CyberCore TECHNOLOGIES

Supply Chain Risk Management – Background Information

CyberCore Technologies

Version 1.3

Abstract: One of the key challenges for Government organizations is managing risks associated with the supply chain. Based on academic, Government, and industry research, CyberCore presents an overview of Supply Chain Risk Management and highlights key academic and Government milestones/ publications.

Introduction

Today's e-world has led to an information explosion from the countless data sources that appear on a daily basis. Supply chain risk management (SCRM) is an area that has recently been receiving a great deal of interest from Government, academics, and practitioners. SCRM is believed to be in an emerging and promising new field (Sodhi et al., 2012) but has a number of open-ended boundaries in its scope. Various authors have carried out a literature review on SCRM at various stages over the last ten years (e.g. Juttner et al., 2003; Vanany et al., 2009; Rao and Goldsby, 2009) who provide a good platform for practitioners trying to make sense of the on-going research and identify the current state-of-art.

However, narrative literature reviews are believed to lack thoroughness and rigor (Tranfield et al., 2003) especially related to Government direction and industry experience. Since 2000, hundreds of articles, conference papers, Government publications, journal, and research papers have investigated SCRM using differing terms: risk management, SCM, risk, disruption, vulnerability, uncertainty, and many others. CyberCore has performed an exhaustive literature search discovering approximately 140 quality papers, 100 Government publications, and 82 research articles across five (5) databases and 39 journals related to SCRM. After reviewing all SCRM literature, CyberCore has identified several significant SCRM milestones and publications among academia (see Table 1), industry, and the Government (see Figure 1).

The following sections provide an overview of SCRM in terms of the background, current advances in research, and related Government-directed publications. With a triune focus on academic research, Government publications, and industry experience, this paper presents analysis of commonalities and divergent aspects of SCRM. Finally, this paper presents recommended SCRM requirements based on all three focus elements for incorporation into the GREENWAY procurement.

Background Research

Managing risks in the modern environment is becoming increasingly challenging (Christopher and Lee, 2004), primarily because of uncertainties in supply and demand, global outsourcing and short product life cycles. Risk in this context can be defined as the potential for unwanted negative consequences that arise from an event or activity (Rowe, 1980). Today, the global business environment is influenced by financial instability, just-in-time outsourcing, company mergers, new technologies, e-business, shorter

time-to-market, etc., thus forcing organizations to adopt new ways of doing business (Stefanovic et al., 2009). However, today's leaner, just-in-time globalized supply chains (SC) are more vulnerable than ever before due to operational and external (natural and man-made) disruptions. Vulnerability is defined as an exposure to serious disturbance arising from risks within the SC as well as risks external to the SC (Christopher and Peck, 2004).

SC risk can be broadly defined as an exposure to an event which causes disruption, thus affecting the efficient management of the SC network. Risk management is becoming an integral part of a holistic SCM design (Christopher and Lee, 2004). There is diverse classification of SC risks found in the literature. Risk itself can be termed as disruption, vulnerability, uncertainty, disaster, peril and hazard. Academic literature within the domain of SC has sought to differentiate between the various forms by focusing on the availability of information and the intensity of these events. Hence, this can range from the completely unknown to the completely known serious and immediate danger.

Vorst and Beulens (2002) define uncertainty as a situation for the SC where the decision maker lacks information about the SC network and the environment; and hence is unable to predict the impact of the event on SC behavior. Although risk and uncertainty are interchangeably used in SC literature, according to Knight (1921) uncertainty is immeasurable as it lacks complete certainty and has more than one possibility. On the other hand, risk is measurable as it is an outcome of uncertainty with some of possibilities involving loss or other undesirable outcomes (Hubbard, 2007, 2009). According to Williams et al. (2008) SC security is a subcomponent of overall risk management strategy within the organization.

While there are many varying definitions of SC Risk (SCR) within Government, academia, and industry, Congress, in 2013 has defined SCR as:

> "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use or operation of such systems."

This definition has the most commonality among Government, academia, and industry, further enhancing the *disruption* element of supply chain risk.

Key Academic Research Contributions

Since 2000, SCRM has been evolved through the contributions of several academic and practitioner researchers. Table 1 below identifies key research, contributions, and findings since 2000.

Table 1. Past literature reviews in SCRM: research method and finding.

Author(s)	*Research Methodology*	*Key Findings/ Contributions*
Juttner et al. (2003)	Literature survey findings are compared with results from exploratory semi-structured interviews, focus groups are undertaken to discover practitioners' perceptions.	Used four basic constructs to develop the concept: sources of risk, adverse consequences of risk, drivers of risk and mitigation strategies. Identified normative issues for future research in SCRM focusing need of empirically grounded research.
Khan and Burnes (2007)	Literature review of broad literature on risk and precise literature on supply chain	Emphasize on the need to devise a robust and well-grounded models. Indepth empirical research is needed to identify adaptable tools in managing

	risk	supply chain risk by incorporate risk management tools and techniques from other disciplines of research.
Williams et al. (2008)	Through review of the literature on supply chain security (SCS) from academic publications, white papers, and practitioner periodicals.	Provides good empirical findings and theory building through categorization of literature on SCS. Quantitative assessments are needed to better understand of SCRM. SCS can lead to improved organizational performance.
Vanany et al. (2009)	Through review of journal publications from 2000 to 2007 with help of classifications into several typologies.	RFID and ERP will become important part of SCRM. Use of IT for visibility, collaborative risk management strategies for making supply chains robust is lacking.
Natarajarathinam et al. (2009)	Review of academic peer-reviewed journals and case publications in supply chain management literature.	Much of the research is focused on external sources and proactive approaches to crisis in supply chains. Recovery planning and scales for crisis management needs attention.
Rao and Goldsby (2009)	Review of the literature on supply chain risk and synthesis of the broader domain of risk management.	Provides a typology of risks classified broadly as environmental, industry and organizational risks based on identified variables from systematic key research findings in SCRM. SCRM is an area in need of further substantive investigation.
Tang and Musa (2010)	Literature survey and citation/co citation analysis using academic database to disclose SCRM development.	Need of an integrated view of SCRM is growing strongly. Requirement of analysis tools for proactively managing risks. Use of quantitative modeling in risk management is lacking and their lies a huge potential in developing quantitative models to make hard decisions SCRM

Throughout the past 14 years, researchers and practitioners have evolved varying models of SCRM and risk assessment. NIST's ICT SCRM Risk Assessment Methodology, initially released in April 2013, is the most comprehensive and mature SCRM model.

The steps in this risk management methodology – Frame, Assess, Respond, and Monitor - are not inherently sequential in nature. The steps are performed in different ways, depending on the particular tier (Organization, Mission/ Business, and Information Systems) where the step is applied on prior activities related to each of the steps. Organizations have significant flexibility in how the risk management steps are performed (e.g., sequence, degree of rigor, formality, and thoroughness of application) and in how the results of each step are captured and shared—both internally and externally. What is consistent is that the outputs or post conditions from a particular risk management step directly impact one or more of the other risk management steps in the risk management process.

Frame is the step that establishes context for ICT SCRM in all three tiers. The scope and structure of the organizational ICT supply chain landscape, the overall risk management strategy, as well as specific program/project or individual information system needs, are defined in this step. The data and information collected during Frame provides inputs for scoping and fine-tuning ICT 737 SCRM activities in other risk management process steps throughout the three tiers.

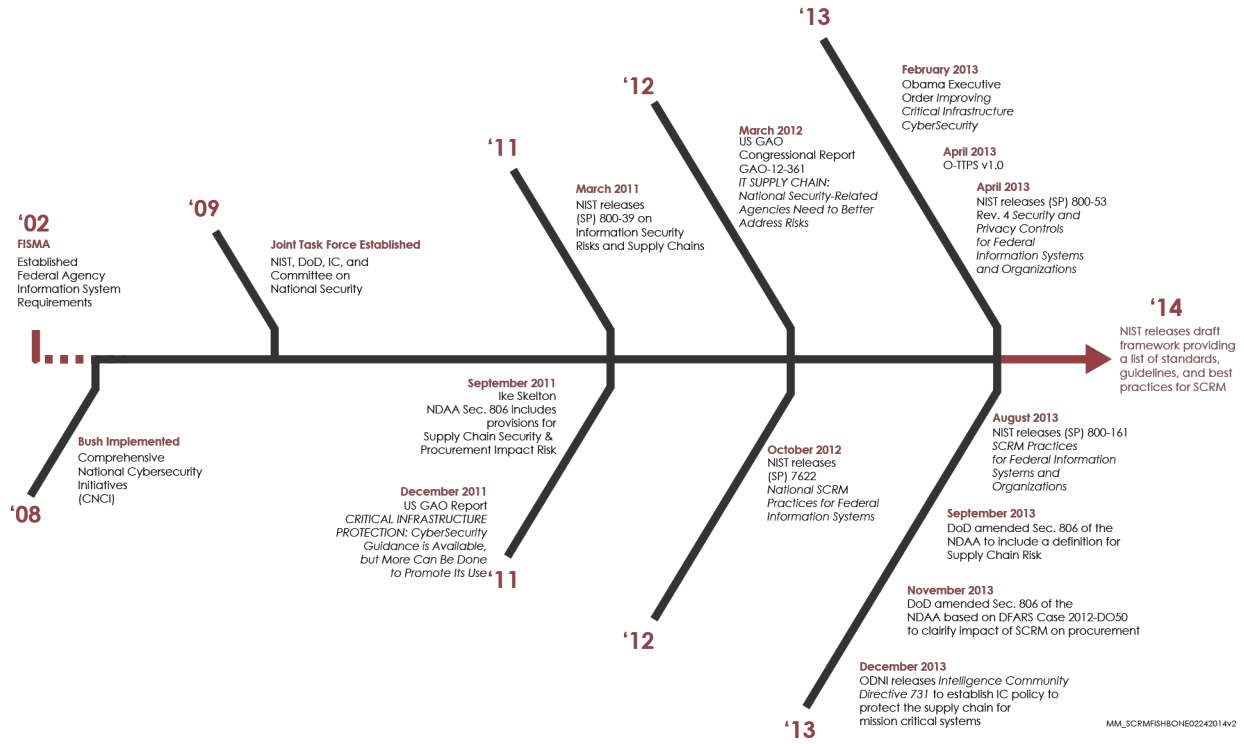
Assess is the step where all the collected data is used to conduct a risk assessment. A number of inputs are combined and analyzed to identify the likelihood and the impact of an ICT supply chain compromise, including criticality, threat, and vulnerability analysis results; stakeholder knowledge; and policy, constraints, and requirements.

Respond is the step in which the individuals conducting risk assessment will communicate the assessment results, proposed mitigation/controls options, and the corresponding risk posture for each proposed option to the decision makers. This information should be presented in a manner appropriate to inform and guide risk-based decisions. This will allow decision makers to finalize appropriate risk response based on the set of options along with the corresponding risk factors for choosing the various options.

Monitor is the step in which the project/ program is routinely evaluated to maintain or adjust its risk posture. Changes to organization, mission/business, or operations can directly impact the risk posture of an individual project/program and of the organization's ICT supply chain processes. Monitor provides the mechanism for tracking such changes and ensuring they are appropriately assessed for impact (in Assess). Organizations should integrate ICT SCRM into existing continuous monitoring programs. In case a Continuous Monitoring program does not exist, ICT SCRM can serve as a catalyst for establishment of a more comprehensive continuous monitoring program.

Government SCRM Milestone & Publication Timeline

After reviewing SCRM literature, CyberCore has identified key Government milestones and publications (see Figure 1), which are occurring at an increasingly rapid pace, further emphasizing the importance of SCRM.



The Federal Information Security Management Act of 2002 (FISMA) established federal agency information security program requirements that support the effectiveness of information security

controls over information resources that support federal operations and assets. Its framework creates a cycle of risk management activities necessary for an effective security program. FISMA requires every federal agency to establish an information security program. Additionally, the act assigns responsibility to NIST to provide standards and guidelines to agencies on information security

In 2008, the Bush administration began to implement a series of initiatives, referred to as the Comprehensive National Cybersecurity Initiative (CNCI), aimed primarily at improving CyberSecurity within the federal government. Specifically, CNCI is composed of a set of 12 initiatives with the objective of safeguarding federal executive branch information systems by reducing potential vulnerabilities; protecting against intrusion attempts; and anticipating future threats through defensive, offensive, educational, research and development, and counterintelligence efforts.

The President's Comprehensive National Cyber Security Initiative (CNCI) 11 is co-chaired by the Department of Defense (DoD) and the Department of Homeland Security (DHS). This initiative seeks to provide federal departments and agencies with a well-understood toolkit of technical and intelligence resources to manage supply chain risk to a level commensurate with the criticality of information systems or networks. Through the work of CNCI 11, an interagency group evaluated a number of source documents and developed an initial set of supply chain assurance methods/ techniques or practices that cover the system development life cycle (SDLC) as part of a government-wide SCRM solution. The initial public draft of this document was developed using these practices as a foundation. Draft NIST SP 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations,* and *The 25 Point Implementation Plan to Reform Federal Information Technology Management* from the U.S Chief Information Officer (CIO) are also foundational to the development of CNCI 11.

In 2009, an interagency partnership was formed among NIST, the Department of Defense, the Intelligence Community, and the Committee on National Security Systems to provide security controls for Federal Information Systems.

In March 2011, NIST published SP 800-39, which provides an approach for organization-wide management of information security risk, including those related to supply chains. Among other things, the publication states that risk management requires organizations to monitor risk on an ongoing basis as part of a comprehensive risk management program. Monitoring programs can aid agency officials in oversight of currently implemented security controls. To support risk monitoring, organizations are expected to describe how compliance with security requirements is verified and how the organization will determine the effectiveness of risk response activities.

In addition, the Ike Skelton National Defense Authorization Act (NDAA) for Fiscal Year 2011 included provisions related to supply chain security. Specifically, Section 806 authorizes the Secretaries of Defense, the Army, the Navy, and the Air Force to exclude a contractor from specified types of procurements on the basis of a determination of significant supply chain risk to a covered system.

In September 2011, the DoD released the *National Defense Authorization Act: Requirements for Information Relating to Supply Chain Risk* which allows the DoD to consider the impact of supply chain risk in specified types of procurements related to national security systems. This act was amended in September 2013.

In December 2011, the United States Government Accountability Office (GAO) issued a report titled "CRITICAL INFRASTRUCTURE PROTECTION: CyberSecurity Guidance Is Available, but More Can Be Done to Promote Its Use." In its report, GAO found similarities in CyberSecurity guidance across sectors and recommended promoting existing guidance to assist individual entities within a sector in "identifying the guidance that is most applicable and effective in improving their security posture."

In March 2012, the United States Government Accountability Office (GAO) issued Report GAO-12-361 to Congressional Requesters titled "IT SUPPLY CHAIN: National Security-Related Agencies Need to Better Address Risks." GAO discovered that reliance on a global supply chain introduces multiple risks to federal information systems. These risks include threats posed by actors—such as foreign intelligence services or counterfeiters—who may exploit vulnerabilities in the supply chain and thus compromise the confidentiality, integrity, or availability of an end system and the information it contains. This in turn can adversely affect an agency's ability to effectively carry out its mission. Each of the key threats presented in the table below could create an unacceptable risk to federal agencies.

Threats to the IT Supply Chain
Installation of malicious logic on hardware or software
Installation of counterfeit hardware or software
Failure or disruption in the production or distribution of a critical product or service
Reliance upon a malicious or unqualified service-provider for the performance of technical services
Installation of unintentional vulnerabilities on hardware or software

Although four national security-related departments—the Departments of Energy, Homeland Security, Justice, and Defense—have acknowledged these threats, two of the departments—Energy and Homeland Security—have not yet defined supply chain protection measures for department information systems and are not in a position to have implementing procedures or monitoring capabilities to verify compliance with and effectiveness of any such measures. Justice has identified supply chain protection measures, but has not developed procedures for implementing or monitoring compliance with and effectiveness of these measures. Until comprehensive policies, procedures, and monitoring capabilities are developed, documented, and implemented, it is more likely that these national security-related departments will rely on security measures that are inadequate, ineffective, or inefficient to manage emergent information technology supply chain risks. In contrast, Defense has made greater progress through its incremental approach to supply chain risk management. The department has defined supply chain protection measures and procedures for implementing and monitoring these measures. The four national security-related departments also participate in government-wide efforts to address supply chain security, including the development of technical and policy tools and collaboration with the intelligence community.

Officials at the four departments stated that their respective agencies have not determined or tracked the extent to which their telecommunications networks contain foreign-developed equipment, software, or services. Federal agencies are not required to track this information, and officials from four components of the U.S. national security community believe that doing so would provide minimal security value relative to cost.

In October 2012, NIST released *Special Publication (SP) 7622*, *Notional Supply Chain Risk Management Practices for Federal Information Systems*. Special Publication 7622 organizes specific Information and Communication Technology (ICT) SCRM practices into those targeting federal department and agency acquirers, developers, integrators of custom-built information systems, and COTS suppliers (including open source software). These practices are recommended to be used for those information systems categorized at the Federal Information Processing Standards (FIPS) 199 high-impact level. However, it is recommended that Federal agency acquirers select and tailor the acquirer practices in the document based on the suitability for a specific application or acquisition and combined impact on the performance, cost, and schedule. Federal agency acquirers may use the integrator and the supplier

practices in the document as examples of reasonable expectations that can be communicated to the integrators and suppliers.

SP 7622 supports the expanded set of ICT SCRM practices in draft NIST SP 800-53 Revision 4. Because the two documents are developed in parallel, it is not possible to reconcile the specific controls and practices at this point in time. It is anticipated that the future special publication addressing ICT SCRM will be fully harmonized and consistent with draft NIST SP 800-53 Revision 4, or subsequent revisions, depending on the timing of the publication.

On February 13, 2013, President Obama issued the Executive Order "Improving Critical Infrastructure CyberSecurity." The Executive Order tasks the Secretary of Commerce to direct the Director of the National Institute of Standards and Technology (NIST) to lead the development of a framework to reduce cyber risks to critical infrastructure. Consistent with existing NIST authorities, the Executive Order requires NIST to engage in an open public review and comment period. The goals of the Framework development process will be: (i) to identify existing CyberSecurity standards, guidelines, frameworks, and best practices that are applicable to increase the security of critical infrastructure sectors and other interested entities; (ii) to specify high-priority gaps for which new or revised standards are needed; and (iii) to collaboratively develop action plans by which these gaps can be addressed. It is contemplated that the development process will have requisite stages to allow for continuing engagement with the owners and operators, or critical infrastructure, and other industry, academic, and government stakeholders. NIST intends to issue a Request for Information (RFI) in the Federal Register to gather initial information on the many interrelated considerations, challenges, and efforts needed to develop the Framework.

In April 2013, The Open Group released *Open Trusted Technology Provider Standard (O-TTPS) Version 1.0: Mitigating Maliciously Tainted and Counterfeit Products*. The O-TTPS is an open standard containing a set of guidelines that when properly adhered to have been shown to enhance the security of the global supply chain and the integrity of COTS ICT products. It provides a set of guidelines, requirements, and recommendations that help assure against maliciously tainted and counterfeit products throughout the COTS ICT product life cycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.

Using the guidelines documented in the Framework as a basis, the Open Group Trusted Technology Forum (OTTF) is taking a phased approach and staging O-TTPS releases over time. This staging will consist of standards that focus on mitigating specific COTS ICT risks from emerging threats. As threats change or market needs evolve, the OTTF intends to update the O-TTPS (Standard) by releasing addenda to address specific threats or market needs.

The Standard is aimed at enhancing the integrity of COTS ICT products and helping customers to manage sourcing risk. The authors recognize the value that it can bring to Government and commercial customers worldwide, particularly those who adopt procurement and sourcing strategies that reward those vendors who follow the O-TTPS best practice requirements and recommendations.

The two major threats that acquirers face today in their COTS ICT procurements, as addressed in the Standard, are:

1. *Maliciously tainted product* – the product is produced by the provider and is acquired through a provider's authorized channel, but has been tampered with maliciously.

2. *Counterfeit product* – the product is produced other than by, or for, the provider, or is supplied to the provider by other than a provider's authorized channel and is presented as being legitimate even though it is not.

On April 30, 2013, NIST announced the final release of *Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*. Special Publication 800-53, Revision 4, represents the most comprehensive update to the security controls catalog since its inception in 2005. The publication was developed by NIST, the Department of Defense, the Intelligence Community, and the Committee on National Security Systems as part of the Joint Task Force, an interagency partnership formed in 2009. This update was motivated principally by the expanding threat space—characterized by the increasing sophistication of cyber attacks and the operations tempo of adversaries (i.e., the frequency of such attacks, the professionalism of the attackers, and the persistence of targeting by attackers). State-of-the-practice security controls and control enhancements have been developed and integrated into the catalog addressing such areas as: mobile and cloud computing; applications security; trustworthiness, assurance, and resiliency of information systems; insider threat; supply chain security; and the advanced persistent threat. In addition, Special Publication 800-53 has been expanded to include eight new families of privacy controls based on the internationally accepted Fair Information Practice Principles.

Special Publication 800-53, Revision 4, provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber attacks and other threats. This "Build It Right" strategy is coupled with a variety of security controls for "Continuous Monitoring" to give organizations near real-time information that is essential for senior leaders making ongoing *risk-based* decisions affecting their critical missions and business functions.

In August 2013, NIST releases *Special Publication (SP) 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. Special Publication 800-161, provides guidance to federal departments and agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels in their organizations. NIST SP 800-161 integrates ICT supply chain risk management (SCRM) into federal agency enterprise risk management activities by applying a multi-tiered SCRM-specific approach, including supply chain risk assessments and supply chain risk mitigation activities and guidance.

In September 2013, the DoD amended the *National Defense Authorization Act: Requirements for Information Relating to Supply Chain Risk* to include section 806. Section 806 defines supply chain risk as “the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system. Section 806 was further amended on November 18, 2013.

On November 18, 2013, the DoD amended Section 806 of the National Defense Authorization Act: Requirements for Information Relating to Supply Chain Risk to address comments identified by DFARS Case 2012-D050, clarifying DoD’s ability to consider the impact of supply chain risk in specified types of procurements related to national security systems.

On December 7, 2013, the Office of the Director of National Intelligence (ODNI) released Intelligence Community Directive 731 which establishes IC policy to protect the supply chain as it relates to the lifecycle of mission-critical products, materials, and services used by the IC through the identification, assessment, and mitigation of threats. This Directive defines the role of supply chain risk management within the IC and is intended to complement other supply chain risk management programs throughout the U.S. Government.

On March 14, 2014, DoD reissued and renamed DoD Directive 8500.01E as a DoD Instruction (DoDI) to establish a DoD cybersecurity program to protect and defend DoD information and information

technology. This Instruction establishes the positions of DoD principal authorizing official (PAO), formerly known as principal accrediting authority, and the DoD Senior Information Security Officer (SISO), formerly known as the Senior Information Assurance Officer, and continues the DoD Information Security Risk Management Committee (DoD ISRMC), formerly known as the Defense Information Systems Network (DISN)/ Global Information Grid (GIG) Flag Panel).

In early 2014, NIST intends to publish for additional comment a draft Framework that clearly outlines areas of focus and provides preliminary lists of standards, guidelines, and best practices that fall within their initial mandate. The draft will also include initial conclusions for additional public comment. The draft Framework will build on NIST's ongoing work with CyberSecurity standards and guidelines for the Smart Grid, Identity Management, Federal Information Security Management Act (FISMA) implementation, the Electricity Subsector CyberSecurity Capability Maturity Model, and related projects.

Conclusion

Since 2000, Government, industry, and academia have placed increasing importance on SCRM and the impact risks have to the supply chain. The frequency of publications has increased significantly since 2008, further emphasizing the growing importance of SCRM. Additional work has been accomplished to both define SCRM and create a working operational model to manage supply chain risks. Finally, recent Government publications have begun to define SCRM requirements and evaluation criteria for national security acquisitions.

References

Christopher, M. and Lee, H. (2004), "Mitigating supply chain risk through improved confidence", International Journal of Physical Distribution and Logistics Management, Vol. 34 No. 5, pp. 388-96.

Christopher, M. and Peck, H. (2004), "Building the resilient supply chain", The International Journal of Logistics Management, Vol. 15 No. 2, pp. 1-14.

Denyer, D. and Tranfield, D. (2009), "Producing a systematic review", in Buchanan, D. and Bryman, A. (Eds), The Sage Handbook of Organizational Research Methods, Sage Publications Ltd, London, pp. 671-87.

Hubbard, D. (2007), How to Measure Anything: Finding the Value of Intangibles in Business, John Wiley and Sons, Hoboken, NJ, p. 46.

Hubbard, D. (2009), The Failure of Risk Management: Why It's Broken and How to Fix It, John Wiley and Sons, Hoboken, NJ, p. 211.

Juttner, U., Peck, H. and Christopher, M. (2003), "Supply chain risk management: outlining an agenda for future research", International Journal of Logistics Research and Applications, Vol. 6 No. 4, pp. 197-210.

Khan, O. and Burnes, B. (2007), "Risk and supply chain management: creating a research agenda", The International Journal of Logistics Management, Vol. 18 No. 2, pp. 197-216.

Knight, F.H. (1921), Risk, Uncertainty and Profit (Hart, Schaffner, and Marx Prize Essays, No. 31), Houghton Mifflin, Boston, MA and New York, NY, p. 19.

M. S. Sodhi, B. G. Son and C. S. Tang, "Researcher's Perspective on Supply Risk Management," *Productions and Operations Management*, Vol. 21, No. 1. 2012, pp. 1-13.

Natarajarathinam, M., Capar, I. and Narayanan, A. (2009), "Managing supply chains in times of crisis: a review of literature and insights", International Journal of Physical Distribution and Logistics Management, Vol. 39 No. 7, pp. 535-73.

Rao, S. and Goldsby, T.J. (2009), "Supply chain risks: a review and typology", The International Journal of Logistics Management, Vol. 20 No. 1, pp. 97-123.

Rousseau, D.M., Manning, J. and Denyer, D. (2008), "Evidence in management and organizational science: assembling the field's full weight of scientific knowledge through syntheses", The Academy of Management Annals, Vol. 2 No. 1, pp. 475-515.

Rowe, W.D. (1980), "Risk assessment: approaches and methods", in Conrad, J. (Ed.), Society, Technology and Risk Assessment, Academic Press, London, p. 343.

Stefanovic, D., Stefanovic, N. and Radenkovic, B. (2009), "Supply network modelling and simulation methodology", SimulationModelling Practice and Theory, Vol. 17 No. 4, pp. 743-66.

Tang, O. and Musa, S. (2010), "Identifying risk issues and research advancements in supply chain risk management", International Journal of Production Economics, Vol. 133 No. 1, pp. 25-34.

Tranfield, D., Denyer, D. and Smart, P. (2003), "Towards a methodology for developing evidence informed management knowledge by means of systematic review", British Journal of Management, Vol. 14 No. 3, pp. 207-22.

Vanany, I., Zailani, S. and Pujawan, N. (2009), "Supply chain risk management: literature review and future research", Int. Journal of Information Systems and Supply Chain Management, Vol. 2 No. 1, pp. 16-33.

Vorst, J.G.A.J. and Beulens, A.J.M. (2002), "Identifying sources of uncertainty to generate supply chain redesign strategies", International Journal of Physical Distribution and Logistics Management, Vol. 32 No. 6, pp. 409-30.

Williams, Z., Lueg, J.E. and LeMay, S.A. (2008), "Supply chain security: an overview and research agenda", The International Journal of Logistics Management, Vol. 19 No. 2, pp. 254-81.