Technovation 34 (2014) 354–361

Contents lists available at ScienceDirect

Technovation

journal homepage: www.elsevier.com/locate/technovation

Cyber supply chain security practices DNA – Filling in the puzzle using a diverse set of disciplines

Nadya Bartol *

Utilities Telecom Council (UTC), 1129 20th St NW, Suite 350, Washington, DC 20036, United States

ARTICLE INFO

Available online 6 February 2014

Keywords:
Supply chain
Cyber supply chain
ICT supply chain
Cyber Supply Chain Risk Management
ICT Supply Chain Risk Management
Multidisciplinary
ISO/IEC 27036

ABSTRACT

This paper describes the journey of the evolving cyber supply chain community towards creating practical and useful standards and best practices. It is based on the author's experience working on the topic since 2006 and contains observations and lessons learned, refined over the years. Cyber supply chain security requires members of several different professional communities to come together including information security, system and software engineering, supply chain and logistics, and process improvement, to name a few. These professional communities have not worked or interacted before and had divergent experiences, vocabularies, frameworks, standards, ways of demonstrating that the practices were performed, and many other things. Over the years these people have learned that many practices that they thought were missing already existed in another discipline and that reinventing them was not necessary. The paper will summarize this journey with the goal of helping those new to this subject matter learn from those who have been working on it for some time.

The paper also describes the current landscape of cyber supply chain standards, including the ones that provide foundational practices that may not be strictly cyber supply chain, those that are truly cyber supply chain, and processes and techniques that can be used in support of cyber supply chain security. The readers of this paper will learn what these emerging efforts have to offer and what is needed to successfully implement the practices that these efforts propose.

1. Introduction and brief history

Cyber supply chain security is an emerging discipline that is still normalizing on its name. A number of terms have been used over the years and are still in use:

- Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM)
- Information and Communication Technology (ICT) supply chain security
- Supply Chain Risk Management
- Cyber supply chain
- Cyber supply chain security
- Cyber Supply Chain Risk Management

While those inside the small but growing community of practitioners understand that these terms are interchangeable, to the outside world those appear to be different things.

The challenge of "what happens when we do not know who, where, when, and how our software or hardware" is created was first identified by the Defense Science Board Task Force in a report on Globalization and Security (Office of the Under Secretary of Defense for Acquisitions and Technology, 1999). Since then multiple US and European governments, consortia, and industry reports have described the problem and proposed actions towards remediation. These included documents by Government Accountability Office (GAO), US Department of Defense (DoD), European Union, European Commission (ENISA, 2009), Software Assurance Forum for Excellence in Code (SAFECode), and other sources (George Mason, 2012; University of Maryland, 2012).

The subject matter received a real boost and attention after it was declared as one of the Comprehensive National Cyber Security initiatives in 2008. Since then the number of government and industry efforts to figure out what to do and how to do it has increased exponentially. After several years of targeted US and international efforts, several standards and best practices have emerged including those from the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), and The Open Group to name a few. Each of these efforts went through roughly a similar journey of brainstorming the scope, figuring out what is included and what is not included, and settling on a set of practices acceptable to all (or at least most) participants.

* Tel.: +1 202 833 6809.
E-mail address: Nadya.bartol@utc.org

0166-4972/$ - see front matter © 2014 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.technovation.2014.01.005

Early efforts adopted two key principles that are in use today:

- Defense-in-breadth is required to manage risks inherent to cyber supply chain. Defense-in-breadth is defined by Committee for National Security Systems Instruction (CNSSI) 4009, *National Information Assurance Glossary* (CNSSI 4009, 2010) as:

  > A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

- System and software lifecycle processes should be used as a foundation for defining cyber supply chain practices. System and software lifecycle processes are described in ISO/IEC 15288:2008, *System and Software Engineering – System Lifecycle Processes* (ISO/IEC 15288:2008), and ISO/IEC 12207:2008, *System and Software Engineering – Software Lifecycle Processes* (ISO/IEC 12207:2008). These should not be confused with a lifecycle: while a lifecycle takes a system or software from beginning to end (e.g., from inception to disposal), lifecycle processes are agnostic to a specific phase of a system or software lifecycle and can be used in any lifecycle phase. For example, configuration management can be used in requirements, design, development, operations, and disposal.

One of the early documents that inspired further efforts was National Defense Industrial Association (NDIA) Guidebook on Engineering for Systems Assurance (NDIA, 2008). The NDIA Guidebook articulated the principles of system assurance and was structured to be consistent with ISO/IEC 15288 and ISO/IEC 12207. The early Cyber Supply Chain practice sets are rooted in the NDIA Guidebook. The same principles were later applied to the development of a multipart standard, ISO/IEC 27036, Information Technology – IT Security Techniques – Information Security for Supplier Relationships.

Another early effort to provide understandable practices for cyber supply chain were two documents produced by SAFECode:

- *Framework for software supply chain integrity* (SAFECode, 2009) that provides a framework and common taxonomy for evaluating software supply chain integrity risks. This framework provides a foundation for the second SAFECode document that provides specific software integrity practices.
- *Software integrity controls, an assurance-based approach to minimizing risks in the software supply chain* (SAFECode, 2010). This document provides specific software integrity controls for a software development organization.

2. Initial practice sets

The individuals working on the early practice sets were either information security/information assurance practitioners (please note, that cyber security as a term did not exist until roughly 2009–2010) or system and software engineering practitioners. As the time went by, they were joined by supply chain and logistics, process improvement, policy, legal, quality, and a number of other professionals each of whom had to get used to different vocabularies and perspectives that the others brought in. The challenge for everyone was that they viewed the potential solutions from their perspective and initially thought that their discipline had some solutions but many practices had to be invented anew.

Fig. 1. Identifying and creating cyber supply chain practices.

The confusion of whether the solution should be developed from the "cyber" or "supply chain" perspective did not help, because practitioners from cyber and supply chain disciplines felt that the problem belonged to them and took some time to absorb the fact that a single discipline was not going to produce a holistic solution. The groups evolved and took at least two years each to normalize around a set of practices that seemed "reasonable" and "appropriate" for the purpose. In those two years the members learned some of the other members' vocabulary and came to understand how the practices from the disciplines that they represented needed to come together to address the particular variant of the challenges we have come to call cyber supply chain, which is basically:

> How do I as an acquirer assure that the hardware or software that I have acquired and installed in my system comes from where it is supposed to have come, in the expected shape and form, will perform as expected, and will not do anything extra it is not supposed to do?

As the groups went along they used similar approaches to evolve to a useful set of practices, depicted in Fig. 1.

The survey and cross-map existing practices was an exhaustive and exhausting effort of mapping anything and everything that was available within the disciplines represented by the participants. For example, one of the early efforts to produce key practices pulled materials from several NIST documents, ISO standards, US government agency documents, and industry papers. The group then mapped all those documents to the NDIA Guidebook, which is based on ISO/IEC 15288:2008 lifecycle processes. Even though the effort included only cybersecurity practitioners, reconciliation was required between proponents of controls vs. processes and US government sources vs. international standards sources. In the process of doing so the group discovered that, for example, configuration management, awareness and training, and a number of other subject matters were addressed slightly differently in multiple sources.

Selecting practices that fit best involved picking through extraordinary amounts of material that appeared to be relevant at first glance. This was useful for helping the groups realize that a lot of practices that were helpful to address the problem were already established and stabilized, such as basic information security, quality, system and software engineering, and supply chain.

This is when the three different ways of doing configuration management were analyzed, mapped, reconciled, and then reduced to what was essential to the problem.

Add what is missing involved figuring out those practices and techniques that have not been already invented by someone and stating them in a way that all of the practitioners from diverse areas of expertise can understand and relate and, most importantly, know what to do when they read that specific text.

3. Current efforts

In late 2009 Department of Defense commissioned a study to identify Standards Development Organizations (SDO) that were developing standards that were relevant to cyber supply chain. The study used liaison relationships of two groups within the umbrella of International Organization for Standardization (ISO) to identify other standards bodies that may be working on the standards relevant to cyber supply chain.