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

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 © 2014 Elsevier Ltd. All rights reserved.

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

Please cite this article as: Boyson, S., Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation (2014), http://dx.doi.org/10.1016/j.technovation.2014.02.001

The full-spectrum cyber supply chain risk management construct seeks to harden both defense in depth, which covers the entire system life cycle starting with design, and defense in breadth, which spans the focal organization's extended supply chain from suppliers to customers. It is this comprehensiveness of strategic control that has made the cyber supply chain risk management construct such a promising and compelling new approach.

Yet *the promise will not be fulfilled unless organizations address the challenge of structural integration across the IT supply chain*. The extent of integration required will bring together the chief risk officer, the chief information officer, the chief supply chain officer, and their respective organizations in a formal enterprise risk management program. This program will employ not only a governance team, but also prescribed risk identification and assessment methods, and a portfolio of active mitigation techniques with delineated milestones for demonstrating risk reduction effectiveness.

Attaining this structural integration represents a significant managerial advance and will increasingly come to represent best practice in the IT supply chain risk management capability/maturity continuum.

This strategic imperative has been recognized by the President's Council of Advisors on Science and Technology (PCAST) in its recommendations on cybersecurity in November 2013: “Industry-driven, continuous-improvement processes are more likely to create an effective cybersecurity culture than are government-mandated, static lists of security measures.” (PCAST, 2013).

This article provides a survey of the evolution of the discipline and an overview of some of the early field research into the types of operating practices aimed at achieving high structural integration and risk management across the IT supply chain. It also captures the spectrum of practices in a formal capability/maturity model developed under a research project for the National Institute of Standards and Technology (U.S.); and compares and contrasts organizational behaviors associated with common, more advanced, and best practices as we currently understand them. The model's overall orientation is that the greater the degree of structural integration and collaboration between key players, processes, and IT platforms, the more advanced the organization both in capability and maturity.

2. Background

“Cyber” is a prefix used to describe a person, thing, or idea as part of the computer and information age. Taken from *kybernetes*, Greek for “steersman” or “governor”, it was first used in “cybernetics”, a word coined by Massachusetts Institute of Technology professor Norbert Wiener and his colleagues to describe control mechanisms for information processing in organisms and organizations. Common usages include “cyberculture”, “cyberpunk”, and “cyberspace”. (Askville, 2013).

It is fitting that the cyber supply chain management construct – with its end-to-end structural integration and overarching effort at strategic control of multi-enterprise IT systems – has arisen to fulfill the very definition of “cyber” itself and to provide a governor/steersman to a diversity of hardware/software and system-integration activities. Wiener himself, the father of cybernetics control theory, emphasized the role of organizational structure in governance of information. He argued that information was a quasi-physical concept related to the degree of organization in a system (Ramage, 2009). The implication of his observation is very relevant today: how information is protected relates to how a system is organized. Thus, *cybersecurity is both structural and technical.*

Similarly, in supply chain management, structural issues – e.g., the extent of integration across the functions and unit boundaries within the enterprises that form an extended chain – act as a determinant of effective performance. Germain et al., 2008 is part of a long tradition of researchers who have emphasized structural integration to overcome environmental uncertainties. Germain observes that in volatile demand environments, formal controls are insufficient to manage supply chain processes; rather, structural integration is key to effectively addressing uncertainties. “Supply chain process variability is a level of inconsistency, or volatility, in the flow of goods intra, through, and out of a firm. We found in a predictable demand, only formal control affects supply chain process variability, leading to improved financial results; but in an unpredictable environment, only cross-functional integration affects supply chain process variability, leading to improvements” (Germain et al., 2008).

In highly volatile operating environments, both in IT systems and in supply chains, the very structure of the organization and how it is configured determines adaptability and performance, with higher degrees of integration leading to better enterprise performance. This has been a consistent finding of major industry surveys and benchmarking activities.

The Supply Chain Council and its 800 corporate members have evolved the Supply Chain Operations Reference (SCOR) Model, which has become the standard process-improvement framework on a global basis. The SCOR Model is based on a capability/maturity spectrum wherein companies move through various stages: from Stage 1 (stove-piped, functional focus); through Stage 2 (internal integration, with demand/supply balancing); through Stage 3 (external integration, where technology and processes are extended to key customers and suppliers); and on to Stage 4 (cross-enterprise collaboration and optimization, with real-time performance improvement). PricewaterhouseCoopers (PwC) created extensive enterprise assessment tools and a benchmarking database of supply chains that contains data from over 1300 supply chains dating back to 1998 and examines performance and end-to-end process metrics that encompass plan, source, make, and deliver functions. PwC reports that Stage 4 best-in-class companies have 25% higher sales growth than other companies; and 40% higher profitability than median companies (Heywood, 2006; PRTM, 2006).

More recently, the Supply Chain Risk Leadership Council (SCRLC), a consortium of mainly high-tech companies, developed and released a Supply Chain Management Risk Maturity Model that enables a company to rate its own leadership, planning, implementation, evaluation, and improvement capabilities. These ratings help a company position its supply chain risk management along a spectrum of maturity ranging from Stage 1 (reactive) through Stage 4 (integrated), and beyond to Stage 5 (resilient). Among the features of Stage 5 supply chain risk management capabilities are enterprise-wide: risk leadership and formal programming; end-to-end supply chain mapping across critical products; comprehensive and integrated processes for conducting threat, vulnerability, and criticality analyses; and risk treatment processes that emphasize an adaptive capacity and preemptive measures (SCRLC, 2013).

Each of the models cited above places great emphasis on structural integration across the supply chain as a hallmark of organizational prowess and maturity. Yet globalization has fragmented and dispersed IT supply chains over the past five or so years, disaggregating production, distribution, and consumption of hardware and software in a similar fashion to the consumer product supply chain in the 1990s and early 2000s. Structural integration has not been the key corporate objective; cost minimization and/or new-market penetration in developing countries such as India or China have been higher priorities in IT supply chain build-outs. That is why we are where we are today: facing an escalating wave of threats from the very supply chains we thought would help us most in building out our IT systems.

3. Scope of the problem

The rapid globalization of the product supply chain had been well documented early on in that process. By 2005:

- 1% of North American manufacturers had moved production to lower-cost locations
- Nearly half of North American manufacturers had sold products in China
- More than 40% of North American manufacturers were planning to expand their marketing base into Eastern and Central Europe, Mexico, and Central America (Deloitte Touche Tohmatsu, 2005).

Accelerating globalization and outsourcing of both software and IT hardware are not as well documented but have now become the norm in the U.S. electronics industry: only an estimated 20% of all computer chips are now made in the United States. A consequence of this phenomenal dispersion of the IT supply chain is that "the attack surfaces" of our systems have grown substantially larger and easier to penetrate. Let us inventory some of the ways that these information and communication technologies (ICT) supply chains are being compromised.

3.1. *Counterfeits*

Counterfeits are flooding federal IT systems in the U.S. For example:

- Integrated circuits
  In 2010, VisionTech Components, a Florida-based company, sold 60,000 counterfeit integrated circuits from Asia that went into U.S. Department of Defense (DOD) missile programs, Department of Homeland Security (DHS) radiation detectors, and Department of Transportation (DOT) high-speed trains, situations where failures in IT systems can be catastrophic (McMillan, 2010).
  In 2013, the U.S. Naval Submarine Base in New London, Connecticut, used three counterfeit products sold by a Massachusetts man who was indicted on conspiracy, fraud, and trafficking charges on July 16, 2013. "According to the indictment … Peter Picone, 40, of Methuen, Mass., and unidentified co-conspirators shipped the counterfeit integrated circuits to the sub base between November 2011 and February 2012. At least two of the circuits were intended for active-duty nuclear submarines … One was intended for an alarm panel, while another was to be used in a radio-transmission test, the indictment said. 'I have to buy from China and risk fake parts to compete… it's my whole biz,' the indictment quotes Picone as saying in a 2008 instant message. … In addition, a defense contractor in Florida bought 33 integrated circuits from one of Picone's companies to be used during repair work on an active-duty nuclear sub's secondary propulsion system, the indictment said. … 'Picone went to great lengths to conceal the true origin of counterfeit semiconductors in order to sell the devices as seemingly legitimate and reliable components for use in nuclear submarines and other complex machinery,' Acting Assistant Attorney General Mythili Raman said in a statement. … The charges against Picone carry maximum sentences of from five to 20 years" (Howard, 2013).
- Routers
  In May 2010, the Federal Bureau of Investigation (FBI) closed a counterfeiting operation that produced phony Cisco routers, switches, network cards, and secure communications devices worth more than $145 million. These routers power government networks all over the world (Kunert, 2011).

3.2. *Malicious tampering*

Apart from IT globalization providing ample opportunities for exercising individual greed through counterfeit sales, it also energizes criminal organizations and foreign intelligence services who are targeting the supply chain.

In 2007, hard drives produced in Thailand by an American firm had "report-back mechanisms" embedded in them by a foreign intelligence service. These hard drives were sent to DOD, copied all of the classified files stored on them, and transmitted the files via the Internet back to the foreign intelligence service (McMillan, 2007).

In 2010, Dell Power Edge 410 servers were shipped with malware pre-installed on the motherboards and required sixteen changes in supply chain procedures to block attack pathways (InfoSecurity Europe, 2010).

Yet external intrusions are only one side of the problem.

3.3. *The "insider threat"*

The "insider threat" is the other part. As IT supply chains proliferate globally, it becomes harder to control and monitor employees. In addition to external threats, the insider threat is also growing. Fraud by employees is increasingly common and difficult to stop. According to the Association of Certified Fraud Examiners, the median loss from inside attacks is $175,000. Most inside attackers are first-timers; 7% have prior convictions, and only 12% were previously terminated for fraud-related conduct (Cole and Ring, 2005).

These examples show the IT supply chain itself offers numerous tiers and echelons of targets for breach and corruption. In fact, a recent study by the computer security firm Symantec 's "2013 Internet Security Threat Report" (Symantec, 2013a), which is based on its network monitoring across 157 countries, has found that the supply chain is the latest threat vector:

> *Manufacturing sector and knowledge workers become primary targets:* Shifting from governments, manufacturing has moved to the top of the list of industries targeted for attacks in 2012. Symantec believes this is attributed to an increase in attacks targeting the supply chain—cybercriminals find these contractors and subcontractors susceptible to attacks and they are often in possession of valuable intellectual property. Often by going after manufacturing companies in the supply chain, attackers gain access to sensitive information of a larger company (Symantec, 2013b).

The composite losses from attacks on the IT supply chain are staggering. The Chairman of the U.S. House of Representatives Intelligence Committee, Mike Rogers, a former FBI agent, revealed that *the combined losses from cyber attacks on U.S. enterprises was about one trillion dollars in lost revenue and 10,000 jobs lost per year* (National Public Radio, 2011).

Despite the escalating consequences of IT globalization and security failures, purely technical approaches to cybersecurity are not keeping up with the threat. In 2011, a Bloomberg Government study surveyed 172 *Fortune* 500 companies that were spending a combined $5.3 billion per year on cybersecurity, out of the estimated total global spend on cybersecurity of $60 billion in 2011 (PwC, 2012) and claimed to be stopping 69% of threats. Furthermore, this sample of companies believed that if they raised spending to $10.2 billion, they would stop 84% of threats, and if they raised spending to $46.67 billion, they would stop 95% of threats, “the highest attainable level”. The question asked by many observers, of course, is whether 95% is good enough (Domenici and Bari, 2012).

The cybersecurity problems cited above are not just technical problems. They are also supply chain problems that require a new, end-to-end assurance model and a deeper level of structural integration across enterprises. Extended global IT supply chain policies, processes, and people must be put into place to attain this level of integration. Just as in the late 1990s – when globalization, outsourcing, and fragmentation of product manufacturing accelerated the development of an integrated corporate management process; e.g., supply chain risk management – so today, the same factors in ICT production are driving the growth of cyber supply chain risk management.

4. Cyber supply chain risk management: Research to date

Like the product supply chain, the cyber supply chain is an end-to-end process. Boyson et al. (2009) defined the cyber supply chain as “the entire set of key actors and their organizational and process-level interactions that plan, build, manage, maintain, and defend the IT system infrastructure”. This business ecosystem is shown in Fig. 1.

Similarly, Simpson (2010) defines the IT system supply chain as a globally distributed dynamic collection of people, process, and technology. Goertzel (2010) states the IT supply chain is constituted by:

- Processes
- Products (including their innate intellectual property)
- Product flows
- Data (e.g., supply chain management data, product data, and metadata)
- Data flows
- Participants (people).

One important concern of the community of government agencies, academia, and practitioners is how to assess and mitigate the risks embedded in the cyber supply chain. Consequently, the community has developed diverse risk frameworks and proactive management models such as: a cyber supply chain assurance reference model (Boyson et al., 2009), an assurance-based approach (Storch, 2011), and a risk-based approach to manage software integrity (Storch, 2011).

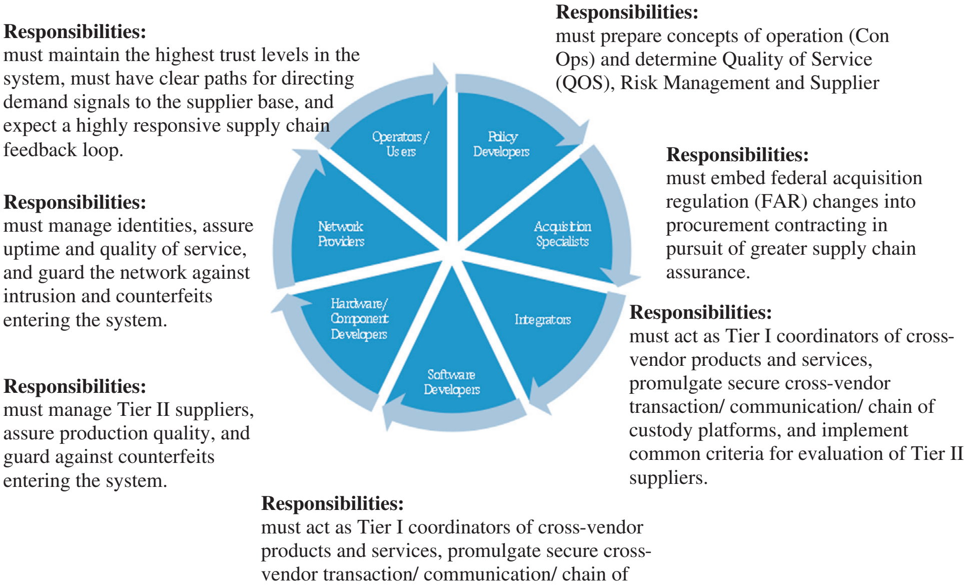
Borg (2010) describes the possible consequences of cyber-attacks on the operation of the cyber supply chain: interruption of the operation, corruption of the operation (inserting malware), discrediting of the operation (undermining trust, damaging brand value), and undermining the basis of the information (loss of control, loss of vital information). He presents remedies that should be applied in all five stages of the supply chain: the design phase, fabrication phase, assembly phase, distribution phase, and maintenance phase. In addition, he states that the assurance framework requires legal relationships between global component suppliers, assemblers, and the focal company.

The Open Group (2011) found that the trustworthiness of global IT supply chains is impeded due to the lack of the following: consistent terms; uniform supply chain standards, practices, and approaches; and comprehensive common ways of providing evidence of a product’s trustworthiness. The group listed effective best practices in four categories: product development/engineering, secure engineering, supply chain integrity method, and product evaluation method.

Simpson (2010) developed an assurance-based approach to minimizing risks in the supply chain. The software assurance is based on the following three pillars:

- *Security*: Threats are anticipated and addressed during the software’s design, development, and testing.
- *Integrity***:** Threats are addressed in the processes used to source software components, create software components, and deliver software to customers.
- *Authenticity*: The software is not counterfeit and the software supplier provides customers with ways to differentiate genuine from counterfeit software.

This study identifies the controls based on the seven principals for software integrity, which include: chain of custody, least privilege access, separation of duties, tamper resistance and evidence, persistent protection, compliance management, and code testing and verification.



Responsibilities:
must maintain the highest trust levels in the system, must have clear paths for directing demand signals to the supplier base, and expect a highly responsive supply chain feedback loop.

Responsibilities:
must prepare concepts of operation (Con Ops) and determine Quality of Service (QOS), Risk Management and Supplier

Responsibilities:
must manage identities, assure uptime and quality of service, and guard the network against intrusion and counterfeits entering the system.

Responsibilities:
must embed federal acquisition regulation (FAR) changes into procurement contracting in pursuit of greater supply chain assurance.

Responsibilities:
must act as Tier I coordinators of cross-vendor products and services, promulgate secure cross-vendor transaction/ communication/ chain of custody platforms, and implement common criteria for evaluation of Tier II suppliers.

Responsibilities:
must manage Tier II suppliers, assure production quality, and guard against counterfeits entering the system.

Responsibilities:
must act as Tier I coordinators of cross-vendor products and services, promulgate secure cross-vendor transaction/ communication/ chain of

Fig. 1. Business ecosystem (Boyson et al., 2009).

Please cite this article as: Boyson, S., Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation (2014), http://dx.doi.org/10.1016/j.technovation.2014.02.001

Ellison et al. (2010) developed an assurance case reference model. This model identifies key strategies for controlling security risk:

- Identify and monitor a system attack and
- Develop and maintain a threat model.

Software supply chain security risks that must be addressed in every phase of the acquisition life cycle were identified as: initiation, development, configuration/deployment, operations/maintenance, and disposal. The authors state that two powerful strategies – attack surface and threat modeling – are key to making supply chain security risk management tractable. Attack surface focuses on analysis for understanding and controlling a system's vulnerabilities, while threat modeling focuses on understanding potential threats that could exploit those vulnerabilities.

Storch (2011) explains a risk-based approach to managing software integrity developed by Microsoft. Microsoft uses the "standard correlation" or "business process modeling" approach to carry out a risk assessment. Microsoft indicated that the "standard correlation" is preferred when mature standards exist that may also mitigate software integrity threats. This approach is less resource-intensive. Business process modeling "is useful to analyze software integrity attack scenarios in order to define areas of risk and to develop or strengthen corresponding controls to mitigate these risks". This approach is particularly effective in software development. Microsoft defined six steps to increase software integrity: (1) plan, (2) discover, (3) assess, (4) develop, (5) validate, and (6) implement.

Oltsik et al. (2010) of the Enterprise Strategy Group surveyed 285 security professionals of U.S.-based critical infrastructure organizations to identify their awareness of and their programs for dealing with cyber supply chain security. The main findings regarding cyber supply chain security issues were: information technology vendor security audits are performed inconsistently and are rarely thorough, and software assurance is a work in progress, with external information technology relationships lacking appropriate security.

There is a high degree of consensus in the cyber supply chain risk management community about the nature of the disconnections that presently afflict the IT supply chain, and about the broad outlines of solution sets that could be applied to enhance assurance.

Despite this unanimity among experts, progress in the field – at the individual corporate level – has been relatively slow and has not kept pace with the intensity of supply chain attacks. In the next section, we will explore the underlying causes of this deficient collective response.

5. The challenges to successfully implementing cyber supply chain risk management: Frontline cases

The challenges faced by global organizations in integrating the cyber supply chain are illustrated in the two case examples below. Both are based on interviews with IT supply chain executives, which were conducted by the R.H. Smith School of Business' Supply Management Center as part of its ongoing cyber supply chain risk management research. The identities of the executives in both organizations shall remain anonymous to protect the confidentiality of the research sources.

6. Global pharmaceutical company

6.1. The risk environment

At the time of this interview in 2010, this company had over $70 billion in revenue, of which an estimated $12 billion was set to disappear due to drugs in its portfolio losing patent protection. Revenue pressures had resulted in a significant cut to the IT organization. Between 2006 and 2009, the budget of the 2000-person business technology organization responsible for identity management, network servers, data storage, and third-party IT outsourcing had been reduced from $2 billion to $1.6 billion.

These cuts had occurred during a time period of escalating regulatory risk.

A major risk area for this company is the Sarbanes Oxley (SOX) legislation, which puts personal liability pressures on members of the company's board of directors and chief executive officer (CEO). Of 352 IT risk management requirements defined by the chief information officer (CIO), 85 are SOX-related. Distinct and separate SOX-compliant servers are built, maintained, and monitored continuously to ensure only authorized access, backups, and version control.

Another major risk area is U.S. Health and Human Services regulations that emphasize guarding against data-privacy breaches and the need to encrypt data. But the company has over 100 backup servers for patient and personnel information. Just to encrypt tapes at the data center for the top 20 servers would cost millions of dollars. If the company goes forward with this investment by itself, it will be at a competitive disadvantage vis-à-vis its competitors. If the regulations are vigorously applied across the industry, then the company that has a high degree of efficiency in asset management wins out. The company is uncertain about what degree of compliance it should seek to attain.

Finally, the U.S. Food and Drug Administration (FDA), which regulates the pharmaceutical industry, represent yet another regulatory risk. The agency has the power to issue a consent decree stopping production and product shipment if it finds the company to be out of compliance with good clinical and manufacturing practices. The company, in effect, must certify to the FDA that the following principles are in place:

> *Qualification*: IT system networks, software, and devices are all built the same way, following a defined process.
>
> *Validation:* Not only is a validated application built according to a specific process, but data in that application also is correct, and inputs/outputs have been validated for accuracy.
>
> *State of control:* Only changes that were planned, tested, and authorized have taken place on the system; there is documented change control; and it is a "trusted System".

Any finding by the FDA that disputes the assertions made by the company in regard to the principles above can result in a consent decree that can reduce revenue from a billion dollars to zero overnight. This is categorically different than a typical corporate risk incident.

Similarly, an intrusion or breach of shop-floor industrial control systems, product counterfeits making their way into distribution channels, or IT systems/product provenance records that are compromised can play havoc with revenues.

6.2. The IT supply chain risk management organization

For these reasons, the chief information officer organization has established a small interface group (called the quality and risk management function) to work with the vice president of global supply chain around IT supply chain assurance issues. This group is responsible for "100% compliance with all requirements managed by the IT organization" and is composed of an executive who manages common requirements and sets rules for the company's 5000 IT vendors; a threat intelligence executive who was a former local FBI director; and an executive in charge of quality and safety.

The overriding mandate of this group is to "keep supply chain threats at a level that will not interfere with strategic IT issues", and to ensure that corporate governance of IT risk extends out to business partners in its ecosystem. Its main task is to work closely with the company's worldwide corporate procurement unit – the unit that deals with large strategic suppliers – to conduct assessments of the most critical vendors before contract initiation and during yearly reviews that involve a three-day, on-site audit utilizing certified IT auditors. In addition, there is a software-code audit of the vendor that is outsourced to an external audit repository center, where vendor source code is automatically scanned for malware and viruses.

There is daily informal communication between the IT threat intelligence executive and the procurement unit's vendor management staff. Emergent vendor risks (events, incidents, and indicators of compromise) are jointly identified, prioritized, and placed on a shared online risk registry for visibility, tracking, and mitigation.

6.3. *The risk "hot list"*

At any given moment, there are ten major risks "currently on fire" and being tracked on the risk registry. These rotate frequently based on how incoming risks are sorted based on quantitative analyses of risk impacts, and on the likelihood of risks impacting privacy and other organizational priorities. The registry itself is a matrix table that lays out: a description of each risk, a risk score, a set of corrective actions, a responsible party to mitigate that risk, and a schedule of mitigation activities.

The quality and risk management function acts as project manager to: broker out the risks to the risk owners, come up with an action plan, work with risk owners and get them to "accept" risk, and audit vendors' follow-up efforts.

Pre-contract, clauses are put into vendor contracts that oblige the vendors to address the risk. Mid-lifecycle, there is a formal agreement with the vendor to execute time-based mitigation steps. A vendor rating system scores compliance, and second chances are given to address risks. Third chances are usually not given.

Given the highly complicated set of regulatory and internal requirements that the company must satisfy, the interface group is seeking to establish and keep current a single integrated risk-assessment tool for IT vendors. This would include data security, privacy, and other concerns as part of the tool.

The severity of IT supply chain risks over the past three years has changed the leadership team's view of these risks and has made a review of these risks a standing item in the CIO's monthly leadership team meeting.

Yet despite these coordination efforts, it is clear that much remains to be done. There is still a lack of integration between the manufacturing/supply chain side of the business and the IT side. For example, shop-floor industrial controls are currently not included in IT security surveillance and audits. Also, the structure of financial compensation for managers is based on financial performance only and not on effective risk management. Thus, IT risk management remains a secondary, tactical issue when judged purely on how incentives are structured.

Finally, the vice president of supply chain and the CIO do not participate together in a C-suite corporate risk council that works toward an enterprise-wide risk management approach. In fact, there is no "chief risk officer" for the company as a whole—someone who might lead this enterprise program and help force the kind of structural integration across the supply chain that could lead to much more effective IT system assurance.

7. U.S. Intelligence Agency

The main question we sought to answer in our discussion with members of the Intelligence Agency's IT supply chain organization was this:

> Is a deadly serious security environment and risk-averse culture supported by a portfolio of advanced cyber supply chain risk management practices?

The key players in the Intelligence Agency's IT supply chain activities all work within their own functions/units but came together as a group for the purposes of this interview. These executives served in diverse roles, including:

- *IT acquisition chief of security,* who vetted vendors and performed risk assessments on both classified and unclassified products. This executive developed assessment standards over an eight-year period and was responsible for over 14,000 vendor/case assessments that reviewed the background of the vendor company; its geographic and operational footprint; and its long-term, mid-term, and daily risk events.
- *IT architect,* who oversaw systems implementation and network security/operations.
- *Director, hardware assurance,* who evaluated/validated microelectronics from design to functionality based on cost, schedule, and trust, or integrity of configuration.
- *Director, software assurance,* who verified the functionality of in-house software and sought visibility into globally sourced software.
- *Director of the Trusted Foundry program*, whose responsibility included development and certification of fabrication facilities for high-assurance integrated circuits used in highly classified IT systems.

These individuals do *not* form a risk council that reviews and manages risks across the IT supply chain on a continuous basis. Rather, they participate on an as-needed basis in a technical review board for each system built by the Agency; provide ongoing certification that all check-listed steps for the project, from pre-request for proposal (RFP) to production, have been successfully completed; or force the program manager back to the process to address risks or necessary project tasks.

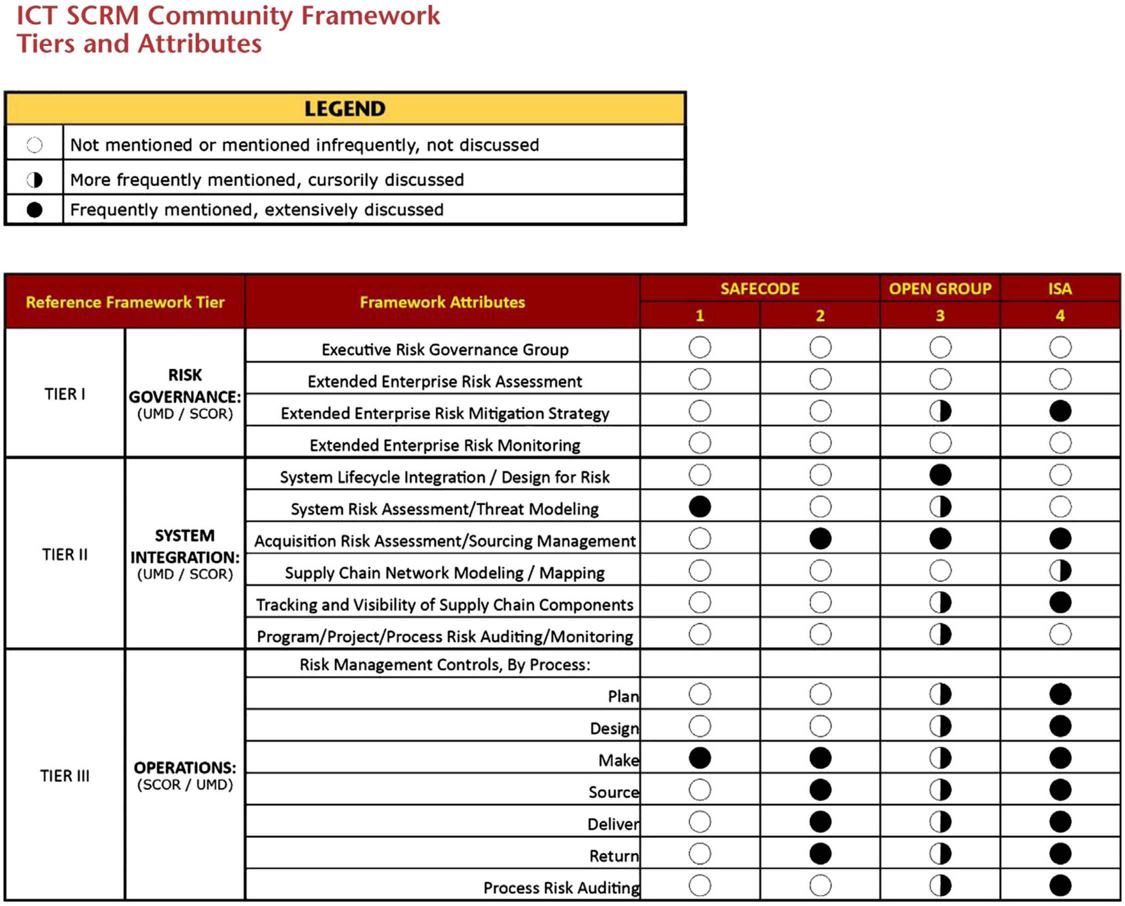
These executives were concerned that, although the Agency always had a "security first" culture, it was proving difficult to generate policies that responded to the rapidly changing IT supply chain risk profile. The globalization and commoditization of hardware and software had forced the Agency to become more market-oriented in its systems development approach. This opened up many new risks: the lack of visibility into a highly dispersed supplier base, especially beyond the most critical Tier 1 suppliers; the new susceptibility to product tampering by foreign adversaries; and the difficulties in harmonizing classified systems' standards and governance approaches with those of the private sector. Fundamentally, the question was: how to effectively deal with strategic control and accountability over the global IT supply chain being redistributed to industry?

Despite those radical shifts in the IT supply chain risk profile, the internal workings of the Agency were not adapting quickly enough to stay on top of the risks. There was no formal risk-governance group that acted as a coherent force to systematically review, assess, and prioritize IT supply chain-wide risks. Risk assessments were made by each unit but were not collected and aggregated into an enterprise-wide analysis. There was not enough data mining of IT supply chain data to identify emerging risks; for example, the 14,000 vendor risk assessments/cases were not being deep mined. There was no formal risk registry to assign responsibilities and track mitigation of priority risks.

The Agency is at a tipping point. Will it integrate risk management activities across the IT supply chain and create an executive group capable of defining new policies in an era of transformed, globalized technology markets?

The two case examples cited above highlight the extreme integration challenges faced by organizations today. Corporate uptake of cyber SCRM is proceeding slowly. In our National Institute of Standards and Technology-sponsored ICT SCRM Vendor Survey

Please cite this article as: Boyson, S., Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation (2014), http://dx.doi.org/10.1016/j.technovation.2014.02.001



ICT SCRM Community Framework
Tiers and Attributes

LEGEND	
○	Not mentioned or mentioned infrequently, not discussed
◑	More frequently mentioned, cursorily discussed
●	Frequently mentioned, extensively discussed

Reference Framework Tier		Framework Attributes	SAFECODE		OPEN GROUP	ISA
			1	2	3	4
TIER I	RISK GOVERNANCE: (UMD / SCOR)	Executive Risk Governance Group	○	○	○	○
		Extended Enterprise Risk Assessment	○	○	○	○
		Extended Enterprise Risk Mitigation Strategy	○	○	◑	●
		Extended Enterprise Risk Monitoring	○	○	○	○
TIER II	SYSTEM INTEGRATION: (UMD / SCOR)	System Lifecycle Integration / Design for Risk	○	○	●	○
		System Risk Assessment/Threat Modeling	●	○	◑	○
		Acquisition Risk Assessment/Sourcing Management	○	●	●	●
		Supply Chain Network Modeling / Mapping	○	○	○	◑
		Tracking and Visibility of Supply Chain Components	○	○	◑	●
		Program/Project/Process Risk Auditing/Monitoring	○	○	◑	○
TIER III	OPERATIONS: (SCOR / UMD)	Risk Management Controls, By Process:				
		Plan	○	○	◑	●
		Design	○	○	◑	●
		Make	●	●	◑	●
		Source	○	●	◑	●
		Deliver	○	●	◑	●
		Return	○	●	◑	●
		Process Risk Auditing	○	○	◑	●

Fig. 2. SCRM community framework tiers and attributes (R.H. Smith School of Business, 2012).

(Boyson et al., 2011), we found that on the strategic side of risk management:

- 47.6% of our sample of 200 companies never use a risk board or other executive mechanism to govern risk
- 46.1% never use a shared risk registry, an online database of IT supply chain risks
- 49.4% never use an integrated IT supply chain risk management dashboard, and 44.9% say they never use a supply chain risk management plan"
- Most companies do not use automated business rules and sensor-driven responses; e.g., they cannot sense and respond to risks in real time.

As they seek to transition from a more passive IT supply chain risk management phase to a more mature, proactive, flexible, and adaptive phase, organizations are spread across a spectrum of capability/maturity phases. We will discuss the parameters of these phases in the following section.

7.1. The cyber supply chain risk management capability/maturity continuum

As shown by the example cases above, cyber supply chain risk management is a still-emerging discipline. This has been repeatedly demonstrated in our own research. In 2011, our Supply Chain Management Center ran a focus group of top federal IT supply chain policy makers and managers to discuss the state of the art. Participants came from the U.S. Department of Defense (DOD), Department of Homeland Security (DHS), National Security Agency (NSA), Federal Communications Commission (FCC), and major vendors such as Intel and Microsoft. Of the 19 participants, eight had been working in this field for two years or less.

In addition, our team built a Cyber Supply Chain Framework that incorporated our corporate survey results and other research. We used this framework to review 60 public- and private-sector SCRM standards and policy initiatives, and evaluate their extent of coverage of the end-to-end cyber supply chain. This three-tier model covered risk governance, system integration, and operations and was used to determine how extensively each initiative addressed the set of key attributes within each tier, as shown in Fig. 2.

By using this end-to-end framework as the benchmark, we were able to analyze 60 public- and private-sector cyber supply chain risk management initiatives and map each initiative's extent of coverage of the tiers and attributes defined above.

As shown in Fig. 3, we found that for a sampling of these initiatives there is a clear clustering of efforts around the internally oriented systems development and key supplier-oriented sourcing functions. Initiatives tend to focus on the focal enterprise itself and a few critical suppliers. Across the "defense in breadth" axis, supplier's suppliers and customers are not encompassed in many initiatives' areas of coverage. In other words, there is inadequate scope of effort to manage the entire supply chain.

At the high end of the "defense in depth" axis, there appears to be extensive gaps in initiatives' coverage of risk governance. At the low end of the same axis, initiatives do not seem to adequately address the need for field-based, real-time sensor networks that can sense and respond to operational threats.

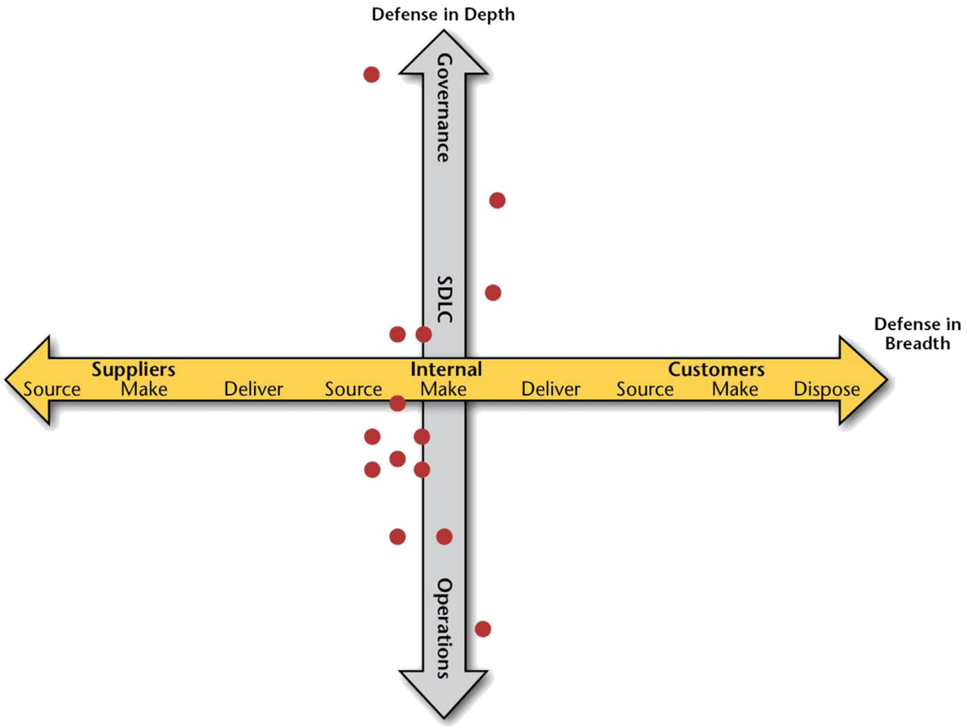


Fig. 3. Strategic orientation of a sample of cyber supply chain initiatives (R.H. Smith School of Business, 2012).

In a more mature management environment, we would expect to see a much more even distribution of management efforts across both the defense in depth and defense in breadth axes.

The examples above highlight the early and immature phase of the cyber supply chain risk management cycle that industry currently is in, and the need for accelerating the development of effective best practices.

7.2. Rationale for a capability/maturity model for the cyber supply chain

As previously discussed, capability/maturity model development is a hallmark of a rapidly growing discipline and one that seeks to differentiate performance among organizations to understand worst, common, and best practices. This process of capability/maturity building occurred relatively early in the historical cycles of both the parent supply chain discipline and its offspring supply chain risk management discipline.

We developed a cyber supply chain risk management capability/maturity model in collaboration with NIST in response to these specific needs:

- The community body of knowledge needs to be built upon a coherent framework of empirical data derived from observations of a range of companies and practices to better determine the effectiveness of specific cyber supply chain risk management activities.
- Companies need to respond to new guidelines issued by the U. S. Securities and Exchange Commission in October 2011, which mandated corporate disclosures of cyber security risks that were "material"—that is, they endangered 10 percent or more of earnings. This ruling was designed to counteract the often-absurd efforts by major institutions to disguise the impacts of cyber attacks. One bank, for example, failed to disclose or report $1 billion in damages from a cyber attack (SEC, 2012). These new disclosure guidelines and the exposure to greater potential liability they can generate for companies means that a cyber supply chain risk management capability/maturity model might be valuable in assessing companies' relative positioning in the industry and provide guidance for improvement strategies.
- The insurance industry needs to underwrite cyber risks and requires better measures of client exposures. Today, over 50 carriers in the industry provide cybersecurity insurance coverage (DHS, 2012). The exposures passed on to insurers can be enormous, yet industry underwriters do not yet appear to have reliable ways to measure a firm's cyber supply chain risk profile. A formal capability/maturity model might help the industry to measure these risk profiles and better differentiate firms' risk behaviors and premium levels.
- Finally, governments need ways to evaluate IT vendor capabilities, to screen proposal claims, and to predict/respond to vendors' risk behaviors. The U.S. General Services Administration has already piloted a process whereby supply chain risk management planning capability is a criterion for selection of vendors.

7.3. Approach to development of a cyber supply capability/maturity model

To undertake the design process, we conducted detailed research into enterprise assessment methodologies both within and outside the ICT SCRM discipline. We also sought to understand best practices in evaluating the capability/maturity levels of enterprise supply chains and cyber systems.

Among the sources consulted (by area of assessment) were:

- *Strategic readiness:* Field visits and extended discussions were held with the Risk Group of the Securities and Exchange Commission; with the executive director of the Independent Distributors of Electronics Association (IDEA); with the Center for Advanced Life Cycle Engineering (CALCE), University Of

Maryland; and with the principal of the Marsh Supply Chain Risk Management Practice, among others. In addition, we drew upon the pool of 500 company responses we received to two survey research projects: the first, our NIST Vendor Assessment Project already cited, and second, a survey we worked on with IBM/Sterling Commerce in 2010 in regard to corporate supply chain risk management. Finally, we included findings from our previously mentioned review of 60 initiatives in this area.

- *NIST principles and practices:* This assessment area was prepared utilizing the NIST IR 7622 on Supply Chain Risk Management as well as previous RH Smith School of Business research that had been conducted for NIST. In addition, we evaluated a variety of capability/maturity models, including the Supply Chain Council's SCOR Model and the Supply Chain Risk Leadership Council's emerging maturity criteria.
- *Field-testing the assessment tools:* We received support for our assessment development activities from the TM Forum, a 25-year-old, 800-member global organization of telecommunications industry providers. This organization selectively recruited a small member pool to validate our survey instruments and provide feedback. All efforts were made to protect the confidentiality of participant information. The survey website used SSL (secure socket layer) and HTTPS technology, and all comparative results were anonymized.

This process allowed us to iterate a first definition of a capability/maturity model that identified and defined average, more advanced, and leading-edge practices in the field. These practices are associated with each tier of capability (governance, systems integration, and operations). We categorized the results of the assessments by grouping practices and company performance into three stages: *emergent* (practices not implemented or in planning stages); *diligent* (limited or early enterprise implementation, but shows steady effort to enact supply chain controls); and *proficient* (seasoned implementation and achievement of process improvements across the supply chain).

The hallmarks of a proficient, mature IT supply chain risk management practitioner are the following:

- A set of extensive risk practices are in place across the enterprise
- There is intensive communication between the IT, supply chain, and corporate risk functions
- There is an emphasis on engaging not only suppliers but also customers in the risk surveillance/due diligence process
- There is greater use of tough contractual mechanisms to enforce risk disclosures and mitigation
- There is a more consistent strategy to assure continuous visibility of software and hardware production/delivery cycles through a field-level sensor network based on RFID, digital locks, video surveillance, and tracking portals.

For the complete capability/maturity model, see Appendix A.

We recognize that this development process is a dynamic one and that, as our research progresses, we will continue to build out the content and expand the validity of this model.

8. Conclusions

Cyber supply chain risk management is an emerging and important new branch of cybersecurity. It is an attempt to gain strategic management control over the rapidly globalizing cyber supply chain and to help compensate for deficiencies in purely technical approaches to security and assurance.

We have defined a research-based capability/maturity model to capture the spectrum of lagging, common, and best practices associated with this new discipline, and we have begun to test out this model's effectiveness in assessing the relative performance of organizations. But much work remains. Further research needs to unfold along the lines described below.

We are hopeful that, over time, assessment tools such as those we have created might be more widely administered and could lead to large-scale datasets able to establish definitive relationships between company cyber risk management practices and process outcomes (such as reduction in dollars or intellectual property lost to attacks). In other words, such large-scale data sets can become the foundations for "effectiveness studies" that can measure the degree to which a specific practice or a combination of practices can lead to improved metrics of performance. Comparative effectiveness research (CER)—defined by the Institute of Medicine as "the generation and synthesis of evidence that compares the benefits and harms of alternative methods to prevent, diagnose, treat, and monitor a clinical condition or to improve the delivery of care" (Institute of Medicine, 2009) has attained a prominent role in reforming the nation's health care system.

Similarly, effectiveness studies are needed to help guide improvements in cyber supply chain risk management. As the information security firm NSS Labs has noted, "Historically there has been a lack of empirical data to drive cybersecurity decisions. As a result, businesses are being compromised at an alarming rate" (NSS Labs, 2013). This lack of effectiveness data is evident in the absence of proof provided by standards bodies and industry associations that costly recommended actions will result in returns on investment to adopting organizations. Such an absence of proof has been an important disincentive to the diffusion of enterprise-wide cyber supply chain risk management practices.

Ultimately, our hope is that such efforts might contribute to the establishment of a data-driven *Corporate Cyber Supply Chain Code of Practice* that includes:

- *Required disclosure of IT risks.* For example, China in 2011 put into place a rule that requires detailed disclosure of the risks associated with 21 categories of IT security products.
- *Required risk governance structures.* In Canada, companies cannot even list on the Toronto Stock Exchange if they have not implemented risk governance mechanisms, such as an executive risk board, a risk registry, and a mitigation/monitoring.
- *Use of empirically proven best practices* derived from large-scale, data-driven effectiveness studies. Obviously, these best practices will be dynamic in nature and will evolve as the science progresses and relationship factors in the cyber supply chain are better analyzed and understood.

Although it is in an early phase of development, cyber supply chain risk management as a discipline offers the opportunity to exert end-to-end process discipline over the information and communications technology domain and provide enhanced systems assurance in a time of great, almost existential danger.

Acknowledgements

The author would like to thank my research colleagues – Hart Rossman, Thomas Corsi, and Holly Mann – for their unstinting devotion to this work; Mr. Jon Boyens for his support and visionary thinking; and Rodrigo Britto and Ngozi Chukwurah for their research and editorial support.

Please cite this article as: Boyson, S., Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation (2014), http://dx.doi.org/10.1016/j.technovation.2014.02.001

Table A1
Capability/maturity model for cyber supply chain risk management.
Source: R.H. Smith School of Business, 2012.

Cyber-SCM Key Factors	**Cyber-SCM Maturity Phase: Emergent** (Not implemented OR in planning stages)	**Cyber-SCM Maturity Phase: Diligent** (Limited or early enterprise implementation but shows steady effort to enact supply chain controls)	**Cyber-SCM Maturity Phase: Proficient** (Seasoned implementation and achievement of process improvements across the supply chain)
Tier 1: Governance			
Responsibility for risk management	Limited to CIO shop	Involves multiple business units	Extensive, enterprise- and supply chain—wide
Interaction between CIO/CSO and other key enterprise executives and supply chain partners	Nonexistent	Limited	Extensive
Enterprise risk management (ERM) program elements	Not defined	Defined and partially implemented	Fully defined and implemented
Systematic risk assessment activities	None	Selected risk assessment activities across the enterprise	Extensive supply chain-wide risk assessment activities involving suppliers and customers
Risk monitoring and/or digital forensics and reporting capacity	No risk monitoring and/or digital forensics and reporting capacity in place	Limited capacity in place	Extensive capacity in place
	Recommendations For Maturity Phases 1 and 2: Need to formalize risk management process with an executive organization, program charter and standardized techniques for risk assessment, prioritization and mitigation		
Tier 2: Systems Integration			
Security control of personnel, facilities, and processes	Due diligence/background checks of new hires and facility access control	Periodic security reviews of current employees and periodic monitoring of physical and IT access logs	Constant due diligence of employees and contractors and suppliers; and continuous monitoring of extended enterprise physical and IT access logs
System risk management embedded as overarching contractual obligation for contractors and suppliers	Not explicitly built into contracts	Explicitly built into contracts but not aggressively monitored or enforced	Explicitly built into contracts; aggressively monitored and enforced; consistent termination of out-of-compliance contractors and suppliers
Design of resilient systems via threat modeling and war gaming	Used sporadically to react to and address escalation in system threats	Used by internal enterprise personnel in proactively designing selective systems	Used as a critical design tool across all critical systems with key supply chain partners
Risk mitigation	Risks not identified and not assigned to specific personnel for mitigation purposes	Some risks identified and assigned for mitigation purposes, with sporadic follow-up	Continuous identification, assignation, mitigation, and monitoring of identified risks
Defense against IT supply chain breaches	Limited to IT perimeter defenses and intrusion detection	Broader IT system surveillance, including mechanisms such as proxy server code repositories for scanning/detecting viruses	Real-time risk dashboards and sensor grids for global situational awareness of IT and physical supply chains
	Recommendations For Maturity Phases 1 and 2: Ramp up use of contractual mandates to increase contractor/supplier disclosure and management of supply chain risk; need to establish risk registry to track risk mitigation activities		
Tier 3-Operations			
Validation of IT system components	Limited to compliance-level testing	System-wide quality assurance processes put into place	Full spectrum strategy to assure integrity of systems: use of embedded signatures, quarantining of suspect components, auditing of certificates of conformance
Software configuration management systems and hardware certificates of traceability	Compliance-level tracking	Attempts to maintain and audit completeness and accuracy of all product and component "pedigree" documents	Full-spectrum strategy to assure continuous visibility of software and hardware production/delivery cycle through RFID, digital locks, video surveillance, tracking portals
Supplier qualification and operational checks	Frequent purchases on gray market; limited due diligence over suppliers	Pre-qualification of suppliers; limited screening of carriers	Comprehensive sourcing strategy and use of only known suppliers and trusted carriers
Protocols to deal with counterfeit parts	Case-by-case response to suspect parts	Built-in contract mechanisms to return suspect parts to suppliers	Pre-established relationships with customs authorities and the FBI; standard operating procedures to remove suspect parts from the supply chain
	Recommendations For Maturity Phases 1 and 2: Reduce liability by transitioning to trusted contractors, suppliers, and carriers; reducing or eliminating gray-market purchases; and creating policies for reporting and disposing of suspect parts		

Please cite this article as: Boyson, S., Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation (2014), http://dx.doi.org/10.1016/j.technovation.2014.02.001

Appendix A

See Table A1.

References

Askville, ⟨http://askville.amazon.com/word-cyber-older-modern-meaning/AnswerViewer.do?requestId=4086267⟩ (accessed August 12, 2013).

Booz Allen Hamilton, 2009. Milestones of Cyber Security. (November) ⟨http://www.boozallen.com/media/file/milestones-of-cyber-security.pdf⟩.

Borg, S., 2010. Securing the Supply Chain for Electronic Equipment: A Strategy and Framework. Internet Security Alliance. ⟨http://www.whitehouse.gov/files/documents/cyber/ISA-Securing the Supply Chain for Electronic Equipment.pdf⟩. (last accessed November 9, 2013).

Boyson, S., Corsi, T., Dresner, M., Harrington, L., 1999. Logistics and the Extended Enterprise. John Wiley Inc./R.H. Smith School of Business, Hoboken, NJ.

Boyson, S., Corsi, T., Rossman, H., 2009. Building a Cyber Supply Chain Assurance Reference Model. (June) www.saic.com/news/resources/Cyber_Supply_Chain.pdf (last accessed November 9, 2013).

Boyson, S., Corsi, T., Rossman, H., Dorin, M., 2011. Assessing SCRM Capabilities and Perspectives of the IT Vendor Community: Toward a Cyber Supply Chain Code of Practice. University of Maryland Robert H. Smith School of Business and National Institute of Standards and Technology ⟨http://csrc.nist.gov/scrm/documents/umd_cyber_scrm_report.pdf⟩ (last accessed November 8, 2013).

Cole, E., Ring, S., 2005. Insider Threat: Protecting the Enterprise from Spying, Espionage, and Theft. Syngress Press, Amsterdam.

CSCMP (Council of Supply Chain Management Professionals). ⟨http://cscmp.org/about-us/supply-chain-management-definitions⟩.

Domenici, H., Bari, A., 2012. The Price of Cybersecurity: Big Investments, Small Improvements. Bloomberg Government. (January 31) www.bgov.com.

Deloitte Touche Tohmatsu, 2005. The Challenge of Complexity in Global Manufacturing: Trends in Supply Chain Management.

DHS, 2012. U.S. Department of Homeland Security, National Protection and Programs Directorate. Cybersecurity Insurance Workshop Readout Report. (November) p.8.

Ellison, R., Goodenough, J., Weinstock, C., Woody, C., 2010. Evaluating and Mitigating Software Supply Chain Security Risks. (May) ⟨http://www.sei.cmu.edu/library/abstracts/reports/10tn016.cfm⟩ (last accessed November 9, 2013).

Germain, R., Claycomb, C., Dröge, C., 2008. Supply chain variability, organizational structure & performance: the moderating effect of demand unpredictability. J. Oper. Manage. 26 (5), 557–570.

Goertzel, K., 2010. Supply chain risk management and the software supply chain. In: Presentation at OWASP AppSec DC Conference. (November) ⟨https://www.owasp.org/images/7/77/BoozAllen-AppSecDC2010-sw_scrm.pdf⟩ (last accessed November 10, 2013).

Harrington, L., Boyson, S., Corsi, T., 2010. X-SCM: The New Science of X-treme Supply Chain Management. Routledge Press, New York.

Heywood, G., 2006. PricewaterhouseCoopers, Personal Interview (September).

Howard, L., 2013. Feds: Counterfeit Submarine Parts Shipped to Groton. The Day, New London, CT, July 16. ⟨http://theday.com/article/20130716/NWS09/130719772/1017⟩.

InfoSecurity Europe, 2010. Dell PowerEdge Servers Shipping with Onboard Malware? (July 22) ⟨http://www.infosecurity-magazine.com/view/11143/dell-poweredge-servers-shipping-with-onboard-malware-/⟩ (last accessed November 8, 2013).

Institute of Medicine, 2009. Initial National Priorities for Comparative Effectiveness Research, Report Brief (June) p.1, ⟨http://www.hrsonline.org/Policy/LegislationTakeAction/upload/CER-report-brief-6-22-09.pdf⟩ (accessed February 27, 2012).

Kunert, P., 2011. Leader of CISCO Counterfeit Ring Jailed for 60 Months. The A Channel. (September 12) ⟨http://www.channelregister.co.uk/2011/09/12/cisco_counterfeit_ring⟩ (last accessed Nov. 8, 2013).

Manufacturing.net, 2012. History of Supply Chain Management. ⟨http://www.manufacturing.net/articles/2012/05/history-of-logistics-and-supply-chain-management⟩.

McMillan, R. 2007. Seagate Ships Virus-laden Hard Drives. (November 13). ⟨http://www.pcworld.com/article/139576/article.html⟩ (last accessed November 10, 2013).

McMillan, R., 2010. Woman Helped Sell Fake Chips to U.S. Military. PCWorld. (November 23) ⟨http://www.pcworld.com/article/211428/article.html⟩.

National Public Radio, 2011. China's Cyber Threat a High-Stakes Spy Game. (November 27) ⟨http://www.npr.org/2011/11/27/142828055/chinas-cyber-threat-a-high-stakes-spy-game⟩ (last accessed November 8, 2013).

NSS Labs, 2013. Invitation to "Securing the Future" Summit (December).

NIST, 2013. Discussion Draft of the Preliminary Cybersecurity Framework. National Institute of Security and Technology. (August 28) ⟨http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf⟩ (last accessed December 8, 2013).

Oltsik, J., Gahm, J., McKnight, J., 2010. Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure. (November 28) ⟨http://www.enterprisestrategygroup.com/2010/11/cyber-supply-chain-security-research-report/⟩. (last accessed November 10, 2013).

Open Group, 2011. U.S. Resilience Project. Cyber Supply Chain Risks, Strategies, and Best Practices, Chapter 4 ⟨http://www.usresilienceproject.org/workshop/participants/pdfs/USRP_Resources_Chapter_4_022812.pdf⟩ (last accessed November 10, 2013).

PCAST, 2013. Immediate Opportunities for Strengthening the Nation's Cybersecurity. President's Council of Advisors on Science and Technology. (November) ⟨http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf⟩.

PRTM, 2006. SCOR Metrics Powerpoint Presentation. (September).

Ramage, M., 2009. Norbert and Gregory. Inf. Commun. Soc. 12 (5), 735–749.

R. H. Smith School of Business, 2012. The ICT SCRM Community Framework Development Project. Robert H. Smith School of Business Supply Chain Management Center. University of Maryland; and National Institute of Security and Technology (NIST) ⟨http://csrc.nist.gov/scrm/documents/umd_ict_scrm_initiatives-report2-1.pdf⟩.

SCRLC, 2013. Supply Chain Risk Management Maturity Model. Supply Chain Risk Leadership Council. (May) ⟨http://www.scrlc.com⟩ (last accessed November 8, 2013).

SEC, 2012. Author Interviews with Securities and Exchange Commission Staff (March, 2012).

Simpson, S.,(Ed.), 2010. Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain. Software Assurance Forum for Excellence in Code. (June 14) ⟨http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf⟩ (last accessed November 10, 2013).

Storch, T., 2011. Toward a Trusted Supply Chain: A Risk-Based Approach to Managing Software Integrity. Microsoft Corp. (July 26) ⟨http://www.microsoft.com/download/en/details.aspx?id=26828⟩ (last accessed November 10, 2013).

Symantec, 2013a. 2013 Internet Security Threat Report, vol. 18. ⟨http://www.symantec.com/security_response/publications/threatreport.jsp⟩.

Symantec, 2013b. Symantec Internet Security Threat Report Reveals Increase in Cyberespionage—Including Threefold Increase in Small Business Attacks. News Release, April 16. ⟨http://www.symantec.com/about/news/release/article.jsp?prid=20130415_01⟩ (last accessed November 8, 2013).

Treadway Commission, 2004. Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Framework Executive Summary, p.2. ⟨www.coso.org/documents/coso_erm_executivesummary.pdf⟩.

WhatIs.com. TechTarget. ⟨http://whatis.techtarget.com/definition/cybersecurity⟩.

PwC, 2012. Cyber Security M&A: Decoding deals in the global Cyber Security industry. (November) ⟨http://www.pwc.com/gx/en/aerospace-defence/publications/cyber-security-mergers-and-acquisitions.jhtml⟩ (last accessed November 8, 2013).

Please cite this article as: Boyson, S., Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation (2014), http://dx.doi.org/10.1016/j.technovation.2014.02.001