Building a Body of Knowledge for ICT Supply Chain Risk Management

Dan Shoemaker

Nancy Mead

May 2013

ABSTRACT: This paper proposes a set of Supply Chain Risk Management (SCRM) activities and practices for Information and Communication Technologies (ICT). This set can be used as a starting point to create a body of knowledge in SCRM to ensure the integrity of ICT products.

INTRODUCTION

ICT is a vital part of our culture. In fact, many would argue that computers and their associated communications technologies have created that culture. Because we depend so much on our ICT products, it is critically important to be able to trust their integrity. Yet, commonly used ICT development and sustainment practices still permit dangerous defects that allow attackers to compromise millions of computers every year [1]. The increasing trend toward building systems out of purchased parts just enhances the importance of getting the acquisition of ICT components right [2].

Early in this decade, NIST estimated that exploitation of ICT defects costs the U.S. economy an average of $60 billion annually, and there is no reason to think that those numbers have improved since then [3]. But the real concern is not cybercrime; it is that the exploitation of a point of failure in an infrastructure component like power or communication could have severe consequences. Therefore, it is not surprising that the U.S. government is addressing the problem of product integrity through a comprehensive program to get better SCRM practices into the workforce. This program includes education, training, and awareness initiatives, which are the traditional means of leveraging the required change in workforce behavior. However, when it comes to SCRM, although much progress has been made [4, 5] there is still no single reference to define what should be taught [6, 7].

An authoritative Body of Knowledge (BOK) of best practices for SCRM is an attractive idea. Such a BOK would portray the SCRM process as a complete set of topics. The BOK would integrate the knowledge needed for effective man-

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

agement of supply chain risk into a framework that contains all of the advice necessary to ensure ICT product integrity. The aim would be to characterize and relate all the detailed knowledge elements needed to develop precise workforce learning requirements, as well as the methods to deliver that learning. In addition, a commonly accepted BOK could be used as leverage to develop new education and training curricula as the field evolves [6, 7].

Several conventional disciplines could be part of a discipline of ICT SCRM, such as hardware and software engineering, systems engineering, information systems security engineering, safety, security, reliability, testing, information assurance, and project management [6]. In addition, it would be possible to consider academic areas such as intelligence analysis and law as potential parts of the discipline. Because these are highly disparate fields, it is important to create a detailed model of the relationship between all of the logical components in order to judge whether the right content is being provided in each education and training setting.

ICT SCRM IN COMMON STANDARDS

ICT products are developed through a global supply chain. Supply chains are no different from any other organizational function in that they are intended to accomplish a specific purpose. The purpose of all supply chains is to provide a product or service through coordinated work that involves several organizations. The concerns about supply chains fall into five categories. Each category has slightly different implications for product integrity: “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 a technical service and installation of unintentional vulnerabilities on software or hardware [2].”

Proper SCRM mitigates these concerns by providing a consistent, disciplined environment for developing the product, assessing what could go wrong in the process (i.e., assessing risks), determining which risks to address (i.e., setting mitigation priorities), implementing actions to address high-priority risks and bringing those risks within tolerance [8]. Typically, supply chains are hierar-

chical, with the primary supplier forming the root of a number of levels of parent-child relationships. From an assurance standpoint, what this implies is that every individual product of each individual node in that hierarchy has to be correct as well as correctly integrated with all other components up and down the production ladder. Because the product development process is distributed across a supply chain, maintaining the integrity of the products that are moving within that process is the critical concern.

The weak link analogy is obvious here, so, whether the product is a common household item or sophisticated military hardware, the activities within that product's supply chain have to be precisely coordinated and carefully controlled. Authoritative control processes already exist, which specifically address the existing coordination and control concerns. These processes are embodied in the activities and tasks of two international "umbrella" standards. The recommendations of these standards have been validated worldwide. So besides providing authoritative real-world advice about how to manage supply chain risk, the detailed activities and tasks that are specified in those standards also provide a coherent and detailed logic for a BOK of SCRM best practices.

BUILDING A FRAMEWORK FOR THE BOK OF SCRM

Education From Two International Standards At present, there is no complete classification structure for the BOK for ICT SCRM. Thus our aim was to derive a conceptual model for the discipline based on existing standards. A standard conceptual model is essential in order to ensure proper associations between the many disparate knowledge, skills, and abilities required to produce, maintain, and acquire trustworthy ICT products. The DHS uses the term Enterprise Security Framework (ESF) to describe the specific set of actions needed to ensure the reliability of purchased products [9]. The aim of an ESF is to factor everybody's actions for achieving secure products into a "who, what, when" structure of defined activities and interrelationships. To create this structure, DHS suggests that the ESF must include responsibilities beyond the typical system and software security activities seen in most organizations. These responsibilities can be implemented by blending top-level risk management activities contained in the ISO 16085 Lifecycle Risk Management standard with the activity and task recommendations of the Agreement processes of the ISO 12207-2008 standard.

The activities embodied in the 12207 Agreement process convey the steps that an organization should take to, "manage the procurement of a system, software, or service product." The agreement processes are particularly relevant to those interested in defining the discipline of SCRM in that they provide a structured and rigorous set of activities and tasks to carry out the effort. The 12207-2008 activities specified for acquisition convey the practices that have to be performed when an organization procures a software system or service, while the supply process (6.1.2) delineates the obligations of the supplier. Using the 12207-2008 standard, it is possible to form a detailed definition of the standard customer supplier activities involved in ICT procurement. However, that definition does not take risk management into consideration.

The purpose of ISO 16085 System and Software Supply Chain Risk Management is to identify potential managerial and technical actions to reduce or eliminate the probability and impact of risk [10]. The standard may be used for managing risk at the organizational, enterprise, or project level in any domain or lifecycle stage [10]. The aim is to support the perspectives of managers, suppliers, acquirers, developers, participants, and other stakeholders and provide them with a single set of process requirements suitable for the management of a broad variety of risks in the supply chain [10]. The standard prescribes a continuous process for risk management and is useful for managing the risks associated with organizations dealing with system or software [10]. Moreover, 16085 is specifically designed to be used in conjunction with ISO 12207-2008.

Thus, the recommendations of the standard can be directly aligned with the risk management activities specified by the 12207 project process area (6.4). When used with ISO 12207-2008, the 16085 standard assumes that necessary managerial and technical processes to perform the treatment of risk are called out by the ISO 12207-2008 model. The addition of the risk management component to the standard procurement model represented in the 12207 agreement processes provides a complete set of practices for ICT SCRM.

CREATING AN INSTRUCTIONAL MODEL FOR SCRM

SCRM issues are different for the acquirer, supplier, and integrator. In addition, there are at least four different types of environments that require a specific ap-

proach to SCRM: high assurance (trusted), government-off-the-shelf, commercial off-the-shelf, and services. Given that diversity, our aim was to derive a standard set of activities and practices from the two standards discussed in the prior section. Our goal was to derive a point of reference for content and teaching development.

The relevant lifecycle process activities that were incorporated in our approach are from the 12207-2008: Agreement, Reuse, Technical, and Supporting and Project Management process areas. These recommendations were integrated with the ICT Risk Management process recommendations that are specified by ISO 16085. The content model derived from integrating these two references ultimately leads to a set of lifecycle activities and practices, which can form a starting point for development of a complete BOK for management of supply chain risk.

Once such a BOK has been perfected, explicit learning behaviors can be derived for each content item. Then, appropriate standard instructional content can be designed and created to reinforce each behavior along with a set of proficiency requirements specified for each action. Instructional content can be customized from the BOK to address each situation in which it will be applied. The approach to content delivery can be referenced to learning and proficiency specifications. From an evaluation standpoint, the ability to perform each task can be characterized as a nominal set of observable actions. The knowledge needed to perform each task and/or the skill required to perform each task can be characterized as an ordinal judgment of proficiency.

The list below summarizes the general subject areas that evolved from our process of creating an instructional model for SCRM, using the recommendations of the two standards.

Subject Area One: Project Initiation and Planning

- Strategic management and policy
- Project management
- Business and assurance case development
- Supply chain component definition and labeling
- Threat/risk and mitigation identification and planning

Subject Area Two: Product Requirements Communication

- Requirements elicitation and specification
- Requests for proposals (RFP) documentation
- Statement of work (SOW) documentation
- Project assurance criteria development (including SCRM)
- Project measurement and metrics development (including SCRM)
- Formalization and documentation of product assurance case requirements
- Preparation and documentation of acceptance criteria

Subject Area Three: Source Selection and Contracting

- Source selection process
- Source evaluation process
- Contract negotiation
- Contract writing
- Lifecycle contract management planning
- Lifecycle project management planning

Subject Area Four: Supplier Contract Execution

- Document framework for ICT project management.
- Document plan to manage the quality and security of the project.
- Implement and execute the project management plan(s).
- Monitor and control progress throughout the contracted lifecycle.
- Manage and control the subcontractors.
- Interface with the independent verification, validation, or test agent.
- Coordinate contract review activities and interfaces.
- Conduct joint reviews in accordance with ISO standard specifications.
- Perform verification and validation to satisfy that requirements are met.

Subject Area Five: Customer Agreement Monitoring

- Monitor the supplier's activities in accordance with the contracted software assurance process
- Develop plan to supplement monitoring with verification and validation as needed

- Develop plan to ensure necessary information is provided in a timely manner

Subject Area Six: Customer Acceptance

- Plan acceptance process based on contracted acceptance strategy and criteria
- Plan test cases, test data, test procedures, and test environment
- Conduct acceptance review and acceptance testing of the deliverable
- Accept product from supplier when all acceptance conditions are satisfied
- Plan to migrate product from supplier to customer

Subject Area Seven: Project Closure

- Make payment or provide other agreed consideration to the supplier
- Install the product in accordance with established requirements
- Ensure agreement terminates when payment is made
- Transfer legal responsibility for the product or service to the customer
- Provide assistance to the customer in support of the delivered product

The subject areas and detailed activities and practices of SCRM provide support for the development of a formal discipline of SCRM. Once the discipline is codified, this material can be integrated into traditional ICT education and training programs. ISO 12207-2008 provides a commonly accepted definition of best practices for ICT acquisition and supply, while activities and tasks specified in ISO 16085 provide an excellent collection of assurance practices for ICT work. This makes it possible to construct a detailed picture of SCRM practices and activities that can be used in building an SCRM body of knowledge.

EXAMPLE ACTIVITIES AND PRACTICES FOR SCRM

Procurement Program Initiation and Planning

- Develop the concept to acquire (business case).
- Define project scope and boundaries.
- Develop an acquisition strategy and/or plan.
- Define constraints.

- Make decision to contract.
- Identify and mitigate outsourcing definitions.
- Install risk management process.
- Perform product assurance risk assessment.
- Develop product assurance risk mitigation strategies.
- Ensure product assurance risk monitoring.

Product Requirements Communication

- Issue written requests to prospective suppliers.
- Standardize elements of the RFP.
- Document SCRM needs and requirements in the RFP.
- Specify SCRM terms and conditions.
- Specify information security features.
- Specify acceptance criteria for COTS integrations.
- Implement common criteria (if required).
- Create a specification.
- Specify SCRM measures and metrics.
- Create assurance language for a statement of work (SOW).
- Assure requirements for C&A in SOW.
- Ensure SOW specifies SCRM education and training.
- Develop SOW to acquire COTS.
- Provide SCRM language in instructions to suppliers.
- Ensure response reflects the specified capabilities.
- Ensure supplier has submitted adequate information.
- Specify initial product architecture.
- Specify product assurance case management procedure.
- Specify product assurance lifecycle.
- Specify product requirements and traceability criteria.

Source Selection and Contracting

- Specify evaluation criteria.
- Ensure standard product assurance evaluation criteria.
- Specify assurance criteria in the Source Selection Plan.
- Perform contract negotiations.
- Perform project/contract management.

- Plan to oversee product assurance reviews and audits.
- Ensure competent product assurance professional(s).
- Oversee the supplier's delivery of product assurance.
- Define the rate at which the supplier will provide assurance statements.
- Define how performance will be evaluated if an SLA is used.
- Define the role that product assurance plays in product C&A.
- Define how the product architecture will be managed.
- Define what will be reviewed from an assurance perspective.
- Define how often the risk management plan will be updated.
- Define how often the product assurance risks will be evaluated.
- Devise an issues resolution plan and process.
- Define circumstances for intelligence updates.
- Define how corrective actions will be monitored.
- Define how product assurance savings will be measured.
- Define how experience level will be monitored.
- Define how to identify key product personnel.
- Define how key personnel will be monitored.
- Define how assurance training program will be monitored.

Supplier Contract Execution

- Create a management framework for the ICT project.
- Select a lifecycle model.
- Select processes, activities, and tasks and map them to lifecycle model.
- Develop a plan to manage the quality and security of the project.
- Develop document project management plan(s).
- Implement and execute the project management plan(s).
- Monitor and control progress throughout the contracted lifecycle.
- Develop the software product using internal resources.
- OR develop the software product by subcontracting.
- Buy off-the-shelf software products from internal or external sources.
- Monitor the progress of the project.
- Manage and control the subcontractors.
- Ensure all contractual requirements are passed to subcontractors.
- Interface with the independent verification, validation, or test agent.
- Interface with other parties as specified in the contract and project plans.

- Coordinate contract review activities and interfaces.
- Conduct joint reviews in accordance with ISO standard specifications.
- Perform verification and validation to satisfy that requirements are met.
- Make reports available as specified in the contract.

Customer Agreement Monitoring

- Monitor supplier's activities using the Software Review Process.
- Supplement monitoring with verification and validation as needed.
- Ensure necessary information is provided in a timely manner.

Customer Acceptance

- Prepare for acceptance based on the acceptance strategy.
- Prepare test cases, test data, test procedures, and test environment.
- Define the extent of supplier involvement in acceptance.
- Conduct acceptance review and acceptance testing of the deliverable.
- Accept product from supplier when all acceptance conditions are satisfied.
- Arrange to make customer responsible for configuration management.

Project Closure

- Make payment or provide other agreed consideration to the supplier.
- Install the product in accordance with established requirements.
- Ensure agreement terminates when payment is made.
- Transfer responsibility for the product or service to the customer.
- Provide assistance to the customer in support of the delivered product.

Conclusion

We have proposed a set of SCRM activities and practices in this paper. These activities and tasks comprise an initial picture of the knowledge needed to correctly and effectively conduct a practical SCRM process. We derived this set of activities and practices from established models of practice for acquisition and supply of software and systems, along with additional risk control elements. We believe that it will be possible to create a true body of knowledge in SCRM us-

ing this set as a starting point. SCRM is clearly a huge field composed of a number of not clearly related subjects. The first step in creating a body of knowledge for the field is to provide a top-level classification structure of its practices and activities, which we propose in this paper.

ABOUT THE AUTHORS

Daniel P Shoemaker, Ph.D., is Principal Investigator and Senior Research Scientist at UDM's Center for Cyber Security and Intelligence Studies. He is also a full time Professor and former Department Chair at University of Detroit Mercy. As the Co-Chair for the, National Workforce Training and Education Initiative he is one of the authors of the DHS Software Assurance Common Body of Knowledge (CBK). He also helped author the DHS IA Essential Body of Knowledge and he serves as a SME for the NIST-NICE workforce framework. Dan's doctorate is from the University of Michigan and within the State of Michigan he leads the International Cyber-Security Education Coalition. This Coalition covers a five state region with research partners as far away as the United Kingdom. Dan also spends his free time authoring some of the leading books in Cyber Security. His book "Cyber Security: The Essential Body of Knowledge," is Cengage publishing's flagship book in the field. His first book, "Information Assurance for the Enterprise," is McGraw-Hill's primary textbook in IA and is in use all over the globe. His next book, "Engineering a More Secure Software Organization," which is also published by Cengage, will be out soon.

E-mail: dan.shoemaker@att.net

Nancy R. Mead, Ph.D. is Senior Member of the Technical Staff, CERT Secure Software and Systems, in the CERT Program at the SEI. She is also a faculty member in the Master of Software Engineering and Master of Information Systems Management programs at Carnegie Mellon University. She is currently involved in the study of security requirements engineering and the development of software assurance curricula. She also served as director of education for the SEI from 1991 to 1994. Her research interests are in the areas of information security, software requirements engineering, and software architectures.

Prior to joining the SEI, Mead was a senior technical staff member at IBM Federal Systems, where she spent most of her career in the development and man-

agement of large real-time systems. She also worked in IBM's software engineering technology area and managed IBM Federal Systems' software engineering education department. She has developed and taught numerous courses on software engineering topics, both at universities and in professional education courses.

Mead has more than 150 publications and invited presentations, and has a biographical citation in Who's Who in America. She is a Fellow of the Institute of Electrical and Electronic Engineers, Inc. (IEEE) and the IEEE Computer Society, and a Distinguished Member of the ACM. Mead serves on the Editorial Boards for the International Journal on Secure Software Engineering and the Requirements Engineering Journal, and is a member of numerous advisory boards and committees.

Mead received her Ph.D., in mathematics from the Polytechnic Institute of New York, and received a BA and an MS in mathematics from New York University.

E-mail: nrm@sei.cmu.edu

REFERENCES

1. Clark R.A. and H.A. Schmidt, "A national strategy to secure cyberspace," The President's Critical Infrastructure Protection Board, Washington, DC, 2003.
2. GAO Report to Congressional Requesters. IT Supply Chain: National Security-Related Agencies Need to Better Address Risks. United States Government Accountability Office, March 23, 2012.
3. Newman, Michael. Software Errors Cost U.S. Economy $59.5 Billion Annually. Gaithersburg: National Institute of Standards and Technology (NIST), 2002.
4. Ellison, Robert, Christopher Alberts, Rita Creel, Audrey Dorofee, and Carol Woody. Software Supply Chain Risk Management: From Products to Systems of Systems. CMU/SEI-2010-TN-026. Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2010. <http://www.sei.cmu.edu/library/abstracts/reports/10tn026.cfm>

5. Ellison, Robert, John Goodenough, Charles Weinstock, and Carol Woody. Evaluating and Mitigating Software Supply Chain Security Risks. CMU/SEI-2010-TN-016. Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2010. <http://www.sei.cmu.edu/library/abstracts/reports/10tn016.cfm>
6. Redwine, Samuel T., ed. Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software, Version 1.1. Washington: U.S. Department of Homeland Security, 2006.
7. Mead, Nancy, Julia Allen, Mark Ardis, Thomas Hilburn, Andrew Kornecki, Richard Linger, and James McDonald. Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum. CMU/SEI-2010-TR-005. Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2010. <http://www.sei.cmu.edu/library/abstracts/reports/10tr005.cfm>.
8. Alberts, Christopher, and Audrey Dorofee. A Framework for Categorizing Key Drivers of Risk. Rep. no. CMU/SEI-2009-TR-007. Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2009.
9. Allen, Julia H. "Security Is Not Just a Technical Issue." Build Security In Website. Department of Homeland Security. 2009. <https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/563-BSI.html>.
10. International Standards Organization. Systems and Software Lifecycle Process Risk Management – ISO/IEC 16085. ISO, 2006.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0001120