Technovation 34 (2014) 342–353

Contents lists available at ScienceDirect

Technovation

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

Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems

Sandor Boyson

R.H. Smith School of Business, University of Maryland College Park, 3356 Van Munching Hall, College Park, MD 20742-1815, United States

ARTICLE INFO

Available online 4 March 2014

Keywords:
Cybersecurity
Risk management
Supply chain management

ABSTRACT

Cyber supply chain risk management (CSCRM) is a new discipline designed to help IT executives address the challenges of the rapid globalization and outsourced diffusion of hardware and software systems. CSCRM is an integrative discipline combining elements of cybersecurity, supply chain management, and enterprise risk management into a new and powerful concept to exert strategic control over the end-to-end processes of the focal organization and its extended enterprise partners. This article provides a survey of the field, as well as a detailed analysis of the results of a four-year research project on CSCRM, conducted by the Robert H. Smith School of Business Supply Chain Management Center for the National Institute of Standards and Technology, that focused on the development of organizational assessment tools and a capability/maturity model for this emerging discipline.

1. Introduction

Cyber supply chain risk management (CSCRM) is an emerging management construct resulting from the fusion of approaches, methods, and practices from the fields of cybersecurity, enterprise risk management, and supply chain management.

Woven together from the disciplines shown in Table 1 below, CSCRM can be defined as the organizational strategy and programmatic activities to assess and mitigate risks across the end-to-end processes (including design, development, production, integration, and deployment) that constitute the supply chains for IT networks, hardware, and software systems.

Each of these disciplines has evolved in separate, autonomous tracks. Enterprise risk management has been largely incubated in the financial services industry and has sought to anticipate revenue shocks and surprises to the focal company. In the post-9/11 period, other sectors such as global manufacturing and energy production have adopted and intensified their use of enterprise risk management practices, such as the one shown below, to detect and mitigate a spectrum of strategic and operational risks. Supply chain management, which began and developed within the manufacturing sector, has now been heavily deployed across services organizations of all types. Cybersecurity has evolved out of the seedbed of the IT integration business and its toolset has been leveraged across companies and governments around the world. Each of these disciplines has generated its own theoretical foundations, its own distinct community of specialist practitioners, and its own hierarchy of standards and best practices.

Table 2 provides an overview of the representative practices that have accompanied the growth of each of these unique and separate disciplines.

Unlike cybersecurity alone, cyber supply chain risk management focuses on gaining visibility and control not only over the focal organization but also over its extended enterprise partners, such as Tier 1/Tier 2 suppliers and customers. In addition, while cybersecurity emphasizes purely technical means of control, CSCRM seeks to engage both managerial and human factors engineering in preventing risks from disrupting IT systems' operations. Unlike enterprise risk management alone, CSCRM is not focused on a top-down control mechanism for relatively static business environments, but rather seeks to address the fundamental dynamism and real-time, world scale of adaptive IT networks. Finally, unlike supply chain management alone, CSCRM must deal with constantly dynamic world-scale network demand patterns and often “masked” supply chain provider identities.

The CSCRM construct has arisen within the past five years in response to the urgent needs of IT architects for strategies and toolsets to effectively control the design, build, and deployment of systems whose hardware and software subsystems and components are increasingly sourced from geographically far-flung suppliers of often unknown pedigree, and whose critical functionalities are hosted, exposed, and accessed on network environments of uncertain integrity.

The escalating malevolence and intentional destructiveness of IT system attackers have led to a general loss of confidence in the use of technical means only to control these attacks.

E-mail address: sboyson@rhsmith.umd.edu

http://dx.doi.org/10.1016/j.technovation.2014.02.001
0166-4972

Table 1
Constituent disciplines of cyber supply chain risk management (Treadway Commission, 2004; CSCMP; WhatIs.com; NIST, 2013; Manufacturing.net, 2012; Booz Allen Hamilton, 2009; Boyson et al., 1999, 2011).

Discipline definition	Milestones
1. Enterprise Risk Management: "A process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"	**1995**—Development of national standards for risk management of financial institutions began in Australia. Similar standards were implemented in Canada (1997) and in the UK (2000) **1996**—National Association of Insurance Commissioners (NAIC) in the United States introduced risk-based capital requirement for insurance companies **2002**—A series of corporate accounting scandals led to the passage of the Sarbanes-Oxley Act in the U.S., which mandated corporate risk governance **2004**—COSO Enterprise Risk Management Integrated Framework is finalized as a global standard
2. Supply Chain Management: "Supply chain management is an integrating function with primary responsibility for linking major business functions and business processes within and across companies into a cohesive and high-performing business model. It includes all logistics management activities as well as manufacturing operations, and it drives coordination of processes and activities within and across marketing, sales, product design, finance, and information technology"	**1982**—Booz Allen Hamilton consultant Keith Oliver coins the term "Supply Chain Management" **1995**—University of Maryland research project documents the rise of supply chain management—not only internal corporate integration initiatives involving procurement, manufacturing, and distribution but also external integration strategies with customers and suppliers. This research is based on surveys and field visits with 1300 companies. *Logistics and the Extended Enterprise* (Boyson et al., 1999), a book based on this research, is published in 1999 **1996**—Supply Chain Council is formed by 69 founding companies and develops the Supply Chain Operations Reference (SCOR) Model, an industry-wide set of standards and process frameworks **2002**—Council of Logistics Management is renamed Council of Supply Chain Management Professionals in recognition of supply chain's emerging key role
3. Cybersecurity: Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access	**1969**—Three members of the British Communications Headquarters invented the first set of asymmetric key algorithms, which would later be incorporated into a technique commonly referred to as "non-secret encryption" or "public-key cryptography" **1970**—RAND Report R-609, "Security Controls for Computer Systems" (also known as "The Ware Report"), was published to identify and recommend critical security-protection mechanisms required to safeguard classified information stored in resource-sharing systems. It also included critical security standards and controls for such systems **1983**—The first version of the Trusted Computer Security Evaluation Criteria (TCSEC), also known as the "Orange Book," was published. The Orange Book would become a U.S. Department of Defense security standard in 1985 and provide technical security guidance and associated system evaluation methodology **1987**—The United States Congress passed the Computer Security Act of 1987 to promote the establishment of minimum security practices for federal computer systems, including the development of enhanced computer security plans for sensitive information **2013**—President Obama signs the Executive Order on Cybersecurity and mandates that the National Institute of Standards and Technology (NIST) develop a cybersecurity framework for the federal government; NIST produces a preliminary version in August 2013

Table 2
Representative practices of the constituent disciplines (Harrington et al., 2010; Boyson et al., 2011).

Discipline	Representative practices
1. Enterprise Risk Management	**Executive risk group**, composed of chief risk officer and members of board of directors and strategic business units, created to set objectives and guide enterprise risk management program development Probablistic methods of analysis (such as Monte Carlo simulations) employed to assess the likelihood and severity of impact of enterprise risks Ongoing audit methodologies used to track the timeliness and effectiveness of risk mitigation activities
2. Supply Chain Management	**Corporate supply chain group**, composed of chief supply chain officer and unit directors for demand planning, sourcing, manufacturing, and distribution, set supply chain-wide policies for demand/supply balancing and ensure process integration across units and with extended enterprise partners Use of sophisticated supply chain mapping/network design tools to ensure maximum efficiency in the establishment of production and distribution points worldwide Use of enterprise resource planning (ERP) systems to fuse disparate planning and production data into a unified, real-time database Use of radio-frequency identification (RFID), digital locks, and other tracking technologies to assure end-to-end visibility of high-value goods in transit
3. Cybersecurity	**IT security group**, composed of a chief information security officer and technical representatives of operating units, sets security policy and assures compliance with key practices Compliance areas include Federal Information Processing Standards (FIPS) certification of cryptographic features Bolster IT network "perimeter defenses" through enhanced intrusion-detection systems Common criteria standards for security of systems, products, and services Build or buy better IT threat-analysis capabilities Screen software code or hardware from offshore prior to domestic integration Increase sourcing from pre-certified "trusted" vendors of IT hardware and software