MANAGING SUPPLY CHAIN RISKS TO DOD SYSTEMS AND NETWORKS

Thomas Barth, Michelle Albert, and Elizabeth McDaniel

The Problem

Global supply chains are vulnerable to attack or manipulation. If an adversary compromises an information communications technology (ICT) component by exploiting vulnerabilities associated with its supply chain, that component can become a system risk. ICT supply chain risk management (SCRM) relies on an in-depth understanding of the risks inherent to global supply chains and the means by which to mitigate or manage those risks.

IDA's research on ICT SCRM issues and responses contributes to the system security and performance of DoD systems and networks.

The environment in which the Department of Defense (DoD) acquires, builds, and operates national security systems is increasingly globalized. DoD weapon systems, business systems, and computer networks are dependent on commercial information communications technology (ICT) and ICT-enabled components. These components are designed, manufactured, packaged, and delivered to end users through global supply chains that create interconnected webs of people, processes, technology, information, and resources around the world (Figure 1).

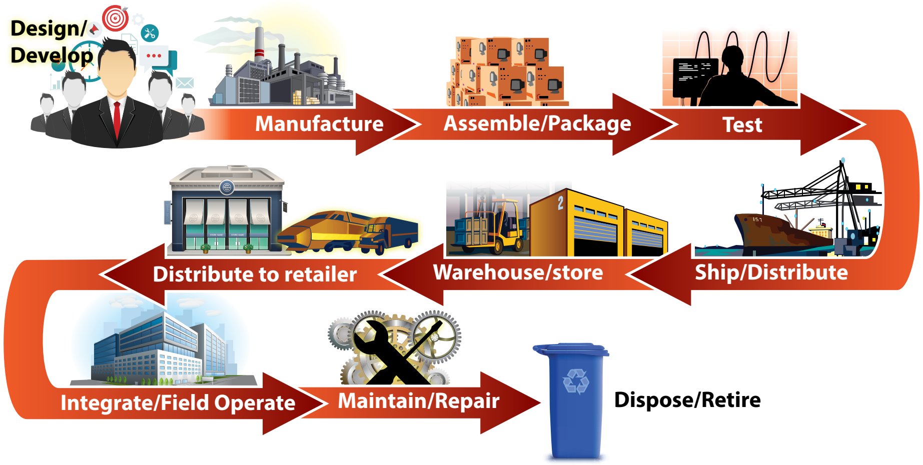


Figure 1. The Supply Chain

These supply chains give DoD access to available technologies and innovations, but they also provide adversaries with opportunities to tamper with ICT components by introducing malicious code, reverse-engineering the components to access design information, finding or adding vulnerabilities they can later exploit, or inserting counterfeit parts that may increase failure rates in systems or provide additional avenues for exploitation.

The DoD Chief Information Officer (CIO), the office responsible for DoD's supply chain risk management policy, leads risk-reduction activities for DoD's acquisition programs. For over a decade, IDA has supported the DoD CIO's efforts to enhance supply chain risk management (SCRM).

Traditionally, the term SCRM refers to the logistics associated with obtaining needed components, a major concern of companies. ICT global SCRM, on the other hand, deals with targeted threats; as such, assessing and managing risk for the security of the systems requires a different set of tools. IDA's research on ICT SCRM issues and responses contributes to the system security and performance of DoD systems and networks.

ICT SCRM AWARENESS MODULE

In support of the DoD CIO, IDA published an education, training, and awareness module to promote awareness of the risks inherent to the ICT global supply chain and to increase understanding of ICT SCRM. The module captured then-current DoD policies and processes. It has a flexible format that allows for revision when policies and/or processes change and for customization for various audiences. The module, which covers SCRM throughout the acquisition lifecycle, is organized around three themes:

Theme 1. The New Insider Threat Is Not a Person – It's ICT

Theme 2. Supply Chain Risk Is a Condition To Be Managed, Not a Problem To Be Solved

Theme 3. Take Action To Manage Global Supply Chain Risk

THE NEW INSIDER THREAT IS NOT A PERSON – IT'S ICT

Theme 1 identifies the elements of SCRM and explains the national security risks associated with global supply chain exploitation. The module defines ICT as technology used for gathering, storing, retrieving, and processing information, including microelectronics, printed circuit boards, computing systems, software, signal processors, mobile devices, satellite communications, and networks.[1]

Today, most of the ICT components used in DoD systems and networks are obtained from commercial sources. These commercial products take advantage of global talent, resources, and manufacturing capabilities, and typically can be purchased at lower cost than other products. However, the globalization that lends these advantages also creates supply chains that are often opaque and difficult to trace, thereby creating security challenges. Products traverse borders and companies many times on their way to the end user and their point of integration into DoD systems or networks.

[1] IDA adapted this definition from DoD Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, and NIST Draft IR 7622, *Notional Supply Chain Risk Management for Federal Information Systems.*

Supply chain attacks can occur throughout the DoD system development lifecycle; entry points for exploitation and manipulation include component design, manufacturing, transport, delivery, installation, and repair or upgrade. Figure 2 illustrates a notional supply chain and highlights possible entry points for an adversary to manipulate or tamper with a component.[2]

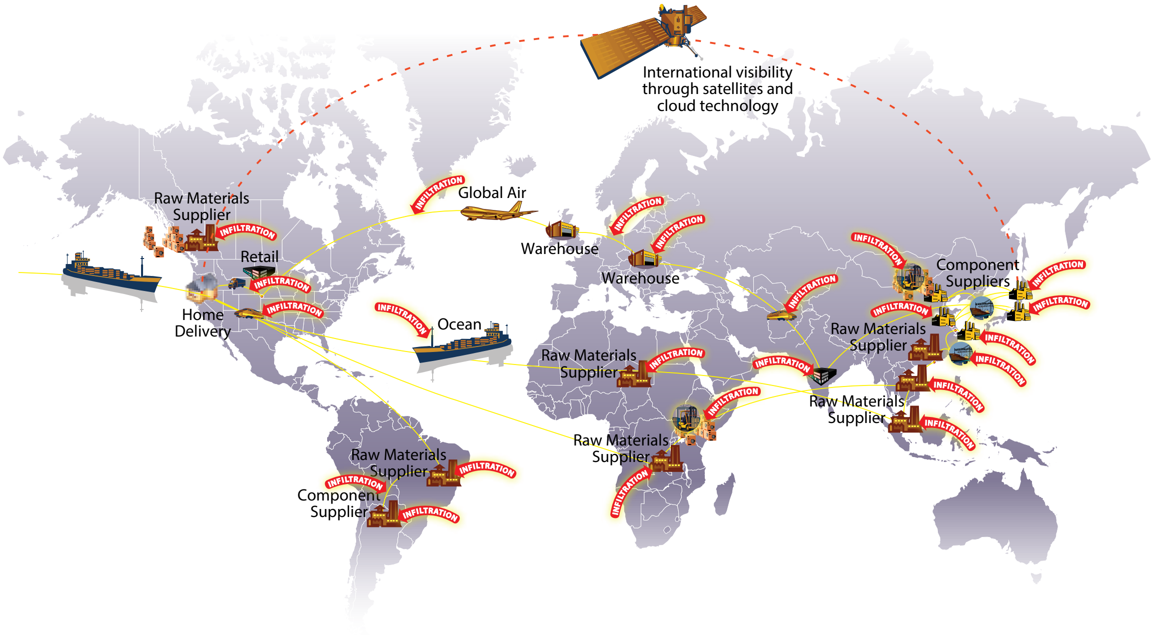


Figure 2. Manipulation along the Supply Chain

As an ICT component traverses its supply chain, it passes from country to country, company to company, and person to person. Each company has its own logistical security standards, and ICT components are often stored or transported in ways that leave them open to tampering. The notional points of manipulation in Figure 2 illustrate vulnerabilities in the supply chain environment that create opportunities for specific attacks. The impacts of such attacks can be disruption of service, insertion of malicious functionality, data exfiltration, and theft of intellectual property. The goal of supply chain risk management is to reduce a component's or system's susceptibility to supply chain threats and the potential impact of those threats.

[2] In the awareness module, components and systems obtained through simple procurement or as part of the Defense Acquisition Management System (DAMS) are described as having system development life cycles that span design through disposal. The module refers to the Joint Capabilities Integration Development System (JCIDS) process as the Requirements phase. The module combines some other DAMS phases for ease of understanding. The Acquisition phase refers to design, development, testing, production, and deployment; the Operation and Sustainment phase refers to operations and support; and the Disposal phase refers to system or component disposal.

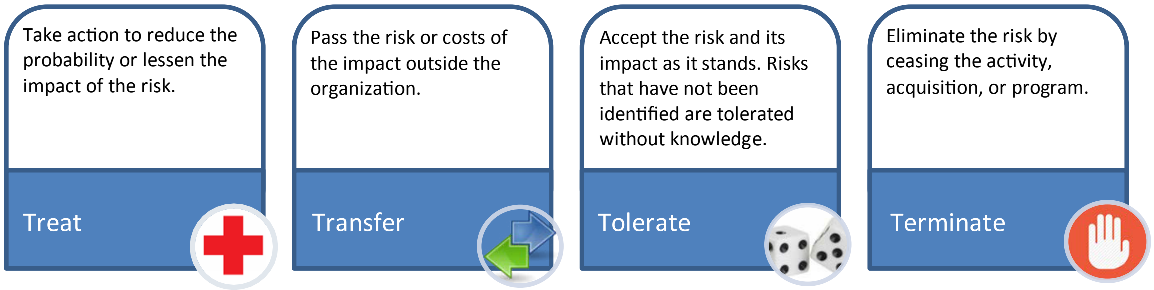
SUPPLY CHAIN RISK IS A CONDITION TO BE MANAGED, NOT A PROBLEM TO BE SOLVED

Theme 2 explains why supply chain risks must be managed, discusses the key concepts of risk management in the context of ICT SCRM, and offers a range of responses to identified risks. It is not possible to anticipate or eliminate every vulnerability, so risks must be managed. And, since everything is connected today, one ICT component that has been tampered with in a DoD system or network can affect that one system or multiple systems. Risk management must be considered for every ICT component purchased or integrated into a system.

ICT SCRM begins with identifying critical components and functions, vulnerabilities, and threats to the supply chain, and developing strategies to respond. Limits on time and money require DoD to focus on risks to mission-critical functions, those functions that, if compromised, could degrade a system's ability to meet its core mission.

If the assessed risk is high, DoD has four basic responses: treat it, tolerate it, transfer it, or terminate it (Figure 3). Treating the risk means applying countermeasures and mitigations to lessen the consequence of a compromised component or system by incorporating risk management strategies throughout a component or system's life cycle.[3]

Transferring, tolerating, or terminating the risk should be considered if it is better to treat the risk at a later time, if there are insufficient resources to treat it now, or if available treatment options do not reduce the risk to an acceptable level. SCRM options range from doing nothing, which entails no effort or extra costs up front, to redesigning a system to avoid using a component with unacceptable risk mitigation options, which involves more effort and higher costs.



Take action to reduce the probability or lessen the impact of the risk.

Treat

Pass the risk or costs of the impact outside the organization.

Transfer

Accept the risk and its impact as it stands. Risks that have not been identified are tolerated without knowledge.

Tolerate

Eliminate the risk by ceasing the activity, acquisition, or program.

Terminate

Figure 3. Four Responses to Identified Risk

[3] According to the Joint Doctrine, countermeasures are devices or techniques applied to impair the operational effectiveness of adversary activity. In the context of ICT SCRM, countermeasures prevent adversaries from exploiting supply chain or component vulnerabilities. Mitigations are actions taken to alleviate the risks or effects resulting from vulnerabilities in critical components or systems.

TAKE ACTION TO MANAGE GLOBAL SUPPLY CHAIN RISK

Theme 3 describes the current complex, dynamic, and evolving environment of relevant government and DoD policies, standards, and strategies that guide the management of supply chain risk across the phases of the system development life cycle. DoD has articulated requirements in Acquisition policy (DoD Instruction 5000.02, *Operation of the Defense Acquisition System*, and DoD Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*) and in cybersecurity policy (DoD Instruction 8500.01, *Cybersecurity*, and DoD Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*). In combination, these policies provide guidance on ICT SCRM for DoD personnel.

Although much of the available policy and guidance focuses on the acquisition phase, most warfighting, intelligence, and business systems, products, and services spend the majority of their existence in the operations and sustainment phase. Risk management is essential during the design and manufacture phases of acquisition, but it is also critical during operations, routine services, maintenance, and planned upgrades or modifications.

GOING FORWARD

The ICT Global SCRM Awareness Module was designed to prompt DoD personnel to care, think, and act in response to real risks that result from the supply chains of ICT products across the life cycle. It was designed to support the efforts of Combatant Commands, Services, and agencies to understand and implement DoD's policies effectively in the face of real threats to system security and performance.

The ICT SCRM Awareness Module on DVD is available upon request; email ETASCRM@ida.org. The module's introductory video is featured on IDA's website at https://idalink.org/ManagingSupplyChain.

Mr. Barth is a Research Staff Member in IDA's Information Technology and Systems Division. He holds a Master of Arts in strategic studies from the U.S. Army War College and a Master of Arts in military art and science from the School of Advanced Military Studies, U.S. Command and General Staff College.

Ms. Albert is a Research Associate in IDA's Information Technology and Systems Division. She holds a Master of Arts in Journalism from the University of Missouri.

Dr. McDaniel is an Adjunct Research Staff Member in IDA's Information Technology and Systems Division. She holds a doctorate in education: supervision, curriculum, and instruction from the University of Miami.