Securing the Information and Communications Technology Global Supply Chain from Exploitation: Developing a Strategy for Education, Training, and Awareness

Elizabeth A. McDaniel
Institute for Defense Analyses, Alexandria, VA

emcdanie@ida.org

Abstract

Exploitation of the global Information and Communications Technology (ICT) supply chain is a growing security concern for government and industry. This paper frames the key elements of global ICT supply chain security and its importance to government as well as private sector companies, and the development of a comprehensive strategy for education, training, and awareness of the U.S. Department of Defense workforce - military, civilians, and contractors - about this crucial aspect of cybersecurity. The foundational elements of the strategy are collaboration among stakeholders to clarify confusing terminology; articulation of core messages regarding decision making about risk that will frame the curriculum; and establishment of a community of interest among defense and government organizations, and partnerships with industry, higher education institutions, and domestic and international professional and standards organizations.

Keywords. supply chain security, supply chain risk management, hardware assurance, software assurance

Introduction

The critical supply chains of government and industry are no longer simple and visible sets of links from raw materials to manufacturers to acquirers immune to outside threats. Supply chains for information and communications technologies (ICT)-enabled components, like other critical supply chains, have become more complex and dynamic, making it imperative to assure that the products delivered for the component, system, and mission do what they are intended to do, and nothing else. The U.S. Department of Defense (DoD) and others in the federal government view this growing threat to the critical ICT supply chain as an emerging national security issue that deserves more attention across the enterprise.

Global ICT supply chain risk management is a new aspect of cybersecurity identified as a priority in the Comprehensive National Cybersecurity Initiative (2009) as Initiative 11: "Develop a multi-pronged approach to global supply chain risk management." Additionally, Initiative 8: "Expand cyber education" led to the creation of the National Initiative for Cybersecurity Education (NICE) (2009) and its National Cybersecurity Workforce Framework (2012) that defines specialty areas; knowledges, skills, and abilities (KSAs); and competencies. Global ICT supply chain risk management cuts across many of the framework's specialty areas and the workforce requirements for ICT supply chain risk management are found in the tasks, KSAs, and competencies of each specialty area. This paper frames the key elements of global ICT supply chain security and its importance to government as well as private sector companies. It also discusses the foundations of an education, training, and awareness (ETA) effort for the DoD workforce, where none currently exist.

A supply chain is defined as the set of suppliers that contribute to the content of a product or system (both hardware and software) or that have the opportunity to modify its content (Ellison & Woody, 2010). Supply chain risk management is the process for managing supply chain risk by identifying critical systems, processes, and components; vulnerabilities; and threats throughout the supply chain, and developing mitigation strategies to combat those threats. According to the U.S. *National Strategy for Global Supply Chain Security* (January 2012), global supply chain systems rely upon an interconnected web of transportation infrastructure and pathways, information technology, and cyber and energy networks (p. 2). "The supply chain is now recognized as a major cyber threat affecting development and operation of computer systems and not just a threat to the transportation of material and goods from supplier to purchaser" (Filsinger, Fast, Wolf, Payne, & Anderson, 2012, p. 9). Private sector companies are increasingly concerned about malicious tampering of software and hardware and counterfeits that lead to loss of their intellectual property, interfere with the successful performance of their products, and potentially damage their brands and reputations.

The term "supply chain risk management" was selected by policy makers to describe this new aspect of cybersecurity; however, the term has different meanings in other communities. The term commonly applies to the efficiency and logistical aspects of the supply chain, not the integrity of ICT or the risks associated with its exploitation. For this new national cyber security concern, the ETA effort, and this paper, the topic is managing the taking of risks associated with global ICT supply chain exploitation with a focus on product integrity and its significance to the design, systems engineering, and sustainment phases of the system life cycle.

Statement of the Problem: Responding to the Global ICT Supply Chain Security Threats

"Federal IT systems are increasingly at risk of both intentional and unintentional supply chain compromise due to the growing sophistication of information and communications technologies (ICT) and the growing speed and scale of a complex, distributed global supply chain" (Boyens, Paulsen, Bartol, Moorthy, & Shankles, 2012, p. 1). Individuals and organizations, including malicious actors who touch products, can affect the management or operations of companies that may result in compromise to the information system, organization, or Nation (p. 7). The four drivers often identified as contributing to the increased risks associated with the global supply chain are dependencies on ICT, globalization, commercialization, and financial complexities. In our interconnected, automated electronic age we have become *dependent on ICT* to communicate and to operate almost everything, including the supply chain itself. As a result our missions are increasingly at risk from adversaries who seek to interfere with the performance of ICT-enabled systems for their own purposes. *Globalization* has increasingly compromised U.S. supply chain immunity, and communications, command, and control technologies have become inextricably interwoven with those of every nation, both friendly and hostile to U.S. interests (CACI International, Inc. & United States Naval Institute, 2010, p. 2). Globalization allows companies the benefit of purchasing the least expensive products while taking advantage of global talent and business practices. Twenty years ago most of the U.S. government's ICT needs were supported with government-off-the-shelf (GOTS) products, but now the government primarily buys commercialoff-the-shelf (COTS) products for its systems and missions. The advantage of *commercialization* for both the government and the private sector is that components are cheaper because they are not custom-built; the disadvantage is that components are more vulnerable and might be flawed or counterfeit, or might contain malicious elements. The integrity of purchased components may be critical depending on whether they end up in a mobile phone or a billion dollar aircraft. Many COTS products, micro-electronic chips, printers, and software applications, for example, are made by companies either operating in other countries or contracting with companies that do. Adding to the challenge are the *financial complexities* that characterize the global and commercialized business world today. The dynamic partnerships and alliances, mergers and acquisitions, reliance on system integrators, and assembly of components from multiple suppliers, even for U.S. “name plate” companies, make it difficult to obtain visibility of one’s suppliers’ suppliers, and so forth, especially when they may change often. The lack of visibility and traceability increases the risk of not being able to detect and remediate intentional and unintentional compromise that may be introduced through a variety of means, including counterfeit materials and malicious software (Boyens et al, 2012, p.6). The supply chain itself is ICT-enabled, and because of the knowledge that it contains regarding workflows, functions, reviews, review techniques, sampling and audit capabilities, and risk management controls, its processes must also be protected from disclosure and exploitation (CACI International, Inc. & United States Naval Institute, 2010).

Espionage, sabotage, and counterfeits in the global ICT supply chain constitute new threats to national security (Hoover, 2009). Responses are hampered by the lack of awareness of the significance of the threat, the immaturity of analysis and risk management processes, and the inadequacy of current tools and testing to detect of hardware and software anomalies. While awareness, training, and education are recognized as critical to advancing cybersecurity goals related to supply chain exploitation, curriculum development relies on having a fully articulated body of knowledge.

Criticality

The complexity of the global supply chains of components that end up in computers, airplanes, and IT systems can feel overwhelming at times, especially if one wishes to consider the provenance of all the components in them. But ignoring the risk is not a valid strategy for managing risk (Lynch, 2009). To narrow the scope of analysis and the investment of organizational resources, it is important to think about how the global supply chain can affect critical functions and priority systems in light of the mission. Criticality assessment in DoD is the process by which the critical functions, essential system operations, and components (hardware, software, and firmware) that implement those functions are identified and ranked in terms of priority. Mission-critical functions are those functions of a system that, if corrupted or disabled, would unacceptably degrade the system effectiveness in achieving the core mission for which it was designed (Baldwin, Popick, Miller, & Goodnight, 2011). Once identified through an end-to-end decomposition of the system, these critical components become the focus of future analyses of threats and vulnerabilities. Using a return-on-investment approach, the organization determines where to spend its resources in assessment and mitigation, and potentially in redesign.

Threats

The criticality analysis provides the foundation for assessing and prioritizing threats, vulnerabilities, and countermeasures. Once the critical mission functions, operations, and components are determined, the components are assessed for the known threats. Threat actors can use the supply chain to insert hardware or software containing malicious logic through tampering during the development and implementation of an information system (Villasenor, 2011). Malicious logic is hardware, firmware, or software that is intentionally included or inserted in a system for a harmful process…in order to take control of entire systems, and thereby read, modify, or delete sensitive information; disrupt operations; launch attacks against other organizations' systems; or destroy systems (United States Government Accountability Office, 2012). Hardware can be compromised by the introduction of malicious logic into circuits to cause unwanted system behaviors. Similarly, software can be compromised with the addition of unwanted code, scripts, active content, or other software to create or disrupt computer operations, collect sensitive information, or gain access to private computer systems. Unfortunately sophisticated actors are capable of compromising both hardware and software in ways that are not easily detectable with current testing and verification tools and techniques. As a result, the end user is left to determine if the supplied hardware and software components can be trusted to perform only those functions defined in the original specifications. Security threats to the global, distributed, dynamic, and complex ICT supply chains are real, but documentation is not widely available.

Criminals and unethical companies who want to make fast and easy money sell counterfeit components (KPMG, 2005). They manufacture, label, and package products that retailers knowingly or unknowingly pass off as genuine, and that sometimes end up in critical systems. These counterfeit products may fail when they are expected to perform because of poor quality, or worse, sophisticated counterfeit products may do something that was not intended, such as surreptitiously relaying information back to their source, destroying data, taking over controls, or degrading missions. Counterfeits manufactured just to make money tend to be easier to detect than those with sophisticated embedded capabilities that perform other as expected. Performance testing often reveals that the counterfeit products are substandard. The processes and tools for threat assessment are evolving. Assessment also seeks to discover the identity of suppliers of one's suppliers (and their suppliers down the chain) who operate in large and distributed webs that are dynamic and not transparent. These assessments inform designers and users of critical systems about the risk that is delivered to them through interconnected and networked components.

Vulnerabilities

Systems are more or less vulnerable to threats depending on the design and flaws of the products or systems in which they are inserted. By analogy, an outbreak of the flu might present a real threat; however if a person had a flu shot this season, he is less vulnerable to the threat. Vulnerability is an attribute or characteristic of a component that can be exploited by an external or internal agent (hacker or malicious insider) to achieve unauthorized privileges in the system or access to data or other system resources. Hardware and software components and the systems in which they are integrated have particular vulnerabilities in light of particular and general threats.

Systems, networks, and applications may be vulnerable to intentionally implanted logic (e.g., back doors, logic bombs, spyware) and unintentional vulnerabilities that are maliciously exploited (e.g., poor quality or fragile code). Vulnerabilities are assessed with respect to exposure and exploitability. An assessment of vulnerability seeks to identify opportunities for introducing and exploiting vulnerabilities; the risks associated with vulnerabilities of the critical components, functions, and systems; and the range of appropriate countermeasures and mitigations. The aim of IT(information technology) risk management is to minimize vulnerability by implementing managerial, operational, and technical controls in an efficient and effective manner, and in the event that IT security controls are not effective, to mitigate the negative consequences (Smith, Watson, Baker, & Polorski, 2007, p. 2600).

Mitigation of Risk

Risk is a measure of the likelihood that a threat will lead to a loss coupled with the magnitude of the loss (Alberts, Ellison, Dorofee, Woody, & Creel, 2011). Unfortunately most threats are unknown and most vulnerabilities are not recognized (Lynch, 2009). The level of impact from a threat is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure, modification, or destruction of information, or loss of information or information system availability (Joint Task Force Transformation Initiative Interagency Working Group, 2012, p. 11). Decision makers need to assess the risk associated with the potential impact of this threat and vulnerability in the context of the mission. They have opportunities to "buy down the risk" with mitigations and countermeasures, both general and specific, at several points along the life cycle of the system, in the context of use, in response to changes in suppliers, threats, and vulnerabilities, and the effectiveness of countermeasures. Mitigation of threats and countermeasures for vulnerabilities in response to suspected exploitations are costly in terms of schedule and budget if they call for redesign of the system, change of suppliers, or cancelation of programs that contain too much residual risk. It may be less expensive to design features for supply chain security into the system than to mitigate them at the point of operation.

From the perspective of risk reduction and return on investment for decisions across the life cycle, there are three types of mitigations: intelligence, technical, and business (Chan & Larsen, 2010). Early in the design phase security can be built in through architecture and the avoidance of certain system vulnerabilities that allow exploitations to occur. Good business practices that align with standards (e.g., IEEE and ISO) reduce vulnerabilities and gaps that allow exploitations. Checking for counterfeits or verifying the locations where and how components were manufactured and transported might be easier or less expensive than testing to affirm that a component that performs well does not have something hidden in it that will either make it stop working or allow it to work in a different way. Mitigating risks is an area of continuing research and testing by government, industry, and academia.

Managing the Taking of Risks

Not all risks will have a huge impact on the mission, and not all risks can be mitigated. A decision maker at every step in the life cycle of a system must assess the risks delivered from the decision makers earlier in the life cycle. This aggregated risk is compounded by the integration of individual components into systems and systems of systems. The consumer of this aggregated risk is typically the end user, who is normally the first decision maker in the life cycle of the system whose primary concern is performance, not cost and schedule. Project managers who delivered the system to the end user have been evaluated primarily on cost and schedule rather than performance. Performance in terms of product and system integrity needs to become a primary criterion, in balance with cost and schedule considerations. Adding product integrity as a performance criterion requires many changes, beginning with contract language, through organizational culture, all the way to personnel evaluation. Thinking through trade-off decisions among performance, cost, and schedule is fundamental to managing the taking of risks. Each mitigation or countermeasure must be evaluated in terms of schedule or budget implications, and analyzed for its return on investment (Chan & Larsen, 2010).

In supply chain risk management (SCRM), decision makers must be concerned with the acquisition, development, and operations of information systems and system-of-systems to meet cost, schedule, and performance requirements in today's environment populated by globalized suppliers and active adversaries (Komaroff, Patterson, Davidson, Mirsky, & Wassel, 2011). Ten best practices as articulated in *Notional Supply Chain Risk Management Practices for Federal Information Systems* (Boyens, et al., 2010, p. 27) cover the complete system development life cycle, if implemented in their entirety:

1. Uniquely Identify Supply Chain Elements, Processes, and Actors

2. Limit Access and Exposure within the Supply Chain

3. Establish and Maintain the Provenance of Elements, Processes, Tools, and Data

4. Share Information within Strict Limits

5. Perform SCRM Awareness and Training

6. Use Defensive Design for Systems, Elements, and Processes

7. Perform Continuous Integrator Review

8. Strengthen Delivery Mechanisms

9. Assure Sustainment Activities and Processes

10. Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle

The end user who assesses the risk delivered to him as unacceptable can attempt more mitigations to reduce the risk to an acceptable level. But this late in the process, mitigations are few and have high costs in terms of money and schedule. If the end user determines that the residual risk is unacceptable, he may decide not to go forward with the mission.

The Approach: A Strategy for Education, Training, and Awareness

ETA related to cybersecurity is well organized and is increasingly aligning with the National Cybersecurity Workforce Framework (2012), but ETA specific to global ICT supply chain security is hard to find. Convinced of the risks associated with this new security threat, the U.S. government is sponsoring an ETA effort focused on the security of the global ICT supply chain. Developing the strategy for ETA begins with determining consistent and meaningful terminology, core content that is relevant to various audiences of leaders, decision makers, and specialists, as well as those in training to assume their roles in various organizations. DoD officials established a roundtable of DoD organizational representatives and researchers to create and share a body of knowledge while policies and processes are developed, mitigations are researched and assessed, and component testing matures. Although the ETA strategy is initially focusing on DoD, the strategy is keeping the entire federal government in mind. Collaboration is ongoing with other government organizations, private sector companies, universities, standards and professional organizations, and their international counterparts. Each of these communities plays an integral role in global ICT supply chain security.

According to Wilson, de Zafra, Pitcher, Tressler, and Ippolito (2003), security awareness efforts are designed to change attitude or reinforce good security practices, and to allow individuals to recognize IT security concerns and respond accordingly. The learner in a training environment has a more active role. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance through the development of higher-level concepts and skills. Education integrates all security skills and competencies of the various functional specialties into a common body of knowledge; adds a multidisciplinary study of concepts, issues, and principles; and strives to produce IT security specialists and professionals capable of vision and pro-active response (p. 15-16).

According to Gary S. Lynch, consultant and author, “Supply chain risk management begins with awareness, a consciousness that everyone is part of the endless stream of supply chains, which are linked together by relationships and configured according to needs” (2009, p. 16). Awareness is the foundational event for all personnel across government organizations, levels, and specialties, and in the private sector. “Public officials and private sector leaders must understand and appreciate their roles and responsibilities in preserving cybersecurity and safeguarding the U.S. supply chain. Individual users must be educated regularly on the importance of complying with applicable cybersecurity safeguards (CACI International, Inc. & United States Naval Institute, 2010, p. 22). As part of the ETA effort DoD is developing an awareness event for decision makers and leaders throughout government to introduce, engage and motivate, and expand commitment to current enterprise perspectives and efforts. If these awareness activities are effective, then all decision makers, no matter how closely they are connected with the specific activities of the life cycle and the effects of the global ICT supply chain, will approach the taking of risk differently and be supportive of government enterprise efforts to assure product integrity.

For some personnel, awareness will be followed by customized training that provides appropriate depth for their particular roles in implementation of processes aligned with new policies. A strong supply chain risk mitigation strategy cannot be put in place without significant attention given to training of federal department and private sector personnel who play important roles in the global supply chain related to cybersecurity policy, procedures, and applicable management, operational, and technical controls and practices (Boyens et al., 2012). For others an awareness event will be the foundation of educational events that include a module or course at the undergraduate or graduate level focused on deep understanding and application of concepts, research, and theories in novel situations, leading others through modeling, and influencing processes and policies in response to this emerging security threat. The ETA strategy must identify the message and core content, audiences, resources, curricula, and instructional formats customized for various audiences, and assess their impact; and must leverage partners, including government training and educational institutions, and civilian higher education institutions.

The Message

At the heart of the ETA strategy is a clear, persuasive, and mobilizing message about security risks associated with the exploitation of the global ICT supply chain. The strategy seeks to engage various communities that can mobilize their workforces to action. Convergence on the right terminology from the perspective of key stakeholders is a challenge, exacerbated by the choice of the term “supply chain risk management” which unfortunately has other meanings for other communities. Words are important, especially in a campaign to change attitudes, minds, and behavior. The intended outcomes articulate how participants will manage risks appropriate to their roles.

Partners

The ETA strategy relies on the power of communities to share information and engage multiple stakeholders in the delivery of the message. The DoD team that is developing and leading the ETA effort is working concurrently to crystallize the core message, engage multiple stakeholders and communities, and to build a network of organizational partners. Partners are individuals who work in key organizations who understand the message and are motivated to engage others. The members of the DoD roundtable are implementing supporting policies and processes, informing senior leaders, and developing organizational training programs for individuals in roles related to product integrity and supply chain security. They share information, best practices, and advancements in research and practice, and raise issues and concerns. In the ETA effort they serve as access points to personnel and test beds for training and awareness activities. Many organizational partners have their own training and educational institutions in support of their workforce development. Systematic outreach efforts are targeting these organizations as prospective partners who might be interested in developing curriculum, sharing content, instructional materials, and lessons learned, as well as other government organizations, standards and professional associations, and private sector companies.

Target Audiences

The ETA effort seeks to foster awareness of decision makers and leaders at various levels, in diverse organizations, some of whom are deployed around the world. The strategy calls for training members of specialized communities who play critical roles in the security of the supply chain and life cycle of systems, e.g., acquisition, contracting, and cybersecurity. These specialists will be targeted for training that is relevant, customized, and impactful so that they can implement processes and policies to assure the security of the global supply chain. The members of the roundtable can identify the points of contact in their organizations to facilitate engagement for ETA of members of their workforces.

Government Training and Educational Institutions

Across government, especially in defense, specialists who are trained and certified by their own workforce leadership and institutions can become partners in spreading the message and curricula as appropriate. The DoD operates its own military higher education system. As part of this initiative one DoD graduate school is developing a pilot course focused on the security of the global ICT supply chain for DoD employees who are seeking to earn a Chief Information Officer or Information Technology Project Management certificate. The course is designed to engage students in critical thinking, theory and practice, research, and application related to the topic. As guest speakers, experts from government enrich the course with enterprise perspectives, research challenges, and policy imperatives to prepare graduates to mobilize their respective organizations to implement policies and processes to secure the global ICT supply chain. Graduates will be urged to participate actively in communities that are deepening and expanding supporting policies and practices.

Training and educational institutions and their leaders across the DoD enterprise are prospective partners who might be interested in developing new curricula on the topic or in sharing curricula with faculty at other institutions. As courses or training events are developed and offered, in residence or online, they may become available to students at other institutions.

Higher Education Institutions

Partnerships with higher education institutions are essential because these institutions offer undergraduate and graduate programs that prepare graduates for positions in the government cybersecurity workforce and the private sector in support government cybersecurity goals. The DoD Information Assurance Scholarship Program and the CyberCorps Scholarship for Service Program began over a decade ago as collaborative efforts of government and dozens of academic institutions. The network of "Centers of Academic Excellence in Information Assurance Education" offers approved curricula for graduates seeking to qualify for government jobs in information security. As the standards for participation align with the NICE framework, higher education cybersecurity curricula will include risk management for ensuring the security of the global ICT supply chain.

Document and Resource Directories

To support the network of experts, key decision makers, faculty, and standards groups who are critical to this strategy, web-enabled bibliographies of academic, government, and research publications and resources are being developed. A body of knowledge is also in development that will align the related and supporting national and international standards for academic, process, and policy purposes. A catalog of existing curricula and current research at universities and training organizations will offer prospective students and faculty information about available courses and programs focused on global ICT supply chain security that align with the competencies articulated in the National Cybersecurity Workforce Framework (2012).

Intended Learning Outcomes

For each ETA event the intended learning outcomes will focus on observable behavior. ETA activities, whether one-hour awareness events, multi-session training, or semester-long courses, will be designed to enable active participants to manage the taking of risks related to the security of the global ICT chain. The intended learning outcomes will be shaped with the appropriate scope and depth for the role of the participants. The observable behaviors are the starting point for assessing the impact of the activities on the participants.

Curricular Content

As a strategy for ETA for the government workforce, the core content of the curriculum needs to be coherent and up to date, even as it is being customized by different organizations for various audiences. The approved government policies and definitions, current research findings, and body of knowledge aligned with standards and best practices must be available and consistently promulgated across the curricula of training and education institutions. This will foster consistent understanding of global ICT supply chain threats, vulnerabilities, mitigations, and the approach for managing risks. The strategy will foster shared understanding of concepts, guiding principles, and messages though collaborative planning and curriculum development. Faculty from academic communities will be invited to participate in events and share concepts, resources, curriculum, and instructional materials.

Instructional Formats

In addition to traditional face-to-face engagements, awareness activities will leverage various instructional formats as appropriate to engage audiences to achieve intended learning outcomes. This is critical because the audiences targeted for awareness are huge, diverse, and distributed. Educational activities such as courses can be delivered using face-to-face, faculty-led interactive or self-paced distance learning formats, online modules and webinars, and virtual reality, as appropriate. Partner higher education institutions will be encouraged to share courses and content, and instructional materials with other faculty, institutions, and students. Training modules and courses will be customized in instructional format for various audiences.

Assessment of Impact

In current practice, government personnel are required to complete annual training on important topics, ranging from information security to ethics, depending on their levels, roles, and organizations. In order to motivate attendance and attention, and to achieve its intended outcomes, the ETA efforts must be customized for each audience. The impact of the activities must be measured to justify the cost of design, development, and delivery of events and programs, and account for the time of government employees invest in attending them.

Conclusion

In 2012, the U.S. government launched an ETA effort to engage DoD and the rest of the federal government on national security issues related to the security of the global ICT supply chain. Partnerships are developing with multiple communities, contacts are being made with selected training and educational institutions, and the core messages are being articulated. The development of curricular content is underway for training the members of the specialized communities who play critical roles in the security of the supply chain and life cycle of systems. This training must be relevant, customized, and impactful in order to result in behaviors that assure the integrity of critical system components and functions. By design, training will be offered by many organizations and institutions across the enterprise, so mechanisms must be in place to ensure that the content remains coherent and up to date. In the year ahead the strategy will be full developed, the network of key communities will be expanded, and the core messages and organizing principles of curricula will be articulated and shared with roundtable members, leaders of various workforce communities, and faculty engaged in curriculum development. The strategy is refining the message designed to motivate others to action and to build partnerships with leaders, educators, researchers, and specialists committed to securing the global ICT supply chain. The impact of the ETA effort can be measured in its next phase by assessing the changes in cognition, attitude, and behavior that result from awareness, training, and education events.

Future Research Opportunities

The ETA strategy relies on on-going collaboration among researchers and policy makers, government organizations, academic institutions, standards bodies, professional associations, trainers in government and the private sector, and international counterparts. Research opportunities abound as the body of knowledge develops, the processes specific to global ICT risk management mature, and the best practices appropriate for target audiences are identified. The content and intended learning outcomes must be refined and assessed for their impact. Research opportunities also exist to assess the value of the processes to assess criticality, threats, and vulnerabilities, as well as specific risk mitigations.

Disclaimer

The publication of this paper does not indicate endorsement by the Department of Defense or IDA, nor should the contents be construed as reflecting the official position of those organizations.

References

Alberts, C. J., Ellison, R. J., Dorofee, A. J., Woody, C., & Creel, R. (2011). A systemic approach to assessing software supply-chain risk. *Proceedings of the 44th Hawaii International Conference on System Sciences(HICSS)*, Computer Society Press, 1-8.

Baldwin, K., Popick, P. R., Miller, J. F., & Goodnight J. (2012). The United States Department of Defense revitalization of system security engineering through program protection. *SysCon 2012 – IEEE International Systems Conference Proceedings*, 411-417.

Boyens, J., Paulsen, C., Bartol, N., Moorthy, R., & Shankles, S. (2012). *Notional supply chain risk management practices for federal information systems* (NISTIR 7622). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved January 28, 2013 from http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf.

CACI International, Inc. and United States Naval Institute. (2010). *Cyber threats to national security: Countering challenges to the global supply chain.* Retrieved January 30, 2013 from http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf.

Chan, S., & Larsen, G. N. (2010). A framework for supplier-supply chain risk management: Tradespace factors to achieve risk reduction-return on investment*. 2010 IEEE International Conference on Technologies for Homeland Security*, Waltham, MA.

Comprehensive National Cybersecurity Initiative. (2009). The White House. Retrieved January 28, 2013 from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

Ellison, R., & Woody, C. (2010). Supply-chain risk management: Incorporating security into software development. *Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS)*, Computer Society Press, 1-10.

Filsinger, J., Fast, B., Wolf, D. G., Payne, J. F. X., & Anderson, M. (February 2012). *Supply chain risk management awareness.* Armed Forces Communication and Electronics Association Cyber Committee. Fairfax, VA. Retrieved January 28, 2013 from http://www.afcea.org/ committees/cyber/documents/Supplychain.pdf

Hoover, J. N. (2009). Securing the cyber supply chain. *Information Week*. Retrieved January 28, 2013 from http://www.informationweek.com/government/security/securing-the-cyber-supply-chain/221600499

Joint Task Force Transformation Initiative Interagency Working Group. (2012). *Guide for conducting risk assessment. Special Publication 800-30, Revision 1.* Gaithersburg, MD. National Institute of Standards and Technology. Retrieved January 28, 2013 from http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf.

Komaroff, M., Patterson, J., Davidson, D., Mirsky, A., & Wassel, J. (2011). DoD advances supply chain management efforts. *IA newsletter, 14*(2), 4-8.

KPMG. (2005). *Managing the risks of counterfeiting in the information technology industry.* Retrieved January 28, 2013 from http://www.agmaglobal.org/cms/uploads/ whitePapers/KPMGAGMA_ManagingRiskWhitePaper_V5.pdf

Lynch, G.S. (2009). *Single point of failure: The ten essential laws of supply chain risk management.* Hoboken, NJ: John Wiley & Sons, Inc.

National Initiative for Cybersecurity Education (2011). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved January 28, 2013 from http://csrc.nist.gov/nice/

National Cybersecurity Workforce Framework (2012). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved January 30, 2013 from http://csrc.nist.gov/ nice/framework/

Smith, G. E., Watson, K. J., Baker, W. H., & Polorski, J.A., II. (2007). A critical balance: Collaboration and security in the IT-enabled supply chain. *International journal of production research, 45*(11), 2595-2613.

United States Department of Defense Strategy for Operating in Cyberspace. (July 2011). Retrieved January 28, 2013 from http://www.defense.gov/home/features/2011/0411_ cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf.

United States Government Accountability Office. (2008). *Cyber analysis and warning: DHS faces challenges in establishing a comprehensive national capability.* (GAO-08-588). Washington, D.C.

United States National Strategy for Global Supply Chain Security (January 2012). Retrieved January 30, 2013 from http://www.whitehouse.gov/sites/default/files/national_strategy_for_ global_supply_chain_security.pdf.

Villasenor, J.D. (2011). Ensuring hardware cybersecurity. *Issues in technology innovation*. Center for Technology Innovation at Brookings. No. 9, 1-9.

Wilson, M., de Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (2003). *Information technology security training requirements: A role- and performance-based model. NIST Special Publication 800-16*. Gaithersburg, MD. National Institute of Standards and Technology. Retrieved January 28, 2013 from http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

United States Government Accountability Office. (2008). *Cyber analysis and warning: DHS faces challenges in establishing a comprehensive national capability.* (GAO-08-588). Washington, D.C.

Villasenor, J. D. (2011). Ensuring hardware cybersecurity. *Issues in technology innovation*. Center for Technology Innovation at Brookings. No. 9, 1-9.

Wilson, M., de Zafra, D.E., Pitcher, S.I., Tressler, J.D., and Ippolito, J. B. (2003). *Information technology security training requirements: A role- and performance-based model. NIST Special Publication 800-16*. Gaithersburg, MD. National Institute of Standards and Technology. Retrieved January 28, 2013 from http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

Biography

Elizabeth A. McDaniel is currently a research staff member at the Institute for Defense Analyses. Dr. McDaniel served as the Dean of Faculty and Academic Programs at the Information Resources Management College, National Defense University from 1999 through 2010. After earning her Ph.D. from the University of Miami in 1978, she began her academic career at the University of Hartford, where she advanced to full professor, and associate vice president for academic affairs. She was an American Council on Education Fellow in the Office of the President at the University of Connecticut in 1989-1990; Executive Provost and Vice President for Academic Affairs at Nova Southeastern University 1995-1998; and Senior Fellow at the American Council on Education in 1998-1999.