Q&A

Stephanie Overby

NO. 141

Supply Chain Fraud: Theft That's Hidden in Plain Sight

COMPANIES ARE LOSING TRILLIONS – YES, TRILLIONS – OF DOLLARS EACH YEAR TO INTERNAL AND EXTERNAL THIEVES. YET MANY COMPANIES DON'T EVEN KNOW IT. HERE'S WHY.

Chances are, if a company's leaders realized that a chronic failure in the supply chain was costing millions of dollars annually, fixing it would jump to the top of the corporate agenda. But that hasn't been the case when it comes to supply chain fraud.

Incidences of every type of corporate fraud increased in 2013, according to Kroll's *2013/2014 Global Fraud Report*, with vendor, supplier, and procurement fraud seeing the biggest growth.[1] The typical organization loses 5% of revenues each year to fraud, according to a 2014 report from the Association of Certified Fraud Examiners (ACFE).[2] That equates to a global loss of nearly US$3.7 trillion annually, a significant portion of which is leaked through the supply chain.

In addition to the bottom-line damage, brands take a reputational hit when they deliver substandard products to their customers. In some industries, such as food, drugs, and aerospace, the stakes are even higher: supply chain fraud can kill. Yet nearly half (47%) of executives and managers did not even know whether their company had experienced fraud, waste, or abuse in its supply chain during the past 12 months, according to a survey conducted by Deloitte in 2014.[3]

We talked to a panel of supply chain experts about fraud risk and about how companies can create a smarter supply chain that can both increase the chances of fraud detection and prevent such insidious scams in the first place.

David Landsman is Global Director with Ariba Discovery.

Mark Pearson is a principal with Deloitte Financial Advisory Services.

Marcus Puschke is a principal consultant with SAP.

Lilliana Grbic is an Engagement Architect with SAP.

Q The numbers are clear: supply chain fraud is a costly and growing problem. Why don't companies do more to prevent it?

Mark Pearson: People think that it can't happen to them. As a fraud investigator, I look at most things – whether it's an M&A deal or a new vendor – and automatically think about what the impact would be if something went bad. Most people don't. They're high-fiving because they got the deal done. It's human nature to want to trust one another, and that's especially true within the business context.

Q What is supply chain fraud? It encompasses more than just financial fraud, correct?

David Landsman: Clearly there is financial fraud, and that's something everyone wants to avoid. But there are also counterfeit goods, stolen goods, lost or damaged goods, and dangerous goods.

Counterfeit parts are one of the biggest problems facing the global supply chain. When you think about component manufacturing, your supplier most likely does not manufacture all the components that go into a subassembly; it has its own supply chain. And if you don't have visibility into who your supplier is buying from, that's a huge blind spot. For an automobile or aerospace manufacturer, that can be very, very dangerous and lead to quality problems, causing not only safety issues but also financial losses and brand impact.

Beyond fraud, there are also issues of waste and abuse in the supply chain. When a textile factory in Bangladesh burns down and people lose their lives, everyone wants to know who's buying from that supplier. That's not fraud; it's corporate social responsibility.

Q Supply chain fraud is not just perpetrated by outsiders. Employees are often involved, too, correct?

Marcus Puschke: Procurement fraud often goes hand in hand with corruption. To make sure that you succeed with your fraudulent attempts, you very often need someone within the company to cover it up, who accepts and signs off on the invoices, for example. Fraud involving collusion between suppliers and employees is often the most costly because it is the most likely to evade detection.

> "RELYING ON SPOT CHECKS OR WHISTLE-BLOWING IS LIKE USING A FISHING ROD TO CATCH FISH: EVERY NOW AND THEN YOU GET A BITE. BUT BY CREATING A MORE AUTOMATED FRAUD DETECTION SYSTEM, YOU'RE FISHING WITH DYNAMITE: EVERYTHING COMES TO THE SURFACE."
>
> – Marcus Puschke, principal consultant with SAP

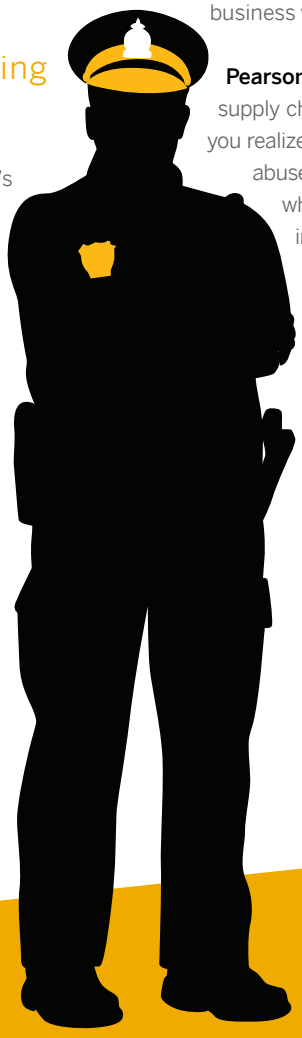
How does the typical company manage the risk of supply chain fraud today?

Landsman: Largely by physical supply chain verification. For multibillion-dollar companies, that's done by their international purchasing offices on the ground. Smaller companies can hire third parties to do on-site supplier audits.

Lilliana Grbic: Where there have been more technical solutions in place, companies have been limited to very narrow slices of data records. They didn't have the capabilities to take the entire population of supply chain data and analyze it until now.

How much fraud is missed using these methods?

Landsman: Once you identify fraud in your organization, it's pretty easy to unravel because it all comes apart at the seams. The problem is noticing it to begin with. The average amount of time from when a fraud begins until it is detected is 18 months, according to ACFE. And passive detection methods (external audits, whistle-blowers) tend to be slow,



Puschke: Relying on spot checks or whistle-blowing is like using a fishing rod to catch fish: every now and then you get a bite. But by creating a more automated fraud detection system, you're fishing with dynamite: everything comes to the surface.

What does a smarter supply chain look like?

Landsman: A smarter supply chain is a transparent one. The critical need for visibility into a company's suppliers and its suppliers' suppliers is driving a move toward analytics. The greater visibility companies get into the depths of their supply chain, the more predictable their entire business will become.

Pearson: Consider the way most companies deal with financial supply chain fraud today. It's pay and chase: You pay an invoice and you realize a year later during an audit that there was fraud, waste, or abuse and you try to get the money back. Instead of doing that, which is incredibly inefficient, companies can use the data and information they're already getting from those audits and get smarter about the invoices that they haven't paid.

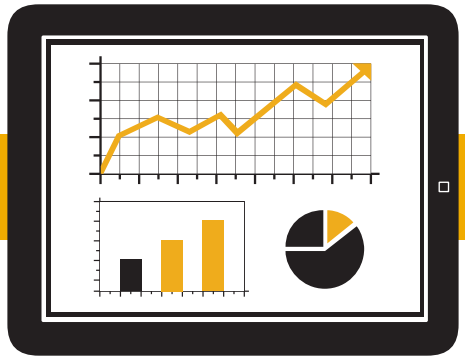
Q How might supply chain fraud detection improve now that companies have access to more powerful data collection and analytics?

Pearson: A tremendous amount of data is being generated – about companies and their products, who they're sourcing from and who they're not sourcing from – every day. And if supply chain leaders aren't using that data to create a smarter supply chain and gain insights about their business, they're exposing themselves to potential scrutiny not just from regulators or shareholders but also from the board and others within management.

Grbic: A typical bill of materials contains approximately 3,000 records. Now that we have tools to manage Big Data, the game has completely changed. And with the explosion of sensor data, the Internet of Things, and mobile devices, we'll have more information than ever before with which to fight supply chain fraud.

Q What are the biggest hurdles when applying analytics to supply chain fraud?

Puschke: The first challenge is defining fraud patterns. Software is not a crystal ball. You have to program it to detect fraud. Secondly, you need to analyze all this data not within weeks but within minutes or seconds. Finally, you need to integrate the data into your business processes. If you have a procurement process that takes place in one system and is operated by one group of people and have another system for fraud detection operated by a separate group of people, you have to integrate them. It's about connecting systems in real time and it's a real challenge. But it's the only way to ensure that once the detection system pinpoints potential fraud a specific business process in procurement is stopped in time while everything else continues on as usual.



There's more.

TO LEARN MORE ABOUT HOW TO MAKE YOUR SUPPLY CHAIN FRAUD FREE, DOWNLOAD THE IN-DEPTH REPORT *3 WAYS TO FIGHT FRAUD, WASTE, AND ABUSE IN THE SUPPLY CHAIN*. PDF

The SAP Center for Business Insight program supports the discovery and development of new research-based thinking to address the challenges of business and technology executives.

1 *2013/2014 Global Fraud Report* (Kroll, Economist Intelligence Unit, 2014), http://fraud.kroll.com/wp-content/uploads/2013/10/GlobalFraudReport_2013-14_WEB.pdf

2 *Report to the Nation on Occupational Fraud and Abuse* (Association of Certified Fraud Examiners, 2014), http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

3 Sabine Vollmer, "Identifying Fraud, Waste, and Abuse in the Supply Chain," *CGMA Magazine*, October 14, 2014, http://www.cgma.org/magazine/news/pages/201411110.aspx