

# Managing the Risks

Every Organization Values Supply Chain Visibility but Sharing Information Can Be a Dangerous Proposition



BY RAJA CHANDRASHEKAR

**S**upply chain visibility is now one of those universal goals – like profitability or high service levels – that every organization wants to achieve. It is certainly easier for businesses to ensure supply chain efficiency if they have real-time visibility into every aspect of their networks – including detailed information on products, suppliers, distributors, carriers and customers worldwide.

In order to achieve a high level of supply chain transparency, companies must share their technology systems and data with the dozens – or even hundreds – of suppliers, distributors, transportation carriers and channel partners that bring their products to market. This information may be seen by thousands of employees in every corner of the world. While there are doubtless benefits to be achieved, increased data sharing also carries an inherent level of risk.

Recently, global media outlets have been reporting on damaging information leaks at consumer electronics companies known for carefully staged product launches. In June 2010, a detailed Windows 8 planning document was leaked, following a forum that Microsoft scheduled with computer and hardware manufacturers<sup>1</sup>. A couple of months later, a Verizon Wireless inventory screen shot was posted online, revealing a number of new SKUs with specific model numbers, product features and even order quantities<sup>2</sup>. Blurry Android product photos showed up elsewhere on the Internet<sup>3</sup>.

With today's competitive pressures, short product lifecycles and continuous innovation, companies cannot lose sight of one simple fact: information is power. A potentially game-changing new product design will not change anything if key competitors obtain classified knowledge. It comes as no surprise that – along with broad visibility – secure information management is emerging as a core competency for supply chain leaders worldwide.

## Leveraging Sales and Operations Planning for Secure Information Management

Just as supply chain technologies and associated business processes have enabled the broad collection and sharing of data, these same tools and processes can help to manage inherent risks that come with collaboration. Involving trade partners at the last possible moment through real-time demand sensing, decision postponement and inventory agility can help ensure the protection of sensitive information. But because many high-tech product components require 6 to 18 months of lead time, some companies must bring their suppliers on board early in the production process.

Supply chain leaders in every industry are demonstrating that data can be safely shared across multiple trading partners – as long as this occurs as part of a carefully controlled, tightly managed, collaborative sales and operations planning (S&OP) process. From the moment that new products are conceived and production planning begins, these leaders implement strategic S&OP activities that involve their trading partners across the global network. Technology supports well-managed S&OP processes by ensuring a high level of collaboration from key suppliers while controlling their access to sensitive information around end products, launch dates and sales forecasts.

## Sharing Point-of-Sale Data to Strengthen Retailer Relationships

The balancing act to ensure that there is information flow, cross-company collaboration and supply continuity while keeping critical competitive information under wraps can be tricky. However, some businesses are emerging as leaders in successfully bringing innovative new products to market – both securely and profitably.

Due to its focus on identifying consumer needs at the individual store level, a leading consumer electronics manufacturer and JDA Software customer generates a wealth of demand and sales information every day. As part of a collaborative S&OP process it executes in partnership with its key retail partners, the manufacturer uses electronic data interchange feeds and other communication tools that provide store-level point-of-sale (POS) information for all of its products. Data arrives daily and is reviewed weekly by the manufacturer. Slicing and dicing this information in various ways reveals demand trends across the company's entire product portfolio down to the product model, retail channel, geographic region and individual store levels. In turn, these insights drive intelligent optimization engines to determine the most effective replenishment and promotional strategies in support of collaborative S&OP. These consumer insights also fuel future product development.

With this incredible level of visibility, the consumer electronics manufacturer has gained a significant competitive advantage and strengthened its retailer relationships. Its deep level of POS information allows the business to anticipate market shifts and monitor trends in real time.

This huge volume of data also presents risks to the business. Information security is paramount as the manufacturer collects and analyzes this information, sharing it selectively with retail partners to demonstrate its knowledge of their own shoppers. To protect this highly detailed consumer data, the company uses a number of closed-loop business processes, software solutions and user protocols to ensure that the information remains secure at every step. Both the company's retail partners and employees are monitored closely to ensure that key data and insights are accessed only by those who have clearance to access this proprietary information. By building data security measures into its foundational S&OP processes, the manufacturer can safely collect and protect an enormous amount of sensitive market data.



### **ON Semiconductor: Earning Customer Trust**

As a leader in providing premier power solutions to global electronics leaders – including Dell, Intel, HP, Samsung and Motorola – ON Semiconductor understands the complex security challenges of high-tech component suppliers. In addition to building its global supply chain for agility and implementing collaborative S&OP, which are essential when supporting consumer product launches, ON Semiconductor uses closed-loop business processes and secure technology to safeguard all component orders, delivery dates and other data that could be used by competitors.

ON Semiconductor strives to meet the stringent demands of its high-tech customers. These companies value trust and collaboration as much as they value high-quality components and on-time delivery. Due in part to its robust, secure business processes, ON Semiconductor is a preferred partner of consumer products leaders and their global manufacturing partners – all of which rely on the company to safeguard their competitive information.

## Maximizing Collaboration While Minimizing Exposure

Robust S&OP processes such as those used by the aforementioned supply chain leaders require close partner collaboration and the secure exchange of valuable information. Organizations that want to adopt a similar approach should bear in mind these four suggestions to minimize risk when sharing supply chain information with their trading partners:

### 1. Synchronize and Align Product Development With the Rest of the Supply Chain

While many companies manage product development as an isolated activity, this is an area of the business where ongoing governance is most needed. The business rules, predefined partner roles, and permissions and authentications demanded by a tightly managed S&OP process ensure that launch information is as carefully controlled as the rest of the supply chain's sensitive data. In addition, the overall supply chain can be properly positioned to phase products in and out, which can otherwise create a great deal of stress on operations.

### 2. When Launching New Products, Carefully Consider the Number of Partners That Are Directly Involved

Product launches are exciting events and it's not surprising that organizations want to share information about their latest innovations with all of their trading partners in order to strengthen their relationships. However, most product launches require the active participation of only a few key partners – and going beyond that limited network exponentially increases the risk that proprietary information will be leaked.

### 3. Limit the Amount of Non-Critical Information Shared With Suppliers

Even when suppliers must be involved in prelaunch activities, organizations can make strategic decisions about when and how much information should be shared. The more sensitive the information, the more suppliers should be operating on a need-to-know basis. Suppliers play a key role in meeting launch deadlines, but do not need to know every detail about product features, price points or sales forecasts.

### 4. Maintain and Enforce Strict Confidentiality Agreements

Every company should manage its trading partner relationships via carefully conceived contracts that, in addition to spelling out roles and deadlines, should also include strict confidentiality clauses and penalties if they are violated. Such contracts remind partners that data security is a shared responsibility and that information access should be limited within their own businesses via passwords, authentications and other security measures.

There is no question that new supply chain processes and technologies have created enormous benefits. Today, information can easily and quickly be shared among a diverse, complex, geographically distributed network of trading partners around the world. Unfortunately, such speed and agility also create the possibility that sensitive information can be mishandled and shared with the world instantly – as shown in recent headlines. The dual-edged sword of visibility makes it imperative that organizations complement their speed and power with an equal measure of discipline and control. ■

<sup>1</sup> What the Windows 8 Leak Tells Us, *CNET News*, June 30, 2010

<sup>2</sup> Verizon's Android Product Launch List Leaked; Includes Motorola's Droid Pro, *ZDNET*, Aug. 16, 2010

<sup>3</sup> Verizon HTC Smartphone: Leaked Photos and Specs, *Product Reviews*, Aug. 9, 2010



Raja Chandrashekar is vice president, high-tech industry strategies, JDA Software. In this role, Chandrashekar is responsible for defining and managing JDA's portfolio of solutions – both as they exist today, and as they should evolve to serve future market opportunities in the high-tech industry.