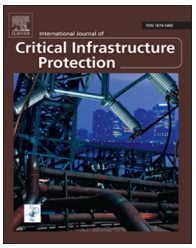
INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip




# Objectives for managing cyber supply chain risk

*Marjorie Windelberg*

*Cyber Pack Ventures, 807 N. Howard Street, #426, Alexandria, Virginia 22304, USA*

ARTICLE INFO

*Article history:*
Received 31 October 2013
Received in revised form
8 November 2015
Accepted 11 November 2015

*Keywords:*
Risk management
Information and communications technology
Hardware
Firmware
Software
Operational technology
Supply chain
Acquisition requirements

ABSTRACT

Cyber-based products and services are acquired through supply chains that typically involve numerous suppliers of hardware, firmware and software components and services sourced globally. When acquisition objectives and their concomitant requirements are not rigorously defined and managed, the cyber-based products and services can pose operational risks to end user organizations and possibly to society if security, reliability and/or safety are compromised, especially in critical infrastructure sectors. However, there is some disagreement about the fundamental objectives of cyber supply chain risk management. Objectives such as trustworthiness, integrity, security and reliability are often noted as key, while safety and other objectives are often omitted. Divergent guidance further compounds the difficulties encountered by an acquiring organization in writing meaningful requirements or policies for managing supply chain risk – whether from products and services, or to the operation of the supply chain, or to sensitive supply chain information. This paper recommends a set of objectives for cyber supply chain risk management and examines the connotations of each objective with the intent to improve risk coverage. It then examines the tradeoffs among the various objectives that acquirers and suppliers make and the trust assumptions that can result in risk exposure. Awareness of the tradeoffs and the degree to which organizations value one objective over another helps clarify their risk tolerance or risk appetite and enables them to apply appropriate management controls.



## 1. Introduction

Cyber-based products and services must be protected from threats and harmful states or consequences, starting with risk originating in or from the supply chain. Minimizing risk fulfills explicit or implicit objectives and requirements of acquirers [5], especially end user organizations that bear the brunt of failures, cyber attacks and maintenance costs such as patching caused by defects and vulnerabilities in supplied products and services. End user organizations in critical infrastructure sectors such as energy, communications, transportation, financial services and emergency services are no exception. They rely extensively on information and communications technology (ICT) and operational technology (OT), including hardware, firmware, software and systems, as well as on services such as installation, maintenance and outsourced, hosted and/or cloud-based computing.

An end user organization acquires cyber products and services from prime suppliers that, in turn, source components or services from other suppliers that have their own suppliers. A supply chain often consists of many tiers of suppliers; a typical acquirer has visibility upstream only into the first-tier supplier or into the first- and second-tier

E-mail address: mwindelberg@cyberpackventures.com

http://dx.doi.org/10.1016/j.ijcip.2015.11.003
1874-5482/

Please cite this article as: M. Windelberg, Objectives for managing cyber supply chain risk, International Journal of Critical Infrastructure Protection (2015), http://dx.doi.org/10.1016/j.ijcip.2015.11.003

suppliers. A complex (and often dynamic) supply chain can comprise vendors that make hardware, firmware or software components, logistics service providers that offer delivery and warehousing services, and distributors, dealers or resellers that handle sales. Software products, once distributed only via media such as CD-ROMs, are now downloaded from websites that typically host services for multiple software developers. The offerings of service suppliers are quite varied. Examples include design, testing, installation, systems integration, maintenance and monitoring services. System integrators, along with providers of hosting and cloud computing services, usually acquire hardware, firmware and software from their own suppliers and may rely on sub-contractors to perform portions of the delivered services. Commercial pressures and the complexity of services can lead to deliberate or inadvertent actions that increase risk.

All the participants in cyber supply chains, including end user organizations, have different understandings of risk management objectives and have varying capabilities for defining requirements and managing supply chain risk. In addition, acquirers and their suppliers have their own risk tolerances and risk appetites. This may push suppliers to make risk tradeoffs in their own interest, but not in the interest of acquirers farther downstream in the supply chain.

This paper presents a framework for understanding the various supply chain risk management objectives for cyber-based products and services. It also illustrates different kinds of tradeoffs made by supply chain participants and possible explanations for the tradeoffs. The next section presents a high-level framework for cyber supply chain risk management objectives. Following this, the connotations of each objective are explored. Finally, tradeoffs among the objectives and the trust assumptions underlying many tradeoffs are discussed.

## 2. Supply chain risk management objectives and framework

The systems engineering disciplines of security, reliability and safety provide a good starting point for a framework for organizing the various supply chain risk management objectives. Reliability is the preferred term instead of the almost equally common term, dependability [2,11]. Quality and trustworthiness are the other major objectives. Each primary objective has a distinct purpose that can be achieved via one or more major methods.

- *Security:*
  - *Purpose:* Maintaining an authorized state of an element and preventing violations of the authorized states; an element denotes a system or one of its hardware, firmware or software components, a service, information or a process.
  - *Primary methods:* Authorization to appropriately interact with a component; controlling access to the component through authorization.
- *Reliability:*
  - *Purpose:* Delivery of services, including services performed by hardware, firmware or software components; if the ability to deliver a service is impaired, a fault occurs and a failure may result.
  - *Primary methods:* Redundancy, diversification, independent components and flexibility.
- *Safety:*
  - *Purpose:* Containment of adverse consequences [21] to the environment, including other components that are interrelated.
  - *Primary methods:* Compliance with specific safety standards such as IEC 61508 [13] or regulations; "design for degraded mode operations, graceful degradation" [12]; diversification or partitioning and independence of components; redundancy; containment when a fault or failure occurs.
- *Quality:*
  - *Purpose:* Conformance to specifications and elimination of defects or errors.
  - *Primary methods:* Assurance techniques, including independent validation and verification testing.
- *Trustworthiness:*
  - *Purpose:* Confidence in the performance or state of something.
  - *Primary methods:* Conformance to standards or good practices; exercising due care and due diligence.

Security and reliability are broad objectives, each composed of more focused objectives. Fig. 1 presents the complete terminology for cyber supply chain risk management objectives within the context of the framework described in this paper.

The framework differs from the canonical information security triad of availability, confidentiality and integrity by placing availability under reliability instead of under security (see also [12]). Other frameworks relate availability to both dependability and security [2,11]. Safety, unlike security and reliability, does not have constituent objectives (see also [11]). Quality and trustworthiness are often used as stand-ins for other objectives. For example, quality is associated with authentic products as opposed to knock-offs or clones, and a reliable supplier or service is considered to be trustworthy.

Other frameworks organize the objectives differently and incorporate less or more terms. Boyens et al. [4] focus on integrity, security, resilience and quality while Bryant [5] identifies safety, reliability, availability, resilience and security as facets of trustworthiness. The largest framework,

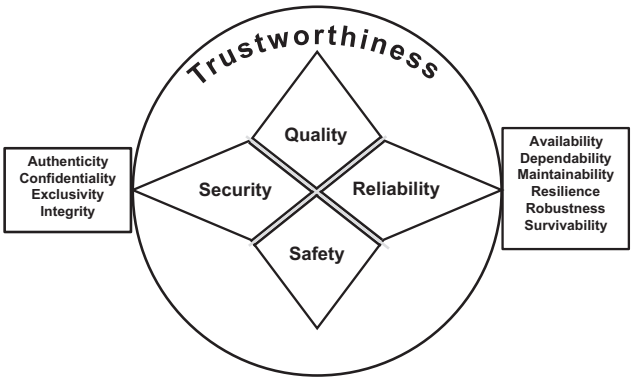



**Fig. 1 – Supply chain risk management objectives.**

Please cite this article as: M. Windelberg, Objectives for managing cyber supply chain risk, International Journal of Critical Infrastructure Protection (2015), http://dx.doi.org/10.1016/j.ijcip.2015.11.003