Cyber Supply Chain: An Approach to Assessing Risk

CANADIAN CENTRE FOR CYBER SECURITY
JULY 2022 | ITSAP.10.070

In today's digital world, cyber threat actors use supply chain weaknesses for malicious activity, and every link in a global supply chain can pose a threat to cyber security. Organizations with valuable information or services should strengthen their cyber security defense by identifying, assessing, and mitigating the risks associated with the global and distributed nature of Information and Communication Technology (ICT) product and service supply chains. Together, these elements form the basis of a robust cyber Supply Chain Risk Management (SCRM) strategy. Organizations are encouraged to follow the Cyber Centre's approach on page 2 of this publication to assess cyber supply chain risks.

Supply Chain Risk Lifecycle

Threat actors can influence products before they are even conceptualized.

Vulnerabilities can be introduced deliberately or accidentally during the design and production of a product.

Once the product is deployed, vulnerabilities can be discovered and exploited by threat actors during operation. Implementation of proper security controls within the environment is essential at this stage.

Products can be compromised during regular maintenance and patches, introducing new vulnerabilities or exploiting existing ones.

Cyber Centre's SCI Program: Providing Valuable Insights for the Government of Canada (GC)

The Cyber Centre's Supply Chain Integrity (SCI) Risk Assessment framework is a comprehensive program developed to perform assessments on ICT products and services that will be deployed onto GC infrastructure. The aim of the program is to safeguard the confidentiality, integrity, and availability of the GC's communications and data by fostering resilience against digital supply chain vulnerabilities and compromise.

Cyber Supply Chain risk assessments include recommendations for mitigation strategies and measures to help lower the risk against potentially vulnerable technologies, to ensure the protection of the GC's information, networks, and IT infrastructure.

The Cyber Centre recommends using Cyber Supply Chain risk assessments as an important input into an organization's existing risk management framework. If an organization uses the Cyber Centre's IT Security Risk Management: A Lifecycle Approach (ITSG-33), SCI risk assessments provide the inputs for security control SA-12(8). Another reference document that aligns with international standards is the Charter of Trust document Common risk-based approach for the Digital Supply Chain.

Communications Security Establishment | Centre de la sécurité des télécommunications

 Cat. No. D97-1/10-070-2022E-PDF ISBN 978-0-660-44134-4

Canada

Elements of Assessing Supply Chain Risk

There are several items to consider when evaluating your supply chain. The Cyber Centre uses a multistep approach to assess cyber supply chain risk for connected products and services which involves the following key elements:

Step 1: Determine the Sensitivity of the Technology

This assessment will be product-specific and should be conducted on a case-by-case basis. Sensitivity will vary depending on the specific context. Sensitivity should be assessed on a low/medium/high scale based on technological and contextual factors.

The Product

- **The Technology's function**-The role a product or service plays, and the impact on data Confidentiality, Availability, and Integrity if a compromise or disruption occurs.
- **Data processed**- The type of data processed by a product or service may affect the attractiveness of the system to cyber threat actors. Data classification and aggregation of data influence the sensitivity and associated risk.

The Context

Importance in the eco system- elements of Critical Infrastructure, Government networks of importance, and emerging disruptive technologies such as quantum computing or Artificial Intelligence may be considered highly sensitive.

The procurement- Monetary value and diversity in options.

Step 2: Assess Supplier Confidence

This assessment will be supplier-specific and should be conducted on a case-by-case basis. Confidence level in the Supplier: To determine a level of confidence in your suppliers, consider factors specific to their business, as well as their cyber security practices that align with international standards. ***The level of effort in Step 2 is dependent on sensitivity level***

The Supplier Ownership

- **Foreign Ownership, Control and Influence (FOCI)** - How closely linked is a company and the government of a nation where it resides, including the potential likelihood of being compelled to carry out activities counter to Canadian interests.
- **Geopolitical Context** – The location of a company's headquarters and operation centers, the legislative framework a company is bound to regarding data protection, and the domestic laws limiting exercise of government powers.
- **Business Practices** – Ethical behavior and adherence to legal and policy frameworks may indicate how trustworthy a company is. Transparent ownership, investment and contracting are also examined.

Cyber Maturity

Standards and certification-Adherence to international technology standards and certifications in design, production and maintenance of products and services.

Data protection -Products or services designed to provide confidentiality, authenticity, integrity and availability of data. Data should be protected from unauthorized access throughout the data life cycle.

Cyber security policies -Proactive cyber security policies and safeguards, and security vulnerability management help to determine a company's cyber security maturity.

Step 3: Determine Your Deployment

Deployment models should be assessed for each product and be aligned to your organization's internal posture. Consider the deployment in the context of your organization's security posture. Determine whether the risk exposure from a specific supplier is acceptable, if stronger mitigations need to be put into place, or if an alternate technology or supplier needs to be selected to achieve the business function. The results of this assessment will determine appropriate mitigation measures, largely based on the security controls outlined in the Cyber Centre's *IT Security Risk Management: A Lifecycle Approach (ITSG-33).*

Your Organization

Threat Actors and Tactics, Techniques, and Procedures - Looking at the lifecycle of supply chain, evaluate which threats the organization could face.

Cyber Defense Capabilities - Evaluate the security controls the organization has in place to protect against such threats.

Mitigation - The ability to implement mitigation advice to reduce residual risk.

Impact of Compromise and Resilience to Recover - Effective incident handling of hacking attempts or data breaches the company has faced.

Based on organizational capability, is the risk exposure acceptable?

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada