THALES

Supply Chain Risk Management

Industry Insights

Supply chain risk management (SCRM) has long been a key element of the manufacturing process, but as technology advances, the risk management challenges go well beyond the world of producing physical products such as hardware. ISO-based standards provide clear guidance on supply chain management, especially for conventional manufacturing, but U.S. Federal Government suppliers need to think more broadly in today's digital economy.

This Industry Insight outlines a more holistic view of SCRM that will help vendors understand the risks that need to be addressed in order to become a trusted supplier to the federal government. The path forward begins by understanding how trends are impacting the nature of manufacturing, and by extension supply chain risk.

SCRM Trend #1 - Technology Evolution

The evolution of technology has created an ongoing shift from hardware to software, and that brings new links in the supply chain to manage. Despite this shift, hardware remains entrenched in most sectors' infrastructures – including government services. Software has its virtues, and in time will become dominant, but most hardware is built for a long lifecycle and with a high comfort level from IT based on a proven track record. Furthermore, once deployed, the Capex-based sunk costs associated with hardware ensures these assets will not easily be displaced.

This reality may provide performance assurances for IT, but it's also true that more innovation is happening with software. While this gives rise to new capabilities, software brings vulnerabilities that are more easily exploited than with hardware, and that introduces new forms of supply chain risk.

However, hardware is not immune to supply chain risks. This Insight also addresses the globalization trend, and for hardware, a prime example of risk comes from the use of offshore contractors and suppliers. As this practice becomes more widespread and accepted, the integrity of your supply chain for hardware becomes harder to ascertain.

Not only do the conventional supply chain risks remain for hardware, but as new threats developed to attack software become more sophisticated, they will most certainty be adapted to hardware since the installed base is so large, and thus attractive to bad actors. As such, technology evolution may provide a false sense of security that existing hardware will be invulnerable to new forms of supply chain risk.

SCRM Trend #2 – Shift Towards Software

As the cloud begins to replace traditional hardware infrastructures, products are being "built" – or more accurately, developed – by things we can't see or touch. Software is increasingly becoming cloud-based, and in this context, the focus of SCRM needs to shift from tracking physical components to programming code used in cloud-based applications.

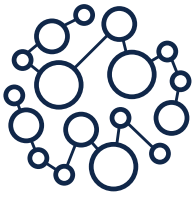
New cloud offerings are launched at a lightening fast pace. In a shared security model, cloud users are responsible for the security of their individual applications and services, while the Cloud Service Providers (CSPs) are responsible for the security of their infrastructure, and therefore the code used in their services. Without tight controls on the supply chain, malicious code could be introduced into the cloud service unbeknownst to the CSP. Today, the majority of software applications, cloud-based or not, are being developed with a high amount of open source code. Having a strong product development lifecycle helps to ensure that any open source code used within a CSP's infrastructure or cloud service offerings will be done in the most secure fashion.

One best practice that can be applied is establishing a technology import process that allows companies, including CSPs, to import software IP in a trusted manner so that the technology can be securely used in products and service applications. This process would start with discovery and inspection to gain a baseline understanding of what the technology is doing, how

it is structured, and its overall level of maturity. A deep-dive review of the technology would follow and may include an architecture review, code analysis and a security design review. All of this data feeds into a risk assessment to identify potential threats, including known vulnerabilities, which would need to be accepted if the technology is pulled into the application or service intended for release to the market.

A second best practice to securely manage risk with software and cloud-based applications is introducing the concept of a software Bill of Materials (BOM) that outlines all components feeding into a software application. With a software BOM, CSPs can carefully list the tools used to build their applications, as well as any third-party components that are included. This provides both the IT and R&D departments the ability to more efficiently and expediently apply software patches and updates.

Furthermore, cloud applications can be hosted just about anywhere. Without knowing where the application is hosted, cloud users run the risk of storing their data offshore which could potentially increase the risk of a compromise.



SCRM Trend #3 - Globalization

Globalization touches everything, but it's particularly relevant to SCRM. This trend has two main drivers, supply and demand, and both impact what vendors must do to become preferred federal government suppliers. Sellers can benefit from globalization by expanding their customer base, as well as tapping into a broader labor pool that can reduce time-to-market along with production costs. Conversely, buyers benefit by having more choice, both in terms of specialized or customized offerings, as well as getting lower prices.

In theory this is a win-win scenario, but in practice, this makes for intense competition that leans to being price-driven. Quality standards are harder to enforce in a global marketplace, and corners are often cut to gain a price advantage. This is easier to detect with hardware and physical products, so this is where software and technology trends intersect with globalization.
Federal government agencies are often price-sensitive, so there is a strong incentive from suppliers to keep costs down. With software, one way to do this is by outsourcing labor for developers and testers to low-cost countries. Another approach is to rely on open source software, which provides greater flexibility for rapid development than more costly proprietary software.

While the end result may be a more cost-competitive product, the supply chain becomes much less transparent for purposes of ensuring that quality standards are being met. This is especially important for federal government agencies where data security is paramount, and this translates into a higher set of compliance requirements than what vendors will encounter in the private sector. Not only must the supply chain be protected to ensure product quality, but also against cybersecurity threats which come in an ever-changing variety of forms.

Understanding the Threats to Your Supply Chain

In a digital environment, the supply chain becomes more fluid, and with government agency purchases becoming more software-based, the associated threats can be harder to recognize. This is especially pertinent with cloud-based software solutions where communication channels are truly borderless and information can flow seamlessly from anywhere in the world. To properly understand these threats, the entire product lifecycle must be considered, as there are a multitude of entry points where supply chain integrity can be compromised. A comprehensive approach to SCRM would entail addressing four classes of threats.

Intentional Threats

These would be deliberate actions with intent either to be malicious or to gain an unfair competitive advantage to win the business. Examples:

- Malware or viruses injected by a competitor to undermine your product or even attack your end customer
- Using prohibited or pirated software to keep production costs down
- Using black market or counterfeit components that pass for OEM in order to cut costs or time to market

Unintentional Threats

These examples reflect poor quality control practices or events beyond the vendor's control:

- Lax enforcement of quality standards
- Unclear or incomplete information with outside contractors
- Lack of attention or human error around data security practices that make the supply chain vulnerable to cyberattacks that do not emerge until later
- Adverse conditions that disrupt or shut down network operations, putting the production process in a state of chaos

Internal Threats

These can take both intentional and unintentional forms, and can come from any type or rank of employee:

- The most dangerous comes from disgruntled or turncoat workers who have motivation to undermine your production from the inside
- Careless workers can unknowingly facilitate the same outcome, either by human error or lack of awareness of data security practices
- Weak policies and procedures to control access and grant privileges for sensitive data

External Threats

These come from outside your organization, and as with intentional threats, the intent is deliberate and usually well-targeted.

- Downstream supply chain partners, perhaps being directed by a competitor, looking to steal IP or possibly disrupt production
- Individual hackers who have found a weak link in your supply chain, and could have any number of motives – malware, phishing, fraud, extortion, ID theft, etc.
- State-sponsored actors on behalf of governments or regimes hostile to the U.S.

Implications for Vendors

When considered together, there is a wide range of supply chain vulnerabilities, and this adds up to a risk profile that goes well beyond conventional hardware manufacturing. As the production process of software and software-based hardware becomes more decentralized, the supply chain becomes more complex and convoluted.

Globalization makes for a highly interconnected ecosystem where supply chain threats can be almost impossible to detect or control. The onus falls squarely on vendors to apply best practices around SCRM, and this starts with understanding the trade-offs that come with the benefits of globalized software production.

In terms of becoming a trusted supplier to federal government agencies, vendors need to align with the requirements in NIST's Cybersecurity Framework. More specifically, for IT decision-makers, vendors need to follow C-SCRM – Cyber Supply Chain Risk Management – a set of processes developed by NIST to mitigate risk pertaining to data security applications.

Compliance with long-standing ISO certifications does not translate into airtight security with federal government agencies, and an end-to-end approach to SCRM will be needed to succeed in this sector going forward.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.comom

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com