- Customer Relationship Management
- Education & Professional Development
- Global Supply Chain Management
- Global Trade & Economics
- Green Energy
- HR & Labor Management
- Quality & Metrics
- Regulation & Compliance
- Sourcing/Procurement/SRM
- SC Security & Risk Mgmt
- Supply Chains in Crisis
- Sustainability & Corporate Social Responsibility

- WAREHOUSING
  - All Warehouse Services
  - Conveyors & Sortation
  - Lift Trucks & AGVs
  - Order Management & Fulfillment
  - Packaging
  - RFID, Barcode, Mobility & Voice
  - Warehouse Automation
  - Warehouse Management Systems
- INDUSTRIES
  - Aerospace & Defense
  - Apparel
  - Automotive
  - Chemicals & Energy
  - Consumer Packaged Goods
  - E-Commerce/Omni-Channel
  - Food & Beverage
  - Healthcare
  - High-Tech/Electronics
  - Industrial Manufacturing
  - Pharmaceutical/Biotech
  - Retail
- THINK TANK
- WEBINARS
  - On-Demand Webinars
  - Upcoming Webinars
  - Webinar Library
- PODCASTS
- WHITEPAPERS
- VIDEOS

Home » Transparent Software Supply Chains Will Usher in Healthcare Cyber Quality
HEALTHCARE

Transparent Software Supply Chains Will Usher in Healthcare Cyber Quality

February 5, 2024

JC Herz, Senior Vice President, Cyber Supply Chain, Exiger and Shannon Lantzy, President, Shannon Lantzy LLC

Analyst Insight: Now that software bills of materials (SBOMs) are an FDA requirement, the medical device market can achieve software supply chain transparency, which means more and better information on cybersecurity risk. As SBOM analysis yields business-relevant risk information, customers will use it to make more informed decisions about what to buy and how to price risk transfers. This allows resilience to be priced into the product.

As transparency illuminates the value of risk reduction, suppliers also can compete on software quality, and can quantify the value of maintenance packages that keep software risk at acceptable levels. While customers and regulators often talk about holding suppliers "accountable," many of those same customers have historically been unwilling to pay a premium for higher levels of cybersecurity quality. SBOMs add a dimension to the trade space between cost, functionality, and quality — trading security for affordability is no longer an invisible choice.

Now, customers may be willing to cede control to increase the affordability of security maintenance. For example, it used to be standard to require human "sneakernet" service calls to update medical device firmware in hospitals. But now hospitals may allow medtech manufacturers direct connectivity to devices in exchange for over-the-air patches.

In the absence of transparency, security is a cost center which rational actors will minimize. As a mechanism for transparency, SBOMs create a more informed mode of contract negotiation, where customers can be explicit about expected cybersecurity quality, and suppliers can gauge security return on investment both in the absolute and relative to competitors.

Software quality degrades over time, new vulnerabilities must be patched, and maintenance should be as frequent as possible to keep weaknesses from entering the healthcare software ecosystem. As SBOMs allow customers to gauge both quality and risk, the best companies aim to demonstrate high-quality software and will insist on subscription or other frequent update models (heretofore rare in medtech).

Leading companies will implement software development processes that prevent vulnerabilities from ever reaching the market, and they'll use their SBOMs to prove it. Customers and suppliers will gravitate toward using leading risk indicators that allow them to remediate risk on a non-emergency basis, in advance of lagging risk indicators like common vulnerabilities and exposures (CVEs).

We'll also see medtech compete on software assurance, with claims that their products are resilient in a supply chain attack — because now they'll have an unbiased market mechanism to demonstrate those claims. As a more transparent marketplace matures, the financial value of higher quality can be audited over time.

Suppliers and customers will shift from a "once-and-done" model for vendor qualification and product approval to an "always-on" assessment that keeps software within acceptable thresholds on a continuous basis. Monitoring becomes the norm, and contractual service-level agreements (SLAs) can be defined based on response times that are quantifiable and can be associated with remedies, including financial. These terms and conditions, like all contractual agreements, are negotiations between suppliers and customers, and the relative leverage of those entities will dictate where negotiations come to rest.

Outlook: How fast we see these changes happening will depend on the market's ability to rapidly intake, process and make use of the information in SBOMs. This includes cybersecurity and supply chain technology vendors who help the healthcare industry derive insight from SBOMs. This nascent field is poised for growth.

Resource Link: