Managing Risk in Global ICT Supply Chains

Best Practices and Standards for Acquiring ICT
Managing Risk in Global ICT Supply Chains

Emerging best practices and standards can significantly reduce cybersecurity risks by helping organizations work closely with suppliers to track hardware and software products throughout their supply chains and lifecycles.

Information and communications technology (ICT) has become the lifeblood of modern civilization. People and organizations rely on ICT to support critical activities and missions.

ICT is created, supported, and integrated into complex, globally distributed networks of ICT supply chains, as depicted in Exhibit 1. These supply chains are not visible to, or well understood by, those who acquire and use the technology. This lack of visibility and understanding creates ample opportunities for intentional compromise of the IT components while they are being created, assembled, and delivered throughout the supply chain. In addition, poor manufacturing, software development, and delivery practices can also open doors for compromising these components after they are installed and operational.

As a result, many organizations face significant risk due to the high probability that the global IT infrastructure, including their own networks and systems, relies on tampered or tainted ICT components that could either stop working unexpectedly or compromise the data that is delivered, processed, and stored by the IT infrastructure.

Exhibit 1 | Modern ICT Supply Chains

Sources:
Diversified ICT Supply Chains Create Benefits and Risks

Diversifying the global ICT supply chains—from design and acquisition to integration, operation, maintenance, and disposal—provides numerous opportunities for cost-savings and flexibility. Unfortunately, it also introduces risks and creates opportunities for adversaries to compromise IT infrastructure. Within the last few years, the media has exposed examples of broken or infiltrated ICT supply chains, particularly with respect to counterfeit assets surfacing within US federal government networks, insertion of malicious code into critical infrastructure, and poor quality ICT design and development that resulted in disclosure of sensitive data and put US government missions and national critical infrastructure at risk.

ICT supply chains incorporate multiple levels of suppliers spanning multiple continents and produce anything from conventional ICT products (for example, servers, routers, mobile devices) to specialized components, legacy systems, and spare parts. The actors in these supply chains range from system integrators to software developers, hardware manufacturers (for example, chips and other logic bearing components), and media storage disposal providers.

Information and Communications Technology

- Encompasses all categories of technology used for gathering, storing, transmitting, retrieving, or processing of information
- Includes microelectronics, printed circuit boards, computing systems, software, signal processors, cell phones, satellite communications, and networks
- Can be a stand-alone component such as a software application or memory chip, a commodity (laptop), or part of a larger system (avionics in a jet airliner)

Examples of ICT Supply Chain Risks

- **Cost-driven Risks.** Cost considerations often drive decisions to obtain inexpensive parts, motivating less trustworthy suppliers to provide lower-quality parts that have faster degradation rates. Some suppliers knowingly flood the market with counterfeit items that do not conform to required standards.
- **Obsolescence.** Vendors discontinue hardware and software production as technology advances or business priorities change. This often results in the lifetime of a system significantly outlasting the lifetime of its components. System owners need to find alternative sources, some of which, unknowingly, are unauthorized suppliers. The only alternative is to perform costly upgrades or replace the systems. The defense and aerospace sector calls this phenomenon Diminishing Manufacturing Sources and Material Shortages (DMSMS).
- **Insertion of Malicious Content.** The insertion of “logic bombs,” “backdoors,” and “spyware” in microchips and circuit logic, firmware, and software can sabotage or subvert the components they supply.
- **Unintentional Supplier Activities.** Unintentional actions, such as errors in software coding, or overlooking faults due to inadequate hardware testing, can result in significant risks to system operation and integrity when the erroneous components are installed.
Incorporating ICT SCRM in Acquisition Decisions

Organizations should address the risks associated with geographically dispersed global ICT supply chains by changing acquisition processes for ICT-enabled systems and components. By integrating ICT Supply Chain Risk Management (SCRM) considerations into the entire system lifecycle—from initial planning and acquisition to disposal, they can increase efficiency and reliability of individual ICT acquisitions.

Acquirers are often unaware of critical supplier processes and practices that could impact their ICT infrastructures. They also often lack the skills required to understand and manage potential risks. Acquirers can mitigate risk by establishing explicit expectations with suppliers regarding specific supplier practices, and monitoring and validating these practices. For example, due diligence in the source selection process should include not just how and where the supplier does business, but the implications concerning how its business culture and practices may affect its readiness or ability to deliver trustworthy products or services.

Analyzing the global risks identified through better ICT supply chain visibility will allow organizations to take preventative measures to reduce risk exposure from malicious threats and intentional and unintentional non-malicious threats at all levels of the supply chain.

Working with ICT Suppliers to Manage Supply Chain Risks

Hardware and software used in ICT solutions have gone through a significant evolution over the last 20 years. Historically, one company could develop and provide a complete solution. The company would design, develop, and manufacture all of the hardware, or design and develop software, using proprietary models and dedicated employees. Today, ICT is assembled and integrated using components from a global web of suppliers. Companies acquire pieces from many providers and merge with or acquire business partners to create custom solutions to meet customer needs. An ICT supplier can simultaneously act as an acquirer and a supplier, depending on their placement in the supply chain.

Cost, schedule, and performance tend to be the factors that drive the risk management decisions of ICT suppliers today. As acquirers demand increased visibility into how ICT is put together, including proof of authenticity and integrity, suppliers are challenged with incorporating appropriate practices into the manufacturing or development lifecycle. Acquirers are using industry standards and best practices as a way

Key Acquisition Considerations

- What do you need to know about supplier practices to ascertain that critical components will perform as intended?
- What specific information can you request from suppliers to obtain appropriate visibility through the multiple tiers of supply chain?
- How much visibility into supplier IT development processes do you need?
- Does a supplier’s physical location present additional risks (for example, is the region prone to unstable political environments or natural disasters)?
- How are the risks of malicious, poor quality, or counterfeit IT components addressed in contracts and contracts oversight?
- Do suppliers have robust delivery practices that ensure that components are not tampered or tainted en route?
- How will the supplier be required to demonstrate compliance with your requirements?
- How will the supplier validate product and service integrity?
to articulate their expectations to suppliers, most of whom have a proprietary approach that may or may not be aligned with these standards. This results in a gap between acquirer expectations and supplier understanding of those expectations, creating further uncertainties about potential liabilities assumed by suppliers. At the same time, suppliers are incurring additional costs to demonstrate compliance with one or more standards.

Regardless of the development practices in use or the standards being required, suppliers must consider how they and their own suppliers are addressing basic acquirer expectations. The primary concern of most acquirers is that the resulting system remains operational within appropriate parameters under adverse conditions (such as an attack or service degradation), and that the information the system is intended to transmit, process, and store remains protected. According to the Software Assurance Forum for Excellence in Code (SAFECode), security and integrity controls are critical to suppliers’ ability to demonstrate that they have addressed acquirer concerns, including protection of intellectual property and the potential of counterfeit components in the supply chain.

Managing ICT Supply Chain Risk During Operations and Maintenance

According to multiple Department of Defense sources, operations and maintenance costs typically represent 60 to 80 percent of the total lifecycle cost of a system. At this level of investment, it is critical that ICT SCRM considerations are included in these sustainment activities to ensure that systems can be trusted to continue operating as intended throughout their life span. Planning for continuous operations and maintenance of the system should be initiated early in the acquisition cycle and include requirements determination, production, and fielding.

One of the challenges of sustaining system operation over the course of a system’s lifetime is replacing parts that break. In some cases, suppliers stop making them or go out of business, making it difficult to find genuine replacement parts to maintain intended system functionality. As a result, organizations are left with unattractive options, such as acquiring replacement parts from unverified third-party suppliers, which can carry multiple risks. For example, an unverified vendor might provide a counterfeit part that does not perform up to specification, or a part with malicious functionality that breaks the system or exposes the data processed and stored by the system to a malicious actor.

Key Supplier Risk Considerations

- What security requirements do you impose on your suppliers and how do you communicate them to the acquirer?
- How do you demonstrate compliance with security and supply chain requirements to the acquirer?
- How effective is your organization at demonstrating that the ICT you produce does not contain unwanted functionality?
- How do you and your suppliers obtain a common understanding of the future operating environment and its impact on deployment?
- How do you ensure that the system will function as intended within its operational environment in adverse conditions?
- What integrity and availability controls have your suppliers implemented to ensure the system remains operational in support of your mission?
- How are deviations from secure design and coding standards identified and resolved?
- How do you ensure your team members have the knowledge to deliver a product that meets the security requirements?
Risk mitigation should consider how critical the system is to the organization’s success, versus the costs and benefits associated with managing the supply chains that support sustainment of operational systems. For example, ICT used in-flight control systems or kidney dialysis machines should be more robust than ICT used in coffee makers.

For systems that are critical to the mission, the first step in solving this problem is determining which components would negatively impact the mission if they fail. The criticality of these components dictates that some components must be managed more carefully than others. Consider the consequences to the entire system if a particular component fails: Will the entire system fail or will operations unacceptably degrade? Will workarounds be possible until the problem can be corrected?

Supply chain threats to operational systems come from malicious and non-malicious sources, and through intentional and inadvertent actions. Managers must consider the combination of all of the threats and vulnerabilities when defining and implementing their strategy for mitigating supply chain-related risks to the health of operational systems.

**How Booz Allen Hamilton Can Help**

Booz Allen Hamilton, a management and technology consulting firm, has the technical expertise as well as the depth and breadth of ICT strategic planning experience to help clients manage supply chain risks associated with acquisition, operations, and maintenance of ICT systems and infrastructures. We have assisted US government agencies and the international community in defining and addressing ICT SCRM challenges.

Our holistic approach integrates the complementary aspects of people, policy, operations, management, and technology, and is based on emerging national and international best practices. Our suite of service offerings can help a diverse range of clients, from policy and acquisition organizations to operators of complex systems with critical ICT components. As we help our clients establish ICT SCRM practices, we identify and integrate internal standards and processes in cybersecurity, acquisition, quality, or other relevant areas that have already proven to be effective. For example, rather than recommend development of separate ICT SCRM acquisition requirements, we work to integrate ICT SCRM concerns into existing security requirements. Our ICT SCRM service offerings include:

- **ICT SCRM Policy Analysis and Development.** Emerging laws, standards, and best practices are influencing how regulatory bodies, government agencies, and industry stakeholders expect acquirers and suppliers to handle ICT SCRM, even as these requirements evolve. Booz Allen analyzes emerging standards and compliance drivers and compares them to the client’s current policies and processes. We identify existing internal standards that cover the new requirements, and make client-specific recommendations on how to develop new content to address those that are not covered.

- **Acquirer Self-Assessment.** Acquirers need to protect their assets by asking the right questions and engaging in appropriate validation activities to ensure their suppliers have addressed ICT SCRM and will continue to do so throughout the lifecycle. Booz Allen works with acquisition stakeholders to conduct a gap analysis of existing acquirer practices against a relevant baseline (NIST, ISO, DoD, or a combination as appropriate) and provides a comprehensive prioritized roadmap for closing the gap based on client resources and priorities. During this assessment, we identify existing best practices that can be repurposed or expanded to address ICT SCRM.
• **Cyber Supply Chain Vulnerability Analysis.** ICT supply chains consist of multiple nodes and delivery routes, all of which are vulnerable. Booz Allen analyzes the supply chain end-to-end and reverse-engineers it to find weaknesses through in-depth knowledge of adversarial tactics and methodology. We identify exploitable vulnerabilities that lead to cascading failures and anticipate what the adversary’s remedial actions will likely be, so we can inform, advise, and help clients develop viable courses of action.

• **Individual Component Assessment.** ICT is composed of a multitude of components, each of which can be compromised while it is created or transported for integration into a more complex device. A compromise of a critical component may result in a failure of the entire system, which could be devastating especially if it is operating as a part of critical infrastructure. Booz Allen conducts a detailed assessment of an individual component’s supply chain, identifies specific risks within that supply chain, and proposes a strategy to mitigate the identified risks.

• **Software Supply Chain Assessment.** Software presents special supply chain-related challenges because it is created and delivered virtually and does not lend itself to the same type of physical separation as hardware or other physical goods. Booz Allen analyzes acquirer and supplier software supply chain practices against emerging standards and guidelines and proposes a practical roadmap for remediation that includes governance and technical remediation.

• **ICT SCRM Training.** Although ICT SCRM recently received significant attention in the press, the public is generally unaware of the problem or the specific mitigation techniques. Booz Allen has developed basic training materials to address ICT SCRM awareness and works with the clients to tailor it to their key stakeholders across the organization. Our training helps clients integrate ICT SCRM considerations into acquisition and engineering efforts to ensure long-term risk management.

---

**A Leader in Defining and Implementing Best Practices for ICT SCRM**

Booz Allen has assisted numerous clients and served as a leader in promoting stronger ICT SCRM.

- Support of Department of Defense in defining and implementing ICT SCRM policies and practices
- ICT SCRM study for a large microelectronics manufacturer
- ICT SCRM framework for leading US bank
- Support of DMSMS Working Group and Counterfeit Materiel Working Group
- Leaders in software supply chain through co-chairmanship of multiple working groups under DoD, DHS, and NIST co-sponsored software assurance efforts
- Project Editor for international standard (ISO/IEC) 27036, *Information Security for Supplier Relationships*
Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, Booz Allen is a leading provider of management and technology consulting services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. In the commercial sector, the firm focuses on leveraging its existing expertise for clients in the financial services, healthcare, and energy markets, and to international clients in the Middle East. Booz Allen offers clients deep functional knowledge spanning strategy and organization, engineering and operations, technology, and analytics—which it combines with specialized expertise in clients’ mission and domain areas to help solve their toughest problems.

The firm’s management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. By combining a consultant’s problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm’s many client relationships that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 25,000 people, and had revenue of $5.59 billion for the 12 months ended March 31, 2011. Fortune has named Booz Allen one of its “100 Best Companies to Work For” for seven consecutive years. Working Mother has ranked the firm among its “100 Best Companies for Working Mothers” annually since 1999. More information is available at www.boozallen.com. (NYSE: BAH)

To see how Booz Allen can help your ICT supply chain risk mitigation efforts, please contact one of our consultants:

**Nadya Bartol**
Senior Associate
bartol_nadya@bah.com
301-444-4114

**Michele Moss**
Lead Associate
moss_michele@bah.com
703-377-1254
# Principal Offices

<table>
<thead>
<tr>
<th>Office Location</th>
<th>Address Location</th>
<th>City, State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Huntsville, Alabama</td>
<td>Indianapolis, Indiana</td>
<td>Philadelphia, PA</td>
</tr>
<tr>
<td>Sierra Vista, Arizona</td>
<td>Leavenworth, Kansas</td>
<td>Charleston, SC</td>
</tr>
<tr>
<td>Los Angeles, California</td>
<td>Aberdeen, Maryland</td>
<td>Houston, TX</td>
</tr>
<tr>
<td>San Diego, California</td>
<td>Annapolis, MD</td>
<td>San Antonio, TX</td>
</tr>
<tr>
<td>San Francisco, California</td>
<td>Hanover, MD</td>
<td>Abu Dhabi, UAE</td>
</tr>
<tr>
<td>Colorado Springs, Colorado</td>
<td>Lexington Park, MD</td>
<td>Alexandria, VA</td>
</tr>
<tr>
<td>Denver, Colorado</td>
<td>Linthicum, MD</td>
<td>Arlington, VA</td>
</tr>
<tr>
<td>District of Columbia</td>
<td>Rockville, MD</td>
<td>Chantilly, VA</td>
</tr>
<tr>
<td>Orlando, Florida</td>
<td>Troy, MI</td>
<td>Charlottesville, VA</td>
</tr>
<tr>
<td>Pensacola, Florida</td>
<td>Kansas City, MI</td>
<td>Falls Church, VA</td>
</tr>
<tr>
<td>Sarasota, Florida</td>
<td>Omaha, NE</td>
<td>Herndon, VA</td>
</tr>
<tr>
<td>Tampa, Florida</td>
<td>Red Bank, NJ</td>
<td>McLean, VA</td>
</tr>
<tr>
<td>Atlanta, Georgia</td>
<td>New York, NY</td>
<td>Norfolk, VA</td>
</tr>
<tr>
<td>Honolulu, Hawaii</td>
<td>Rome, NY</td>
<td>Stafford, VA</td>
</tr>
<tr>
<td>O’Fallon, Illinois</td>
<td>Dayton, OH</td>
<td>Seattle, WA</td>
</tr>
</tbody>
</table>

*The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com.*