ICT SUPPLY CHAIN RISK MANAGEMENT

Information and communications technology (ICT) is integral for the daily operations and functionality of U.S. critical infrastructure. From cell phones to cloud storage to satellite connectivity, the ICT supply chain encompasses the entire life cycle of hardware, software, and services and a diverse array of entities—including third-party vendors, suppliers, service providers, and end users. However, the globally distributed and interconnected nature of ICT also means that compromise of vulnerabilities in the supply chain can have cascading impacts across multiple critical infrastructure sectors.

The **Cybersecurity and Infrastructure Security Agency (CISA)**, through the **National Risk Management Center (NRMC)**, is working with partners and industry to identify and develop supply chain risk management (SCRM) strategies to mitigate and address supply chain risks. Enhancing the security and resiliency of the ICT supply chain is imperative for national security, economic security, and public health and safety.

RISKS TO THE ICT SUPPLY CHAIN

Supply chain risk is amplified by adversaries' attempts to exploit ICT technologies and their related supply chains for purposes of espionage, sabotage, and foreign interference activity. Vulnerabilities in supply chains—either developed intentionally for malicious intent or unintentionally through poor security practices—can enable data and intellectual property theft, loss of confidence in the integrity of the system, or exploitation to cause system or network failure. Increasingly, adversaries, including foreign adversaries such as Russia, China, North Korea, and Iran, are looking at these vulnerabilities as a principal attack vector.

Compounding the risk associated with supply chains is that vulnerabilities may be introduced during any phase of the ICT life cycle: design, development and production, distribution, acquisition, deployment, maintenance, and disposal. These vulnerabilities include malicious software and hardware; counterfeit components; and poor product designs, manufacturing processes, and maintenance procedures. Coordination between the public and private sector helps with the understanding of these vulnerabilities and sharing of expertise for developing solutions to global supply chain risk.

To learn more about the ICT life cycle, visit: cisa.gov/publication/cisa-scrm-essentials.

COLLECTIVE ACTION: ICT SUPPLY CHAIN RISK MANAGEMENT TASK FORCE

Public-private partnerships are central to CISA's collective defense approach to address the most significant risks to the Nation's critical infrastructure. In December 2018, CISA established the **ICT SCRM Task Force**—a public-private partnership focused on global ICT supply chain security. The Task Force is composed of a diverse range of professionals within the Information Technology and Communications Sectors with representatives from large and small private sector organizations and federal agencies. This includes subject matter experts, infrastructure owners and operators, and other key stakeholders who provide recommendations and guidance to help shape trusted supply chain practices.

Since its establishment, the Task Force has assembled an inventory of existing SCRM efforts across government and industry, and has launched working groups to:

- Study challenges and potential solutions around the bi-directional sharing of SCRM threat information;
- Identify processes and criteria for threat-based evaluation of ICT supplies, products, and services;
- Identify market segment and evaluation criteria for Qualified Bidder and Manufacturer List(s);
- Recommend how to incentivize purchase of ICT from original manufacturers or authorized resellers; and
- Develop a supply chain risk management assurance template for vendors

In addition, the Task Force has published two reports (the **ICT SCRM Interim Report** and the **ICT SCRM Report on Threat Scenarios**). To learn about the Task Force or to read the reports, visit cisa.gov/ict-scrm-task-force.

BUILDING RESILIENCE: RECOMMENDED ICT SCRM PROGRAM BASICS

Protecting your organization's information in a digitally-connected world requires understanding not only your organization's immediate supply chain, but also the extended supply chains of third-party vendors, service providers, and customers. These essential steps will assist your organization in managing supply chain risks and building an effective SCRM practice.

1. ***Identify*** the people: Build a team of representatives from various roles and functions of the company (e.g., cybersecurity, information technology, physical security, procurement/acquisition, legal, logistics, marketing, and product development). Ensure personnel at all levels are well-trained in the security procedures of their role or function.
2. ***Manage*** the security and compliance: Document the set of policies and procedures that address security, integrity, resilience, and quality. Ensure they are based on industry standards and best practices on how to conduct SCRM such as those from the National Institute of Standards and Technology (NIST).
3. ***Assess*** the components: Build a list of ICT components (e.g., hardware, software, and services) that your organization procures to enable your business. Know which internal systems are relied upon for critical information or functions, and which systems have remote access capability that must be protected to prevent unauthorized access.
4. ***Know*** the supply chain and suppliers: Identify your suppliers and, when possible, the suppliers' sources. In today's world of increased outsourcing, it is important to understand your upstream suppliers as part of the larger supply chain ecosystem.
5. ***Verify*** assurance of third-parties: Verify that your suppliers maintain an adequate security culture and SCRM program to appropriately address the risks that concern your organization. Establish the protocols your organization will use to assess the supply chain practices of your suppliers.
6. ***Evaluate*** your SCRM program: Determine the frequency with which to review your SCRM program, incorporate feedback, and make changes to your risk management program. This may also include auditing suppliers against practices and protocols established by your organization.

ICT SCRM RESOURCES

- ICT SCRM: cisa.gov/supply-chain
- ICT Supply Chain Essentials: cisa.gov/publication/cisa-scrm-essentials
- NIST Supply Chain Resources: https://csrc.nist.gov/Topics/Security-and-Privacy/supply-chain
- NRMC Resources: cisa.gov/nrmc-resources

For questions or to seek additional help, contact us at NRMC@hq.dhs.gov.