INTERNAL AUDIT AND IT AUDIT SERIES

Supply Chain Risk Management

Applying Secure Acquisition Principles to Ensure a Trusted Technology Product

Ken Sigler • Dan Shoemaker • Anne Kohnke

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Supply Chain Risk Management

Internal Audit and IT Audit

Series Editor: Dan Swanson

Cognitive Hack: The New Battleground in Cybersecurity … the Human Mind
James Bone
ISBN 978-1-4987-4981-7

The Complete Guide to Cybersecurity Risks and Controls
Anne Kohnke, Dan Shoemaker, and Ken E. Sigler
ISBN 978-1-4987-4054-8

Corporate Defense and the Value Preservation Imperative: Bulletproof Your Corporate Defense Program
Sean Lyons
ISBN 978-1-4987-4228-3

Data Analytics for Internal Auditors
Richard E. Cascarino
ISBN 978-1-4987-3714-2

Ethics and the Internal Auditor's Political Dilemma: Tools and Techniques to Evaluate a Company's Ethical Culture
Lynn Fountain
ISBN 978-1-4987-6780-4

A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)
Dan Shoemaker, Anne Kohnke, and Ken Sigler
ISBN 978-1-4987-3996-2

Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework
Anne Kohnke, Ken Sigler, and Dan Shoemaker
ISBN 978-1-4987-8514-3

Internal Audit Practice from A to Z
Patrick Onwura Nzechukwu
ISBN 978-1-4987-4205-4

Leading the Internal Audit Function
Lynn Fountain
ISBN 978-1-4987-3042-6

Mastering the Five Tiers of Audit Competency: The Essence of Effective Auditing
Ann Butera
ISBN 978-1-4987-3849-1

Operational Assessment of IT
Steve Katzman
ISBN 978-1-4987-3768-5

Operational Auditing: Principles and Techniques for a Changing World
Hernan Murdock
ISBN 978-1-4987-4639-7

Practitioner's Guide to Business Impact Analysis
Priti Sikdar
ISBN 978-1-4987-5066-0

Securing an IT Organization through Governance, Risk Management, and Audit
Ken E. Sigler and James L. Rainey, III
ISBN 978-1-4987-3731-9

Security and Auditing of Smart Devices: Managing Proliferation of Confidential Data on Corporate and BYOD Devices
Sajay Rai, Philip Chukwuma, and Richard Cozart
ISBN 978-1-4987-3883-5

Software Quality Assurance: Integrating Testing, Security, and Audit
Abu Sayed Mahfuz
ISBN 978-1-4987-3553-7

Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product
Ken Sigler, Dan Shoemaker, and Anne Kohnke
ISBN 978-1-4987-3553-7

Why CISOs Fail: The Missing Link in Security Management—and How to Fix It
Barak Engel
ISBN 978-1-138-19789-3

Supply Chain Risk Management

Applying Secure Acquisition Principles to Ensure a Trusted Technology Product

Ken Sigler, Dan Shoemaker, and Anne Kohnke

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper

International Standard Book Number-13: 978-1-138-19735-0 (Hardback)
International Standard Book Number-13: 978-1-138-19733-6 (Paperback)

Library of Congress Cataloging-in-Publication Data

Names: Sigler, Kenneth, author. | Shoemaker, Dan, author. |
Kohnke, Anne, author.
Title: Supply chain risk management : applying secure acquisition principles
to ensure a trusted technology product / Ken Sigler, Dan Shoemaker,
Anne Kohnke.
Description: New York : CRC Press, [2018] | Series: Internal audit and IT audit
Identifiers: LCCN 2017030801 | ISBN 9781138197350 (hb : alk. paper) |
ISBN 9781138197336 (pb : alk. paper) | ISBN 9781315279572 (e)
Subjects: LCSH: Business logistics. | Risk management. | Data protection. |
Computer networks--Security measures.
Classification: LCC HD38.5 .K64 2018 | DDC 658.7--dc23
LC record available at https://lccn.loc.gov/2017030801

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Foreword

Complexities in the cyber supply chain have introduced new avenues for exploitation and manipulation attracting numerous U.S. adversaries.

Megan Mance
Cyber Supply Chain Security and Potential Vulnerabilities within U.S. Government Networks (June 15, 2016)

On November 19, 2015 Admiral Michael Rogers, the Chief of the National Security Agency and U.S. Cyber Command, told an audience that his principal concern is data manipulation through network intrusion. U.S. adversaries are continually looking for new and creative ways to gain access to U.S. government networks. One specific cyber threat that deserves greater attention is the *cyber supply chain security* within the federal government and the vital role of government contractors in this area.

The 2017 U.S. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (dated May 11, 2017) calls for the U.S. government departments and agencies to report "on cybersecurity risks facing the defense industrial base, including its *supply chain*, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks."

Even a trusted supplier can unwittingly integrate components that might be obtained from untrustworthy sources. Unfortunately, this is the likely situation given the globally sourced commercial off-the-shelf (COTS) strategies popular in our current national security and information and communication technology (ICT) business organizations.

It is too difficult to provide across-the-board assurance for all tiers/levels of all products, because most products are agilely sourced in a global environment; if we cannot do it all, the key concept here is to take a risk-based approach to secure what we can, to at least provide across-the-board assurance for some critical capabilities. Therefore, it will be necessary for enterprises to identify their most critical capabilities or functions, and for those mission-essential functions, they will seek to ensure trustworthiness of every product, component, and subcomponent enabling that capability/function.

Planning for the tracking of subcomponents and components brought together in a select product or system is required, because it would be nearly impossible to trace back after the fact. So, a big part of ensuring a trustworthy sourcing process rests on the ability of the supplier to prove that they can deliver the knowledge of their supply chain processes: what is planned and how they will manage deviations from predicted plans. This type of detailed supply chain planning (SCRM) also leads to on-cost, timely delivery of these trusted components. This is an especially difficult requirement with complex technology projects, due to their layers of design complexity and a multitiered global supply chain.

Currently, given this complexity of most ICT projects, it is difficult for any supplier to provide this sort of assurance/supply chain guarantee. Part of the problem is that until recently there had been no defined requirement for this type of process/system or any adequate description of what it takes to plan and provide end-to-end technology supply chain assurance. That has changed recently, primarily due to the recognition that elements of our critical infrastructure and national security systems may already contain poor quality and/or malicious items placed through insecure supply chains and slipshod sourcing.

Currently, efforts are increasing to address problems with embedded malware and counterfeits due to supply chain breakdowns and ultimately enabling compromised functional capabilities. These efforts are driving a need for supply chain assurance for select systems/capabilities. Coordination of this complex work requires a common and coherent set of control processes and activities, which will allow managers to understand the precise security status of any given component as it moves through design, manufacture, final product integration, testing, and assurance of a well-documented build of materials (BOM), which become well-maintained and dynamic BOM, due to strong configuration management for both hardware and software, throughout the life cycle. In that respect, an authoritative, mutually agreed-upon process for independently assuring organizational trust in sourced products becomes a necessity.

This is not a common situation today because of the distances and global elements of business. The ideal would be a well-defined (risk-based) process, with agreed-upon taxonomy, to evaluate and verify trust at all levels up and down the supply chain, to ensure that control is maintained through a formal and disciplined process. This overall control framework with well-defined processes, activities, and tasks has a good start in NIST 800-161 standards, practices, and controls for supply chain assurance. This is a critically enabling first step in the process of assuring globally sourced products, enabling trusted mission essential functions, through ICT SCRM.

Donald R. Davidson Jr.
Director, Cybersecurity (CS) Risk Management

Preface

Today's information and communication technology (ICT) organizations increasingly find themselves relying on others for their success. Historically, medium- and large-size organizations have spent less than a third of their budgets on purchased goods and services, having relied on internal sources for these. Today, those same organizations spend most of their budget on purchased commercial off-the-shelf (COTS) goods and services. This is in large part because of the advantages ICT organizations have found in strategies such as globalization, outsourcing, supply-base rationalization, just-in-time deliveries, and lean inventories. Additionally, many companies have consolidated operations both internally and externally to achieve economies of scale.

While globalization, extended supply chains, and supplier consolidation offer many benefits in efficiency and effectiveness, they can also make supply chains more brittle and can increase information security risks that can lead to supply chain disruption. Historic and recent events have proven the need to identify and mitigate such risks. Recent political accusations have shown how security breaches can extend well beyond domestic boundaries and interfere with international trade and disrupt many elements of global supply chains, including supply, distribution, and communications. In extreme cases, a single security breach at one location can severely interfere with the capabilities of an organization.

Effective supply chain risk management (SCRM) is essential to a successful business. It is a competence and capability many enterprises have yet to develop. In some areas, both problems and practices are well defined. In others, problems are defined, but practices are developing. In still other areas, both the definition of the problems and the practices needed to address them are developing. In sum, SCRM is an evolving field.

It is important to note that ICT security risk cannot be eliminated. Because of its complex nature, various tools can be used to give organizations and governments the ability to build up an overall picture of the risk situation and plan a mitigation strategy to address critical areas. Likewise, with the growing emphasis on globalization, business process outsourcing, and the need to control terrorism, there is a greater need to understand and handle supply chain vulnerabilities throughout the entire life cycle from agreement to procurement and operation.

Guidelines for managing information security risk were developed by the National Institute of Standards and Technology (NIST) in March of 2011; they propose risk management practices at all levels of the organization and should be followed to facilitate adequate risk assessment, response, and monitoring (NIST SP 800-39). In 2015, NIST expanded the scope of the guidelines in the development of new guidelines (NIST SP 800-161) that address the ever-increasing implications of SCRM while incorporating the requirements of specific management, operational, and technical ICT security controls under the Federal Information Security Management Act. Until now, however, there has not existed an "easy-to-understand" approach for implementing NIST SP 800-161 parallel to the definitions of other international standards, such as ISO/IEC 12207, for the purpose of providing security mechanisms within end-to-end ICT supply chain agreement, procurement, and operation that lead to a comprehensive capacity maturity model.

This book is based upon the belief that the acquisition process is a strategic planning and governance concern. The solution is a formally defined and implemented infrastructure of best practices aimed at specifically optimizing the coordination and control of the acquisition process across the organization. As with any complex process deployment, this can only be substantiated through a rational and explicit framework of auditable procedures. The creation and deployment of those procedures is at the core of what is being presented.

One of the underlying premises of this book is to detail the reasons why formal organizational processes and methods for acquiring secure products are valuable. You will see how fundamental security activities provide the basis for the most effective assurance of the technology used. You will also discover the importance of expert advice concerning the best practices for building these formal processes. Since continuous capability improvement is the essence of maintaining an effective security posture, we will describe a maturity model-based approach to acquisition process improvement.

Who Should Read This Book?

This book will provide a valuable insight to anyone who acquires technology products. This includes COTS and government off-the-shelf products as well as the participants in the supply chain at any level. However, given the management focus, it would be particularly useful to process architects and higher level executives responsible for assurance of the technology infrastructure.

This book can also serve as a good general knowledge text for general interest practitioners. Since the ideas have practical business application, they seem highly attractive to any manager responsible for acquiring any form of complex products. The inclusion of a maturity model in Chapter 7 makes it especially attractive to strategic planners and any other type of security policy manager or upper level strategic decision-maker.

In a very detailed and organized fashion, this book presents the concepts of secure acquisition and ICT SCRM operations as an all-in-one concept. As such, there is no assumption about specialized knowledge. You will learn how to create a systematic and secure acquisition process as well as how to create a risk-based control structure for all levels of the supply chain. You will learn how to establish systematic sustainment and reporting within this structure and how to increase its capability.

This revolves around the steps to define the standard processes, activities, and tasks for the customer–supplier relationship, the attendant control objectives, and the auditing and reporting systems for the supply chain. Guidance for carrying this out is supported by expert standards of best practice, which are commonly accepted in the field and easily understandable.

At the end of this book, you will be able to

1. Implement a formal, organization-wide, standards-based trust in sourced products.
2. Define a comprehensive control structure to ensure continuous assurance.
3. Create a standard process to achieve higher stages of requisite capability.

Authors

Ken Sigler has been a faculty member of the Computer Information Systems (CIS) program at the Auburn Hills Campus of Oakland Community College in Michigan since 2001. His primary research is in the areas of software management, software assurance, and cybersecurity. He originally developed the college's CIS program option entitled "Information Technologies for Homeland Security" and correlated the relationship between that program and the Committee for National Security Standards of the National Security Agency. Mr. Sigler serves on the board of directors of the Colloquium for Information System Security Education (CISSE) and represents his college as the liaison to the Midwest Chapter for CISSE. Throughout his tenure at the college, he has also served as post-secondary liaison to the articulations program with Oakland County Michigan secondary school districts. Through that role, he developed a 2+2+2 Information Security Education process leading students through information security coursework at the secondary level into a 4-year articulated program, leading to a career in information security at a federal agency. Mr. Sigler is a member of the University of Detroit Mercy Center for Cybersecurity & Intelligence Studies Board of Advisors, Institute of Electrical and Electronics Engineers, Distributed Management Task Force, and Association for Information Systems.

Dan Shoemaker, PhD, is principal investigator and senior research scientist at the University of Detroit Mercy (UDM)'s Center for Cyber Security and Intelligence Studies. Mr. Shoemaker has served 30 years as a professor at the UDM with 25 of those years as department chair. He served as a cochair for both the Workforce Training and Education and the Software and Supply Chain Assurance Initiatives for the Department of Homeland Security and was a subject-matter expert for the NICE Workforce Framework 2.0. Mr. Shoemaker has coauthored six books in the field of cybersecurity and has authored more than 100 journal publications. He earned his PhD from the University of Michigan, Ann Arbor, Michigan.

Anne Kohnke, PhD, is an assistant professor of information technology (IT) at Lawrence Technological University, Southfield, Michigan. After a 25-year career

in IT, Anne transitioned from a vice president of IT and chief information security officer (CISO) position into full-time academia in 2011. Anne's research is focused in the areas of cybersecurity; risk management; threat modeling; and user's attitudes, decision making, and comprehension of the risks of installing Android mobile applications. Anne has coauthored four books in the field of cybersecurity and earned her Ph.D. from Benedictine University.

This text is one of several titles these three authors have written on the topics of cybersecurity, risk management, and security controls within the Taylor & Francis Internal Audit and IT Audit Series. Other titles include *The Complete Guide to Cybersecurity Risks and Controls* (2016), *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework 2.0* (2016), and *Implementing Cybersecurity—A Guide to the National Institute of Standards and Technology Risk Management Framework* (2017).

Contributions

The collaborative work of the authors would not be successful without the organizational assurance and support of Tamara Shoemaker, who continues to be a solid rock for each of the authors and thoroughly enjoyable to work with. In addition to her role, affectionately referred to as *The Boss*, Shoemaker is the director of the University of Detroit Mercy's Center for Cybersecurity and Intelligence Studies. Additionally, Shoemaker serves in the capacity of operations manager for the Colloquium for Information Systems Security Education (CISSE).

None of our titles would be successful without the continued guidance and support of our acquiring editor, Rich O'Hanley, and the lead to the Internal Audit and IT Audit Series, Dan Swanson. Much thanks is also extended to the project management and editorial staff that helped bring this book to successful publication.

Chapter Structure and Summary

Chapter 1: Why Secure Information and Communication Technology Product Acquisition Matters

The goal of this chapter is to demonstrate how a formal approach to acquisition security can be used to ensure the integrity of the technology base of an organization. The key concept here is "across-the-board trust." Because ALL of the potential components of the technology base are involved in the secure functioning of the system, every aspect of that base must be trustworthy. The reader will discover how formal processes and a standard point of reference are necessary to establish adequate trust.

Chapter 2: Building a Standard Acquisition Infrastructure

Two standards are relevant to the definition of a robust acquisition assurance infrastructure. At the concept level, this is the customer–supplier process defined in the "Agreement" processes of the ISO/IEC 12207 Standard. This standard has been widely accepted for over 20 years as the authoritative definition of what, at a minimum, must be undertaken to achieve proper technology acquisition. These standard recommendations can then be tailored into a specific process for any given organizational application. Thus, the need for a single, fully defined infrastructure is a precondition for the definition of the body of knowledge for secure supply chain risk management. As such, the remainder of this book will outline the means to specifically implement the recommendations of the NIST IR 800-161 model within the larger ISO/IEC 12207 Agreement process. The aim is to detail

how these explicit recommendations for customer, integrator, and supplier performance fit and work with the 12207 requirements for proper customer–supplier relationships.

Chapter 3: The Three Building Blocks for Creating Communities of Trust

In this chapter, you will learn why a formal, comprehensive, standards-based definition of the activities and tasks necessary to ensure trust is critical to the process. The elements of the product supply chain are hard to identify, let alone ensure. Due to its layers of complexity, this is a difficult task to perform with complex technology development and integration projects, particularly given the fact that most products are integrated up a multilevel supply chain that is often offshore based.

The aim of this chapter is to give an overview of the only existing standard framework for the practice of comprehensive control over complex builds. Most products are developed in multilayered, multivendor, and even multicultural team settings. In order to ensure trust, all of this must be fully coordinated and controlled up and down the supply chain. Coordination of this degree of complex work requires a common and coherent control process and control activities, which will allow managers to understand the exact security status of any given component as it moves to final product integration, testing, and assurance.

Chapter 4: Risk Management in the ICT Product Chain

The process of risk management (identifying and controlling information as it is created within the supply chain), risk identification (examining, documenting, and assessing the security concerns represented by a given component within the supply chain), and risk control (applying controls to reduce identified risks), as well as prioritizing its importance will be described here. It is hard to ensure against threats to the components of an evolving product because the development process is normally dispersed across a number of organizations at various levels of integration. That is potentially risky because any breach of the product development chain can compromise the entire product. The term "weakest link" applies here. Also, there is the issue of offshore development of COTS products. Work across organizational boundaries as defined by agreement is the basic approach to the development of most complex technology products. But most of these relationships are undefined. Software in particular is intangible and dynamically changeable. Thus, it is almost impossible to get an exact understanding of product status as it moves up the development chain. Consequently, explicit and trustworthy risk control processes have to be applied at all levels of the supply chain.

Chapter 5: Establishing a Substantive Control Process

It might seem a little simplistic to say that the problem with developing any complex technology is that it is too complex. But the fact is that control must be established at all levels up and down the supply chain in order to be able to say with certainty that the product can be trusted. The only way to ensure that control is through a formal and disciplined process of assurance. This is the role of a formally constituted and organizationally sanctioned set of processes, activities, and tasks, which have been formulated into a standard acquisition control structure. The problem lies in knowing exactly what constitutes the elements of proper behavior. Thus, this text will present the only existing standard recommendations for the activities needed to ensure the acquisition process. This includes the description of the overall control framework itself as well as the processes, activities, and tasks that the organization must undertake to establish actionable behaviors that can be audited for compliance with the recommendations of standard best practice. In this respect, the ISO 12207 Agreement process will be mapped to the recommendations of NIST 800-161 in order to describe a top-to-bottom concept of secure acquisition assurance. The aim is to help you understand how to establish a standard and auditable secure acquisition process. This includes methods for initiating, planning, executing, and following up/remediating active behaviors for the purposes of systematic control. It includes the definition and assignment of all roles and responsibilities for every participant in the supply chain—customer, supplier, and integrator—and the best practices for documentation and reporting of control information to appropriate sources.

Chapter 6: Control Sustainment and Operational Assurance

The only way to ensure proper implementation of a critical process is through the routine operational sustainment of the active controls that constitute it. This in essence involves tailoring, deploying, and validating a suitable set of behavioral controls and then monitoring their integrity and effectiveness throughout the life cycle of the acquisition process. Basic steps must be carried out to ensure systematic integrity no matter what the actual situation might be. It is necessary to validate the selected control set to assure the effectiveness as well as confirm the accuracy of the defensive scheme. Thus, it is necessary to conduct regular monitoring testing and analysis of the complete set of acquisition assurance activities to understand its status and functioning. This includes steps to detect any malfunctioning within the control set and procedures to ensure that subsequent corrective action will be undertaken.

Sustainment operations begin after the acquisition process is operationally deployed. The sustainment process is planned, implemented, and monitored in the

same fashion as any other organizational-level activity. It normally embodies the criteria and factors for judging success. The intention is to be able to say with assurance that the aggregate controls for any given acquisition are effective given the aims of the organization. Operationally, this should take place within a defined reporting and decision-making structure. Because the overall purpose of assurance is to produce a trustworthy assurance outcome, the outcome of sustainment is continuous assurance of process correctness.

Chapter 7: Building a Capable Supply Chain Operation

The role of any form of assurance process is to ensure continuing confidence in the products that are being acquired. However, since managers do not actually do the work, and the product is normally too complex to understand anyway, the organization has to adopt and utilize some form of standard control process in order to ensure product integrity. A capability-based process ensures that reliability and integrity are designed for and built into the products in the first place rather than added on at the end.

The assurance of the proper functioning of the control process is what actually certifies the correctness of the product. In that respect, the aim of all technology assurance activity is to ensure the continuous trustworthy and reliable functioning of all of the deployed controls. Process capability improvement provides a given organization with a template for continuous adaptation and improvement. The assumption is that a technology management system that is based on and follows a commonly accepted model of best practice ensures best-of-breed acquisition assurance. The problem is how to get there. The objective of this chapter is to provide a standard model for capability maturity development for any organization. The assumption is that capability is attained in easy-to-accomplish stages rather than in one impossible leap. Capability maturity models have been utilized in a number of high-technology settings for years. Their general form is well understood and adaptable to the standard practices we are discussing here. Thus, we will specify and describe what needs to take place in a practical sense in order to implement such an approach to acquisition security.

Chapter 1

Why Secure Information and Communication Technology Product Acquisition Matters

At the conclusion of this chapter, the reader will understand the following (Figure 1.1):

- The role and importance of a formal sourcing process in ensuring organizational security
- The standard elements of acquisition management practice
- The concerns and issues associated with insecure supply chains
- The general structure and principles of the ICT supply chain risk management (SCRM) process
- The nine large elements of formal ICT SCRM
- The role and importance of standard models of best practice

Introduction to the Book

The purpose of this book is to ensure an understanding of the strategic process of trusted product acquisition, which is directly associated with the discipline of SCRM. This chapter will introduce the concepts and principles of formal trusted

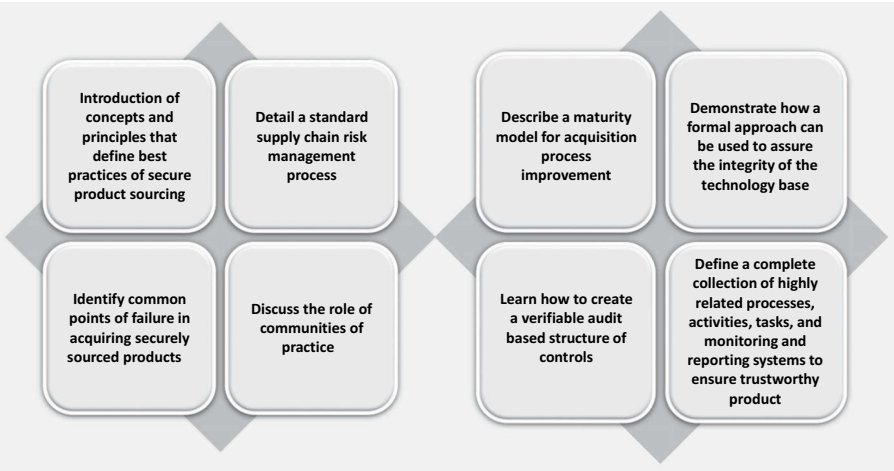

Figure 1.1 Objectives of the book.

product acquisition governance as well as the standard principles and underlying activities that define best practice in the performance of secure product sourcing.

This book will also detail a standard SCRM process that is integral to securing ICT acquisition in a global business environment. It will identify the common points of failure in acquiring adequately secure sourced products, and it will explain the factors that drive those failures. Readers will see how difficult it is to acquire ICT products that are trustworthy and secure, and they will understand the fundamental causes of that difficulty. Readers will discover the role of communities of practice in the overall process of building a complex ICT product, and since continuous capability improvement is the essence of maintaining an effective security posture, Chapter 7 will describe a maturity model for Acquisition Process Improvement.

The goal of this chapter is to demonstrate how a formal approach to acquisition and supply chain security can be used to assure the integrity of the technology base of any organization. The key concept here is "across-the-board trust" because *all* of the potential components of the technology base are involved in the secure functioning of the system. Consequently, every aspect of that base must be dependably secure or "the weakest link" applies. The reader will discover how formal processes and a standard baseline reference are necessary to establish that requisite level of trust.

Underwriting Trust and Competence

The vast range of ICTs have created our digital culture. Consider that 30 years ago you could not shop, bank, buy stocks online, play games, or interact with people on a mobile device. Now that is all possible, and new opportunities seem to pop up at an unthinkably frantic rate. At the same time, because of the dependence on the

Internet, it is critically important to be able to trust the security and integrity of all of our ICT products, and that is demonstrably not the case.

According to the Privacy Rights Clearing House, close to one billion consumer records have been lost or stolen over the last decade. According to McAfee and the Center for Strategic and International Studies, that translates to $300 billion to $1 trillion in annual loss. Therefore, it is not surprising that industry and government have decided to address the problem of ICT product security. Just like buying a suit off the rack rather than having it bespoke tailored means that the customer will get it faster and cheaper, the business logic makes it inescapable for most modern companies to purchase rather than develop their own ICT products. Businesses want their solutions now, not at some time in the indeterminate future, and they do not want to spend the R&D money to back the development of custom packages. In many respects, because solutions are purchased rather than built, the procurement staff is as critical to the security of the ICT operation as the technical staff.

An organization's ICT procurement process is no different from any other purchasing function in that the purpose of any procurement activity is to acquire an effective product for the organization. Consequently, whether the product is a video game or a piece of sophisticated military hardware, the activities that take place within the acquisition process have to be logically related, controlled, and coordinated. A standard model of the best practices to be carried out within that process simply ensures that the control is implemented systematically and is effectively maintained through the specific actions of the individuals who are responsible for performing the assigned task.

From a security and integrity standpoint, what this implies is that every individual action in the overall process has to be rationally and properly placed in the timeline for execution. Additionally, each task must be fully and correctly integrated into the overall activity. Therefore, at its core, the acquisition process that will be discussed here must be well defined and properly executed. It must ensure that proper relationships are maintained among the larger set of actions that have been arrayed to achieve a given purpose.

Justification and Objectives of the Book

Perhaps the best way to justify this book is the statement that it has been long overdue. Technology systems are complex and their elements are indistinguishable by normal inspection. Thus, the usual way to acquire trustworthy ICT products has been to only deal with suppliers who are "known and trusted" over a reasonable period of time. Even so, in a modern global sourcing environment, a trusted supplier has the potential to integrate subcomponents that are obtained from untrustworthy sources into a system. Therefore, when it comes to acquiring the technology needed, any purchaser of an ICT product is essentially "buying a pig in a poke," so to speak. This is a particularly egregious situation given

the "faster-cheaper-better" mentality of current companies, and it has led to an overreliance on suppliers' commercial-off-the-shelf (COTS) system security to leverage development strategies.

The problem is that until recently there has been no common body of knowledge that can be relied on to provide a standard set of practices for executing secure, end-to-end technology purchases. Fortunately, this has changed primarily due to the dawning recognition that elements of our critical infrastructure may already contain malicious items, which have been placed there as a result of insecure supply chains and a slipshod open-source acquisition process.

The ideas presented in this book are well-established aspects of a single process that has been developed and promulgated by the federal government to ensure trusted product acquisition in its particular space. Specifically, this book presents the concepts of ICT SCRM from the perspective of NIST SP 800-161, which is the first standard body of knowledge for secure SCRM (NIST, 2015). In this book, you will learn how to create a verifiable audit-based structure of controls, which will ensure comprehensive security for all types of sourced ICT products. We will explain how to establish systematic security within the supply chain as well as how to build auditable trust into the products and services that are acquired by the organization.

In addition, we will detail a unique capability maturity development process that will help foster an increasingly competent process. The overall aim of this book is to define a complete and correct collection of highly related processes, activities, and tasks as well as the attendant monitoring and reporting systems to ensure a trustworthy product. A practical and standard means of leveraging the acquisition process to higher levels of capability maturity is also explained in this text. The details of this process are captured in a very well-known and widely accepted approach to capability maturity development. Thus, the information in this book is both authoritative and commonly agreed upon.

The Five-Part Problem

As we said in the last section, this book centers on the belief that SCRM is a strategic governance concern. Thus, the practical governance solution to the acquisition process is a formally defined and concrete infrastructure of best practices, which are aimed at ensuring sufficient coordination and control over the entire process. The objective is to ensure that all sourced products fall within certain levels of trust. As with any complex goal, the assurance of product trustworthiness can only be substantiated through activities that take place within a rational and explicit framework of auditable procedures. Thus, the basis for creating and deploying these procedures is presented in this chapter.

The General Accounting Office (GAO) summarized the concerns associated with organizational ICT SCRM in a March 23, 2012, report. ICT risk issues fall

into five categories, each of which has a slightly different implication 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" (GAO, 2012, p. 1) (Figure 1.2).

Malicious logic is embedded in a product to fulfill some specific purposes. Malicious objects are by definition not part of the intended functionality; therefore, in order to find and eliminate any instance, rigorous testing and inspection is required. Embedding a malicious object in a product is always a hostile act, and assurance that a product is free of malicious code should be a high priority with any ICT customer. Nonetheless, since it is hard enough to ensure the quality and security of the functions that *ought* to be present in a piece of software, it is asking a lot to expect that functions that should *not* be present should also be identified and eliminated. Therefore, it is almost impossible to estimate how much malicious code currently resides in ICT products. Because the decision to embed a piece of malicious logic in a product is intentional, one of the most effective ways to ensure against the presence of such objects is to maintain strict oversight and control over ICT development, sustainment, and acquisition work.

Counterfeits are not just an acquisition issue. Counterfeit parts can appear at any stage in the development and sustainment of ICT products. Counterfeits execute product functions as intended and threaten product security and integrity because they are not the same as the actual part. Generally, the purpose of a

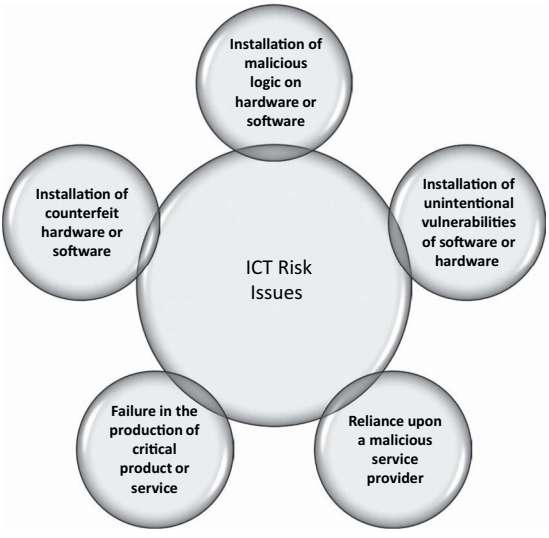

Figure 1.2 ICT risk issues.

counterfeit is to save money or supply a feature that the maker is otherwise incapable of providing. As a result, counterfeits embody shortcuts in product quality or security that can fail in many ways. Because they function like the original part, it is often hard to spot a counterfeit in a large array of legitimate components. Therefore, it is critically important that customers fully and completely understand their supplier's business and technical practices prior to engaging in any use of the products. A capability model is particularly helpful in enforcing that understanding since it establishes a common and auditable basis between organizations.

The problems caused by breakdowns in the supply chain mirror the problems encountered in conventional manufacturing, in that the failure lies in the inability to do the work due to the lack of a component. The same is true with the technical service concern. From the standpoint of product security, a failure to deliver a critical part prevents the ICT product from being used, which is the equivalent of a denial of service in conventional security terms. Thus, efforts to mitigate security risks or risks to product integrity tend to concentrate on identifying and managing single points of failure. Capability models help in that respect because they establish common management functions designed to monitor and control the overall process of construction or maintenance.

From a technical service standpoint, the focus is on learning whether the supplier's operation is capable of delivering the product as specified. Since supplier capability is at the center of any acquisition or outsourcing decision, it is important to find out in advance whether the contractors that comprise the supply chain possess all of the capabilities required to do the work. Specifically, suppliers have to prove that they are capable of developing and integrating a secure product. Overall capability is usually demonstrated by the supplier's past history with similar projects as well as their documented ability to adopt good software engineering practices. A commonly accepted and fully auditable model of best practice shared by the customer and the supplier helps to cement that assurance.

The issue of unintentional vulnerabilities is just a specific application of the overall development and sustainment problem in that defects in software and hardware occur because of failure in the process. By definition, the installation of unintentional flaws is not a hostile act; however, since the problem is so pervasive, the sheer number of exploitable vulnerabilities placed in ICT products makes unintentional flaws and defects a major concern.

There is an extensive body of knowledge in ICT product assurance; however, since the steps necessary to ensure product integrity have to be instituted, managed, and sustained in a logical way, best practices are often not followed or performed half-heartedly. The result is that common defects in ICT products are exploited by a growing array of criminal and other bad actors. The installation and sustainment of a commonly accepted capability model addresses this concern directly. Nevertheless, it is critical that the activities in that model be executed in a continuous and disciplined fashion.