Guidehouse

The Critical Role of Supply Chain Provenance

Gaining a clear view of supply chain provenance is key to assessing and managing supply chain risk in a complex business landscape.

outwit complexity™

Guidehouse

One of the most vital parts of building a successful supply chain risk management (SCRM) program is understanding the provenance behind the assets, data, software and hardware, and intellectual property in your supply chain.

Supply chain provenance refers to understanding the origin or source, of goods and materials in a supply chain, and their "chain of custody." Managing supply chain provenance risk is, therefore, critical for both public and private sector organizations. Commercial businesses that fail to address supply chain provenance risk can face negative impacts, such as financial loss, operational disruptions, reputational damage, and legal liability. For government agencies, the risks can have broader economic, national security, and societal impacts.

In an ever-changing and complex business environment, critical organizations are increasingly the targets of both hostile state actors and hackers. As the threat ecosystem grows more complex, understanding the supply chain risk landscape and the origins of an organization's highly valued assets and their components becomes more challenging—and more important.

The global shift in the availability of goods; the possibility of counterfeit, reused, or substandard parts; cybersecurity and software vulnerabilities; and the need for alternative suppliers are formidable to navigate. Organizations often must now also uncover whether an entity in the supply chain has links to, for example, the Chinese Communist Party, China's defense establishment, the predominantly Uyghur Xinjiang region in China, or has been involved with intellectual property theft or human rights abuses.

A systematic and risk-informed enterprise-wide program is essential to identify concerns and safeguard production, systems, data, sustainment, maintenance, security, platforms, suppliers, and products. The key is first understanding the risks and vulnerabilities throughout the supply chain, then setting a strategy for mitigating them. Building and operating a SCRM program is a crucial element in this vigilance.

Guidehouse
outwit complexity™

Assessing Supply Chain Threats

Guidehouse's experience and research show that US companies and agencies will likely continue to face major supply chain threats and challenges for the foreseeable future, including:

Cyberattacks focused on suppliers and vendor systems

A single breached supplier can compromise a network of its business partners.

Complex procurement, fragmented systems, and inconsistent company or business unit practices

These characteristics make it difficult to uncover provenance, chain of custody, and associated risks, and could result in noncompliance with laws and regulations.

Increasing use of counterfeit and/or substandard parts

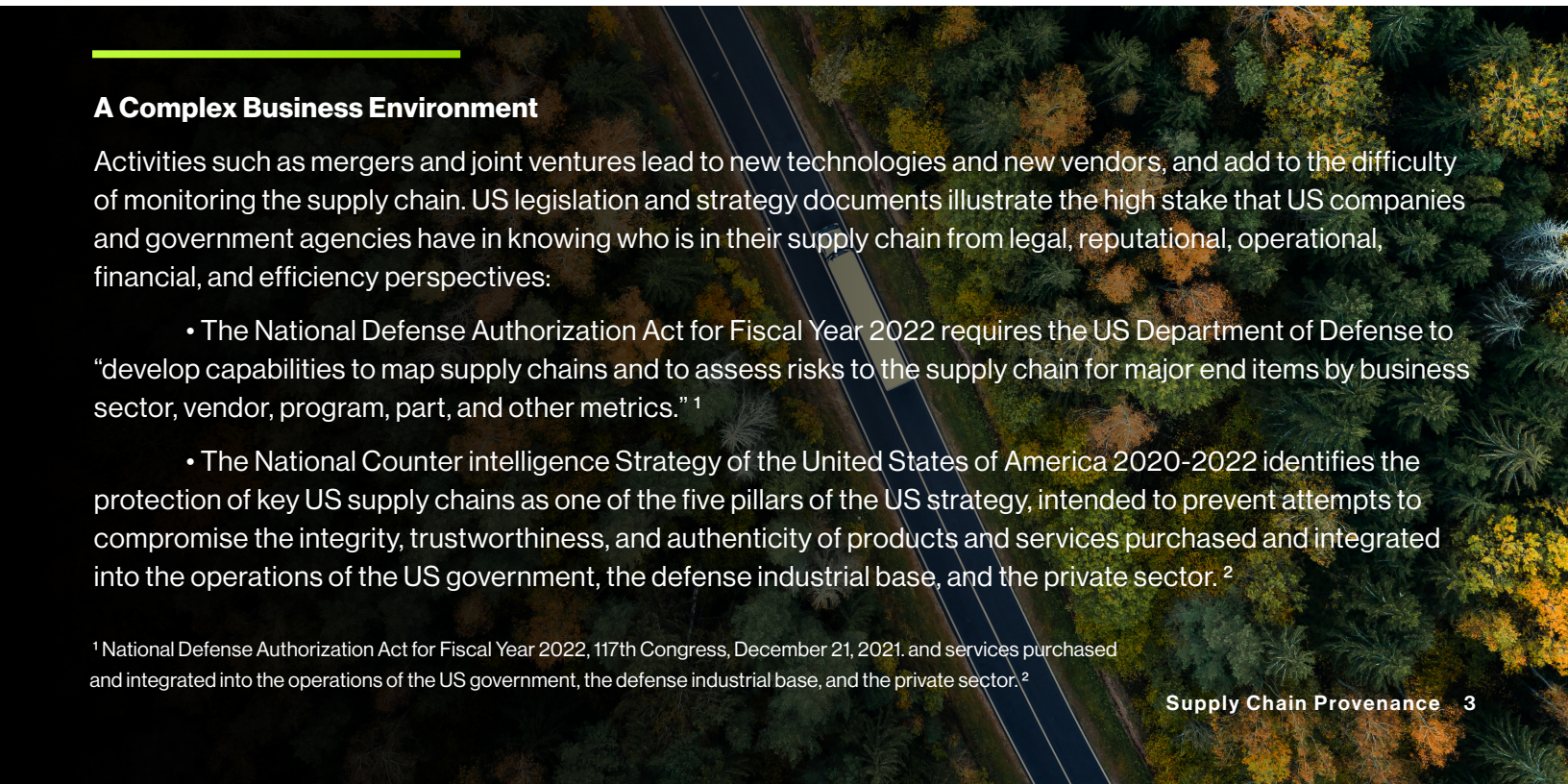
Unknowingly incorporating faulty materials can compromise systems and adversely impact operations.

Natural or man-made disasters

Tornadoes, hurricanes, fires, floods, chemical spills, and other extreme events that disrupt supply chains can have knock-on effects and cascading impacts that adversely impact third parties.

Vendor risk

Limited transparency, understanding, and control over the entire vendor lifecycle process (including risk assessment, contracting, onboarding, hierarchy, monitoring, and offboarding) creates significant risk.



A Complex Business Environment

Activities such as mergers and joint ventures lead to new technologies and new vendors, and add to the difficulty of monitoring the supply chain. US legislation and strategy documents illustrate the high stake that US companies and government agencies have in knowing who is in their supply chain from legal, reputational, operational, financial, and efficiency perspectives:

- The National Defense Authorization Act for Fiscal Year 2022 requires the US Department of Defense to "develop capabilities to map supply chains and to assess risks to the supply chain for major end items by business sector, vendor, program, part, and other metrics." [1]

- The National Counter intelligence Strategy of the United States of America 2020-2022 identifies the protection of key US supply chains as one of the five pillars of the US strategy, intended to prevent attempts to compromise the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of the US government, the defense industrial base, and the private sector. [2]

[1] National Defense Authorization Act for Fiscal Year 2022, 117th Congress, December 21, 2021. and services purchased and integrated into the operations of the US government, the defense industrial base, and the private sector. [2]

Guidehouse
outwit complexity

Cyber Threats to Supply Chains

Recent government announcements indicate that the threat of cyberattacks is expanding and becoming more complex:

• In April 2022, the Department of Energy, the Cybersecurity and Infrastructure Security Agency, the National Security Agency, and the Federal Bureau of Investigation warned that advanced persistent threat actors had developed "custom-made tools" capable of gaining access to multiple industrial control systems, supervisory control, and data acquisition devices.[3]

[2] "The National Counterintelligence Strategy of the United States of America 2020-2022," Office of the Director of National Intelligence (The National Counterintelligence and Security Center), January 7, 2020.
[3] "Alert (AA22-103A): APT Cyber Tools Targeting ICS/SCADA Devices," Cybersecurity and Infrastructure Security Agency, April 14, 2022.

• In September 2022, the White House Office of Management and Budget issued a memorandum directing US government agencies to only use software that complies with secure software development standards, requiring attestations from third-party software providers to confirm compliance.

Per the memorandum, agencies can also require vendors to provide a software bill of materials to prove compliance.[4]

Integrating Supply Chain Provenance

A strong SCRM program should incorporate the following areas: risk governance; risk appetite, tolerance, and culture; risk identification and assessment; risk response; risk reporting; and risk tools and technology. Integrating supply chain provenance into an SCRM program enhances and drives progress in the following areas:

Risk Governance

The establishment of a system or body that determines and periodically reviews policies and determines how supply chain risk issues fit into the broader enterprise risk management of a company or government agency is key and establishes the guiding SCRM principles that run a supply chain-smart entity.

Risk Appetite, Tolerance, and Culture

In their operations, every business or government agency makes significant, routine decisions—implicitly or otherwise—about its risk appetite and tolerance and, therefore, its culture.

For example, in making selections and tradeoffs about the prices, service terms, past engagements, experience, reputation, financial wherewithal, and hundreds of other dynamics related to their suppliers, choices are being made about risk.

Risk Identification and Assessment

Identify high-value assets and their risk by conducting an illumination review of the assets' supply chains, including suppliers and vendors, manufacturers, brokers, and freight forwarders.

Risk Response

Once provenance risks are identified and assessed, an organization's risk management principles will drive decisions when possible. Risk management practices are compared to commercial and government prevailing practices to determine appropriate standard operating procedures and the most effective way to proceed for risk mitigation.

Risk Reporting

A provenance risk solution can be established as an ongoing, continuous monitoring process of documenting and reporting risks associated with the key supplier base as relevant changes occur.

Risk Tools and Technology

Especially in today's world, there are all sorts of SCRM-related and other business tools and technology that can be used to help with SCRM in myriad ways, including determining the provenance of assets, data, software and hardware, and intellectual property that you're considering acquiring or that is already in your supply chain.

Managing Challenges

The complexity of processes, vendor ecosystems, and assets creates numerous opportunities for things to go wrong, both "naturally" or as a result of threat actors. Without understanding supply chain provenance, organizations may lack insight into the chain of custody or location of origin, leaving risks in the supply chain inadequately identified, assessed, and prevented or mitigated.

Most SCRM-related efforts are narrow in focus and lack the depth to uncover security or operational risks that could negatively impact business, mission readiness, and operational effectiveness. The complex dynamics of worldwide supply chains provide ample opportunity for everyday things to go off track, but also give bad actors the chance to make malevolent insertions into sensitive and important systems, data, and products.

This all takes place, furthermore, in a changing environment where software-based systems are more and more overtaking hardware-based systems, organizations are increasingly shifting to the cloud, and connectivity, shared services, crowdsourcing, and the use of machine learning are growing dramatically.

[4]Enhancing the Security of the Software Supply Chain through Secure Software Development Practices," The White House Office of Management and Budget, September 14, 2022.

Guidehouse

Examples of Threat Adversary's Goals

OBFUSCATE OWNERSHIP

INFILTRATE THE SUPPLY CHAIN

ENTER THE DESIGN, BUILD, ASSEMBLY, TESTING, OR MAINTENANCE PROCESS

INSTALL COUNTERFEIT, REUSED, OR FAULTY/SUBSTANDARD PARTS

ACCESS OR STEAL SENSITIVE DATA

CIRCUMVENT CYBERSECURITY MEASURES

INSTALL MALICIOUS CYBER PAYLOADS OR BACKDOORS

DEGRADE MISSION AND BUSINESS READINESS

CARRY OUT ECONOMIC OR INDUSTRIAL ESPIONAGE

UNDERMINE NATIONAL AND ECONOMIC SECURITY

The Value of Provenance

To protect and maintain smooth operations, organizations should especially—and certainly initially—focus on the provenance risks of critical and high-value assets. These assets may include essential data repositories; finished goods and products crucial to business, mission operations, or the revenue stream; industrial control systems; intellectual property; vital raw materials; security-related software; and key transportation or logistics assets.

Organizations that succeed in assessing and understanding provenance in these areas will improve the stability and reliability of their supply chains while often realizing costs savings and increasing visibility into their risk exposure too. Sometimes a critical supplier deep within a supply chain is actually supplying multiple Tier 1 suppliers.

Uncovering these situations can help organizations make more informed supplier decisions and avoid having a false sense of diversification. Supply chain provenance additionally helps organizations optimize spending on key vendors and raw materials, and decrease compliance risk through improved monitoring of supplier compliance obligations throughout the supply chain.

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 16,500 professionals in over 55 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit .guidehouse.com.

@GHTechSolutions

guidehouse.com/cybersecurity

linkedin.com/company/guidehouse-technology-solutions

Contact

Rodney Snyder
Partner
rsnyder@guidehouse.com

Jason Dury
Director
jdury@guidehouse.com