain risk management process.

There have been a variety of efforts designed to raise awareness of software risk and supply chain issues with the intent to influence change in business practices (Ellison & Woody, 2010). One practical example is the U.S. Department of Homeland Security's Software Acquisition Working Group guidebook. It focuses on enhancing supply chain risk management throughout the software acquisition and purchasing process (Polydys & Wisseman, 2009). The US National Institute of Standards and Technology (NIST) published several relevant items on the issue of security and the supply chain (Boyens, Paulsen, Moorthy, Bartol, & Shankles, 2014; US National Institute of Standards and Technology (NIST), 2015).

The incorporation of cybersecurity risk into supply chain risk management curricula has ramifications for education and student preparation for careers in the field. The scope of cybersecurity and supply chain is very wide, and for this paper the focus is only on risk associated with software security. This paper examines the use of specific curriculum additions to include key points of software cybersecurity as part of a typical undergraduate program in Supply Chain and Logistics Technology. A series of targeted additions of software cybersecurity knowledge can be added to the curriculum for the purposes of improving understanding of the risks and mitigation methods associated with software security risks. Introducing software related cybersecurity risk into a supply chain education program is not a complete solution to the problem, but over time as more supply chain professionals are educated with an expanded knowledge base, the solutions will be easier to achieve. This is a long term first step in attacking this complex problem. This paper covers a set of points in series: first is an examination of what are the types of risks associated with cybersecurity and supply chain; next the notional curriculum elements of the education program are explained; and last a menu of the learning points and their placement is presented. It is worth noting that the curricular prescriptions offered here, like almost any involving cybersecurity, are a work in progress, and that the level of detail associated with the curriculum changes are still evolving.

Software is commonly a part of many large-scale integrated systems that are managed through an acquisition process focused on the whole as opposed to the individual elements. The approach suggested in this article, aimed at educating supply chain professionals toward cybersecurity risk associated with software applications is not a complete solution for large scale acquisition cybersecurity supply chain risks. It can clearly play a role in the examination of decomposition of specifications and procurement policies, but we are not proposing this as a complete solution to large scale acquisition risk issues.

2. BACKGROUND

The issue of software security and its inherent risk has been understood for a long time (Allen, Barnum, Ellison, McGraw, & Mead, 2008) (Boehm, 1991). Continued reduction in the cost of embedded computing has led to the inclusion of microprocessors and networking into a wide range of devices. The overall