www.pwc.com

Needle in the haystack: Monitoring vendor networks through supply chain risk analytics

July 2016

pwc

The increasing severity of consequences for regulatory violations by vendors in complex global supply chains is matched only by the corresponding damage to reputation when vendor network violations get exposed. The growing volume and widening range of transactions in global supply chain networks have weakened global geographic barriers and amplified company exposure to issues that were once considered distant threats. Not only are companies at risk, but also, increasingly, leadership and board members are being held accountable for their companies' supply-chain-related regulatory breaches.

Many companies perform due diligence and monitoring of their direct vendors, but those legacy minimums are no longer sufficient: reputational and compliance liabilities extend further down the supply chain now than ever before. Companies must safeguard themselves against vendors' vulnerabilities—especially with regard to information security—across their entire supply chains, extending from their direct vendors to secondary and tertiary suppliers, service providers, and shippers. The situation demands that executives carry out a progressively difficult mission: to reduce risk while sustaining rapid decision making and to price competitively as they meet global demand.

Many current supply chain risk management efforts are ill-suited to contend with the complexity involved in monitoring extended vendor networks and the volumes of disparate information therein. A new course of action is necessary. Advanced data analytics and visualization capabilities can support efficient detection and remediation of vendor-related regulatory noncompliance and produce real-time risk reporting. Organizations that adopt an analytics-focused approach to managing vendor-associated supply chain risk stand to prevent and mitigate potentially costly reputational and regulatory risks.

Discovering more-complex supply chain infiltration—only when it's too late

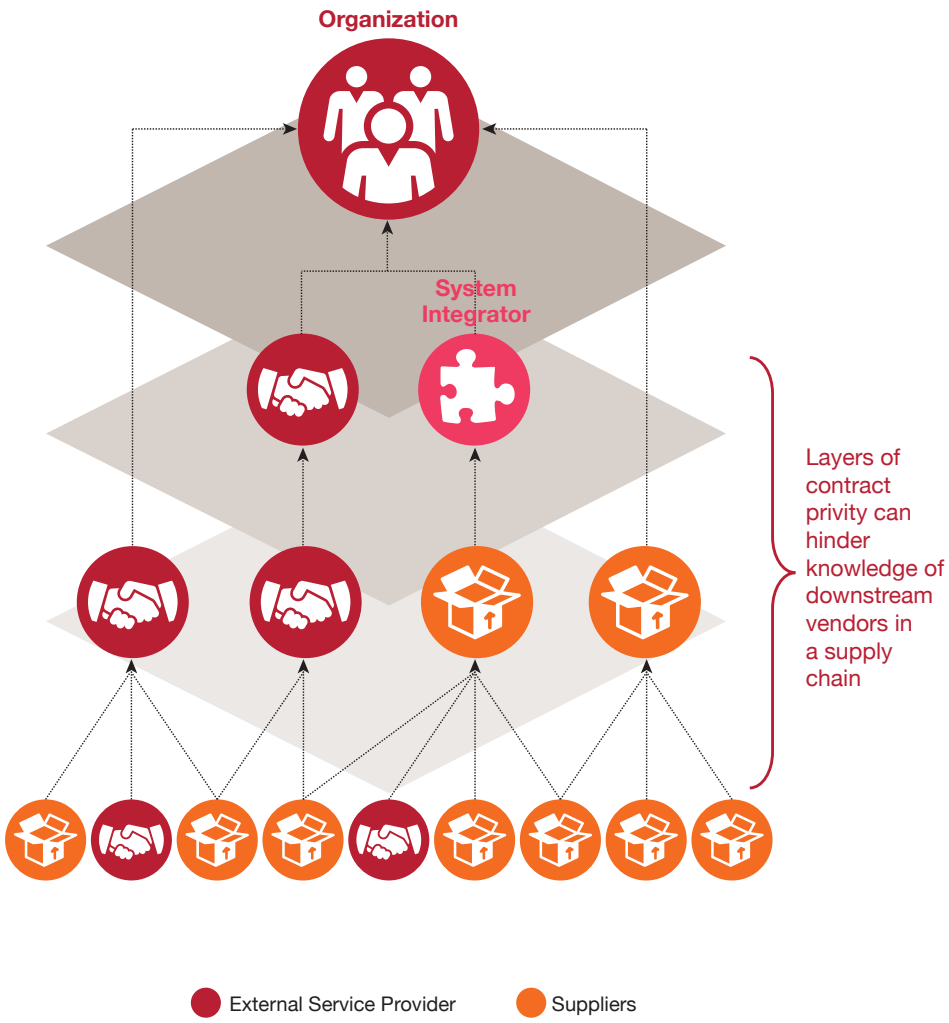
Companies are operating in a global environment of complexity, uncertainty, and volatility. In response, 83% of companies in PwC's 2016 Risk in review: Going the distance study revealed they have either completed or are going through a business transformation—up from 75% the year before.[1] But no matter how advanced or diversified a company may be, it is impossible for any single company to be an expert at everything. Partnering with third parties—be they suppliers, service providers, or channel partners—is a necessity of running a successful business, and 71% of those designated in the study as high performers say they are able to quickly add third-party resources as needed.[2]

Each addition of a third-party relationship carries increased exposure to risk, yet reputational liabilities to a company are no longer limited to a company's immediate pool of external providers, because multiple entities in multiple countries can become involved in the provision of a single product or service (Figure 1). The complexities inherent in providing services in a global economy and the relevance of those complexities to average consumers are coming to light through high-profile media exposés. In one such story, supermarkets, restaurants, and foodservice companies were found to have been purchasing seafood that could have originally been caught by modern-day slaves and sold into reputable sources through a multistage supply chain.[3] Other examples include consumer electronics that could contain batteries that contain an ingredient mined illegally (see sidebar "The reputational risk of accusation").[4] Consumers staying at hotels may eat complimentary chocolates made by a company that sourced cocoa beans originally picked by child laborers.[5] Moreover, the insertion of counterfeit goods into licit supply chains is a growing threat to all commercial sectors, with counterfeit information technology components drawing particular attention.

The reputational risk of accusation

In complex global supply chains, the need for sophisticated Know Your Vendor programs is critical to managing reputational risk. The stakes are high, with risk extending beyond actual breaches. Many highly visible cases have shown that companies need only be publicly accused of affiliation with a corrupt vendor to suffer reputational and financial damage, which is termed *naming and shaming*. Consider the recent accusation that major electronics and automobile manufacturers were connected to child labor. Amnesty International and African Resources Watch mapped a supply chain beginning with children as young as seven years of age who were mining cobalt by hand in the Democratic Republic of Congo. According to those groups, the cobalt is sold to a subsidiary of China's largest cobalt producer, exported to China, refined, and sold to a number of battery manufacturers. Batteries are then produced and sold to manufacturers of consumer goods—predominantly in South Korea and China. Even though no charges were ever filed and companies have refuted the accusation, several major brands received negative press, fueling speculation among the buying public.

Figure 1: Understanding vulnerabilities in the full supply chain can help mitigate reputational and regulatory risk



As supply chains become more and more complex, legacy supply chain risk management solutions no longer suffice for dealing with modern threats to compliance and reputation. Multisource supply chains that include layers of middlemen pose extreme challenges to map and observe—particularly by way of traditional investigative means. Take, for instance, a US shipping company that incurred liabilities for itself and its clients by inadvertently allowing cargo to be transported for part of the cargo's journey by an Iranian-flagged carrier.[6] An example with even direr consequences occurred in 2006, when unapproved Chinese chemicals were shipped to a cough syrup manufacturer in Panama. The Chinese vendor substituted diethylene glycol, a component of antifreeze, for glycerin, which resulted in the deaths of many individuals, including children, in Panama.[7]

In the wake of several high-profile incidents, governments across the world have enacted legislation aimed at addressing illegal activities in the supply chain: The US Trade Facilitation and Trade Enforcement Act and the UK Modern Slavery Act specifically address human trafficking and forced labor in supply chains, with the European Union and other governments expected to impose similar requirements in the near future. (See PwC's white paper "Human trafficking and forced labor: Ethical supply chain challenges for multi-national companies" [8] for more on human trafficking controls.) The US Foreign Corrupt Practices Act and the UK Bribery Act are intended to prevent corruption in the supply chain. And other regulations such as the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations control the export of sensitive technology and data.

Increased pressure to monitor vendor networks extends into the public sector. The National Institute of Standards and Technology (NIST) has briefed and recommended to all federal contracting officers that the guidance it set forth in its Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,*[9] be included in those officers' source selection criteria (see sidebar "The guidance from NIST and CISA"). In other words, federal contractors—particularly those involved in information technology—are likely to undergo increased scrutiny when bidding on federal work, and they could be compelled to demonstrate their understanding of the vulnerabilities represented across their full supply chain, extending from their direct vendors to vendors of vendors.

As regulators and prosecutors start feeling the pressure to escalate enforcement of regulations governing supply chain risk, they are turning their attention to individuals.[10] In a September 2015 memo (commonly known as the Yates memo), US Deputy Attorney General Sally Yates laid out new guidance for US Department of Justice prosecutors and civil litigators that strengthens the priority of pursuing and punishing individuals accountable for corporate wrongdoing. For example, to qualify for cooperation credit, corporations must disclose to the Department of Justice all relevant facts related to individuals responsible for wrongdoing.[11] Further, prosecutions against ITAR and the Arms Export Control Act are increasing, resulting in both administrative and criminal penalties for companies and their executive leaderships.[12]

Risk and compliance leaders and heads of procurement should also understand their extended vendor networks' connections to specially designated nationals and other sanctioned entities, because reputational risks extend beyond the compliance realm. Company brands can easily suffer from third-party relationships with politically exposed persons, terror networks, shell companies, conflict minerals, money-laundering schemes, tax havens, trafficked labor, child labor, conflict zones, and counterfeiting. Staying ahead of all of those threats takes a persistent, systemic approach that keeps pace with business while meeting cost objectives.

The guidance from NIST and CISA

NIST Special Publication 800-161 points out that managing information and communications technology (ICT) supply chain risk requires ensuring the integrity, security, and resilience of the supply chain and its products and services. The onus is on information and communications companies that do business with the government so that those companies manage and report identified risk within their supply chains. The publication defines the scope of the ICT supply chain infrastructure as an integrated set of components (hardware, software, and processes) that together constitute the environment in which a system is developed, manufactured, tested, deployed, maintained, and retired or decommissioned.

The Cybersecurity Information Sharing Act of 2015 was signed into law on December 18, 2015, and is seen by many organizations doing business with the government as the enforcement of NIST 800-161 guidance on ICT supply chain risk management. With the aim of improving cybersecurity in the United States, the act encourages contractors to establish Information Sharing and Analysis Organizations (ISAOs) for coordination of cybersecurity information sharing and analysis between their organizations and the federal government. Such information sharing extends to gathering information from extended suppliers that are helping produce hardware and other components in contractors' technology supply chains.

Understanding the need for persistent and full-population monitoring

Current supply chain risk management efforts are unsuitable for addressing the complexity of continuous monitoring of multiple tiers of vendor connections. According to a Global Supply Chain Institute survey, 90% of companies do not formally quantify risk when sourcing production.[13] Even though most companies have processes in place for monitoring operational risk—such as disaster recovery and business continuity—in their supply chains, which may include the use of Service Organization Controls (SOC) 2 reports or SOC 2+(Vendor Controls Assurance) reports,[14] many do not focus on the reputational risk provoked by vendors involved in such illicit activities as corruption or trafficked labor. Those that do investigate vendor corruption typically follow an analog vendor verification process—in the form of onetime visits or embassy consultations—that involves a largely manual and cost-intensive approach based on sampling their primary vendors. Rarely do they extend their investigations to the supplier network of those vendors.

Companies must be able to verify whether each individual entity in the network is abiding by all the laws of the countries with jurisdictions over it.

As companies turn to their component and materials vendors that in turn source from a variety of vendors down the chain, traditional due diligence models that use periodic monitoring of sample sets have become outmoded. The documentation and disclosure of extended business relationships varies among vendors, and constantly shifting supply chains can make sampled data quickly obsolete. Further, in many companies, the analog human capability to monitor for potentially aberrant or suspicious behavior among the company's vendors' vendors is costly enough to demand more-automated solutions.

The complexity of monitoring vendors and the layers of suppliers that a vendor works with demands robust surveillance models that can integrate and report on high volumes of constantly changing internal and external data. Global Internet traffic is now being measured in zettabytes, and much of it is metadata that will expand client exposure and the scope of surveillance. A regulator or a journalist need find only one potential problem, yet to prevent that, a company has to ensure that 100% of its supply chain is free of compliance issues or adverse media issues.

Consider the demands of monitoring at a company with, say, 20 primary vendors. If each primary vendor has in turn 20 suppliers that each have in turn 20 suppliers, the extended vendor network consists of 8,000 companies and tens of thousands of executives. Companies must be able to verify whether each individual entity in the network is abiding by all the laws of the countries with jurisdictions over it. They must be able to identify any association with a sanction or other watch list—even through a fragmented ownership chain or holding company. They must be able to assess the personal linkages of company executives. And they must be able to do all of it continuously.

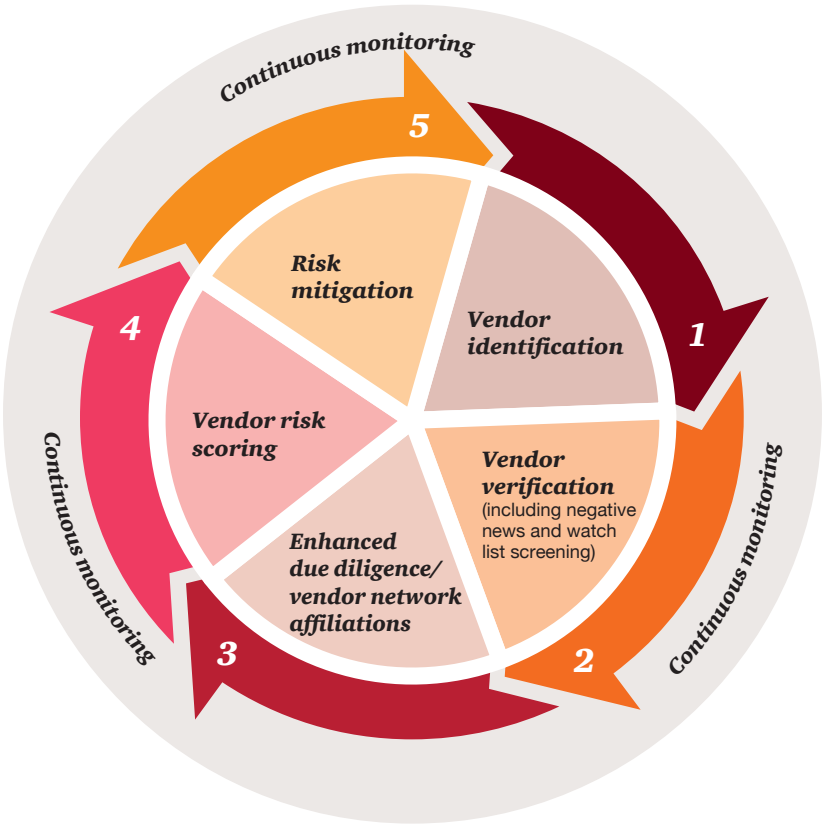
Many of the threat-screening requirements, such as lists issued by the US Treasury's Office of Foreign Assets Control, are constantly evolving. At the same time, vendors' associations are constantly changing due to executive turnover, individual relationship changes, acquisitions, divestitures, new products, and new sources of investment. For example, the chief financial officer of a vendor's vendor might suddenly become registered as the chief financial officer of an offshore bank. A decision by a vendor's vendor to enter into a new product or service line could start new employees and new tertiary business relationships that cause risk exposure for companies all the way up the supply chain, even if the new business is completely unrelated to that supply chain.

In today's dynamic information environment, manual monitoring and investigation alone become unsustainable. An analytics-driven surveillance and reporting solution that harmonizes with current tools and processes will enable companies to continuously monitor vendors.

A framework that keeps pace with business demands

Motivated by escalating personal and corporate reputational risk and the potential impact on revenue due to failure to demonstrate awareness of parties in their supply chain, forward-thinking organizations are exploring new approaches to knowing their vendors' vendors by applying advanced analytics that facilitate continuous monitoring of the entire vendor pool. As companies consider their need for new supply chain risk management tools, frameworks are useful mechanisms to enhance decision making. A potential framework (Figure 2) contains six core capabilities to consider—from vendor identification, vendor verification, and due diligence to vendor risk scoring, risk mitigation, and continuous monitoring. The framework also assists companies in gathering and structuring disparate data relevant to applicable regulatory, reputational, and internal risks, and in improving their data quality as needed.

Figure 2: A robust Know Your Vendor framework can enhance decision making and streamline risk management



The first wave of framework implementation focuses on uncovering the vast network of vendor relationships that many companies have been unable to fully identify. Once the complete network of vendors has been mapped, a company can then begin to implement active measures such as persistent monitoring in order to ensure compliance and defend its brand throughout distant chains. Such persistence is essential, because a so-called snapshot of a supply chain network cannot account for the constant changes vendors make in their own supply chains.

Ultimately, supply chain risk management analytics should bring together all source data into actionable intelligence and be adaptable so it can meet unique compliance requirements. The solution should simplify decision making at all levels. And the solution should streamline risk management by (1) focusing on the most-critical attributes that increase risk exposure and (2) evaluating vulnerability to risk versus impact.

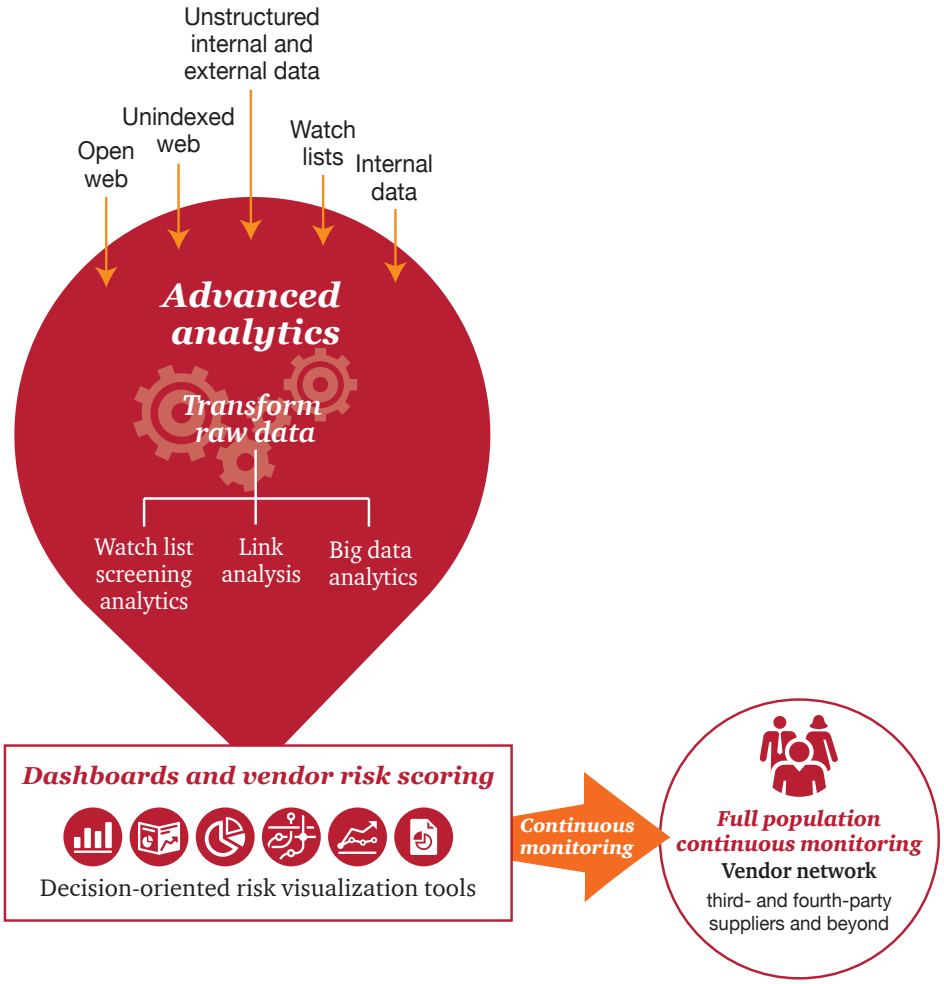
Finally, some companies use supply chain risk management analytics to augment existing risk detection, prevention, and mitigation models. Others implement solutions as stand-alone processes in parallel with—or as the future basis of—third-party risk models.

Next-generation analytics for robust surveillance

Analytics techniques are increasingly being used for conducting surveillance tasks such as vendor screening and risk scoring as a way of alerting organizations when a barred vendor has burrowed into a supply chain or when a vendor's profile, practices, or relationships create unacceptable risk (Figure 3).

The techniques also require an adaptive approach that protects the company from high-risk relationships by staying current with emerging monitoring methods and data sources while managing brand risk and compliance in a cost-effective way. Potential solution components are discussed next.

Figure 3: Continuous supply chain monitoring through advanced analytics



Watch list screening and link analysis

Organizations are taking a tool out of the standard national security and law enforcement toolkit by applying watch list screening analytics to supply chain monitoring. Use of techniques such as adverse media scanning, alert consolidation, and link analysis (which identifies the connections between a vendor and other, potentially suspicious, parties) are enhancing screening program efficiency and efficacy. Advances in analytics have taken the screening process well beyond the analogs of traditional watch list screening and scoring by digging deeper into the web and employing link analysis. (See PwC whitepaper "Name, set, match: Enhancing watch list screening through analytics"[15] for more on watch list screening.)

Use of techniques such as adverse media scanning, alert consolidation, and link analysis (which identifies the connections between a vendor and other, potentially suspicious, parties) are enhancing screening program efficiency and efficacy.

Total population continuous monitoring

Without continuous surveillance, if a vendor passed screening at one point in time and before the next static screening gets blacklisted, a company would not be aware of that vendor issue. Big-data analytics is bringing companies the processing power to efficiently—and continuously—monitor the total population of vendors via automated processes and to surveil vendors with a more holistic, 360-degree view. Such solutions go beyond historical batch-list screening techniques by taking advantage of the fastest and most-comprehensive Web search capabilities—in an analytics environment—that have the capacity to search broadly and persistently.

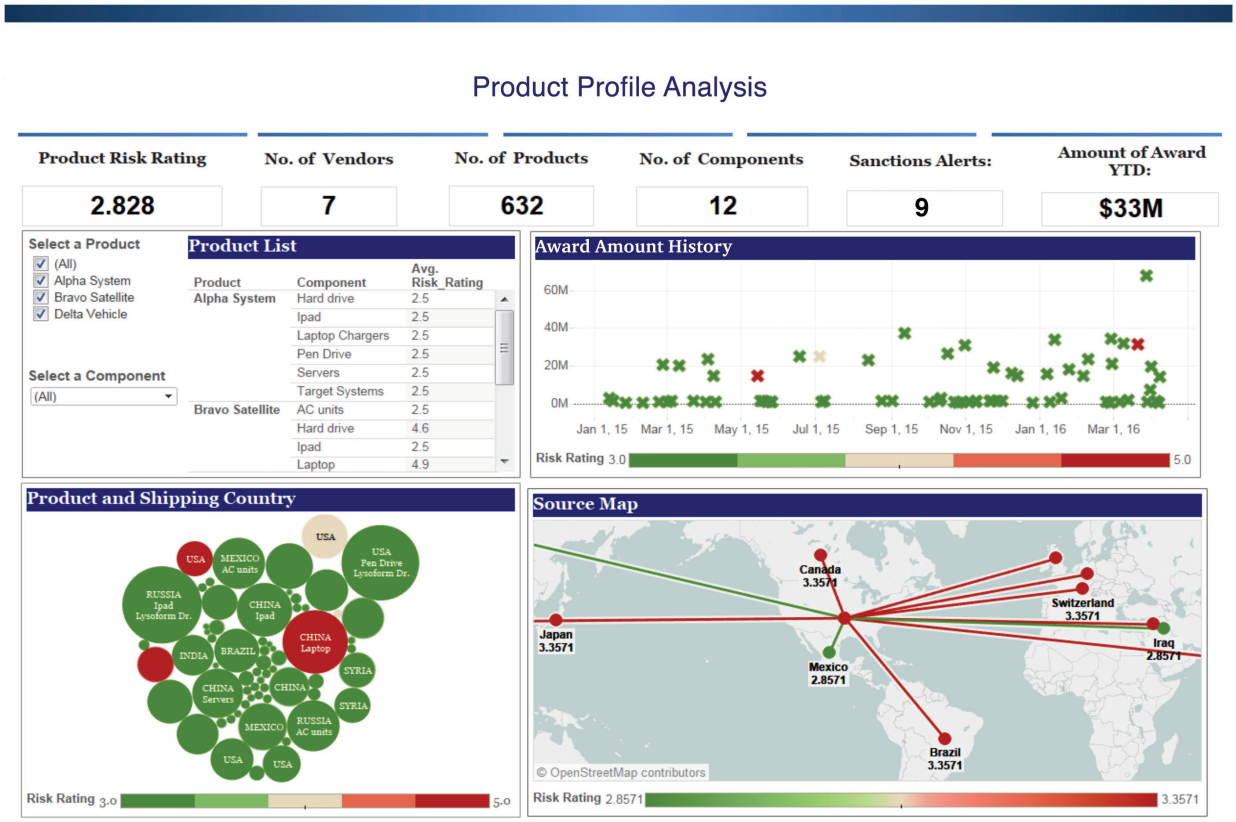
Analysis of unstructured data and unindexed Web sources

Unstructured data such as vendor contracts, site visit reports, informal documents produced by procurement, and external data sources can contain valuable information. Many companies are investing in pattern recognition, sentiment analysis, and other natural-language-processing tools to better understand their customers for marketing and service purposes, but they're also increasingly applying those tools to address supply chain risk. For example, sentiment analysis informs risk scoring by categorizing and rating comments on a positive-to-negative scale. And it's estimated that up to 90% of information on the Internet is not indexed by traditional search engines and is therefore hidden from traditional browsers.[16] This so-called deep Web is the next frontier to monitor, enabling companies to analyze entities more thoroughly. Advances in cybercrime detection and the drive to protect national security are raising levels of sophistication and availability of tools with which commercial companies can access—and draw insights from—this hidden data.

Visualization

By fusing all source surveillance into visual depictions of intelligence, leaders become able to act quickly when risk or uncertainty levels increase. Dashboards create linkages across the broad spectrum of structured and unstructured data and synthesize that disparate data into intelligence that is actionable so that decisions can be made at the speed that business requires (Figure 4). Dashboards can be tailored to fit decision-making needs at all levels and in all functions of an organization: for corporate leaders, compliance officers, and business unit managers. Corporate leaders can access risk readouts with broad indicators that support strategic decision making, and compliance and procurement can monitor the day-to-day statuses of vendors, flags, and investigations.

Figure 4: Sample supply chain risk dashboard flags vulnerabilities in the vendor network



Making it work for business

As companies invest in more-robust Know Your Vendor capabilities, certain factors will contribute significantly to building sustainable programs for them.

Success starts with leadership support

Effective change needs a tone at the top when it comes to the importance of building a culture of transparency and of managing supply chain risk. A tone-at-the-top initiative is far more than a tool implementation, and executives will be accountable to attest to external parties regarding its effectiveness. Further, this new view of supply chain risk management requires communication both up and down the organization. To accomplish it, companies must have effective governance models that can conduct investigations and manage their decision making based on the persistent and robust intelligence that analytics can provide.

It's about intelligence, not just data

The capability to create actionable intelligence from disparate—and many times unstructured—data is the key to leaders' ability to make smarter, quicker business decisions that serve to reduce risk and protect the brand. The ability to conduct link analysis enables companies to come to know the over-the-horizon vendor landscape and to understand relationships. A critical step involves making sure vendor risk ratings get combined with other supply chain risk indicators so as to have an overall risk index that increases the level of certainty behind decision making.

Don't underestimate process and training needs

Companies should invest equally in training and reskilling employees on the latest technology infrastructure and analytic tools. Qualified staff is essential for managing that overall process and completing investigations recommended by the tools and alerts. Establishing a case management process and, when possible, identifying opportunities for consolidated investigation are important to designing and implementing an efficient solution.

Costs should go down, not up

Solutions should produce net decreases in costs and reduced financial need to offset risk. Decreases in costs result from higher compliance rates, avoidance of fines, prevention of damage to brand and reputation, and reductions in the time and resources required for investigations and adjudication.

Supply chain risk 2.0: Know your vendors' networks

Analytics-based solutions are paramount to companies' ability to efficiently and effectively manage and monitor the complexity of global supply chain risk. Organizations that take a more-analytics-focused approach to managing vendor-associated supply chain risk stand to better defend themselves and their companies against costly reputational and regulatory risks. Reducing supply chain uncertainty to an achievable minimum enables companies to anticipate risk and to then act to mitigate consequences.

Beyond direct supply chain risk mitigation, companies can also derive a number of additional benefits. Supply chain risk analytics can (1) contribute to reduction of fraud exposure, (2) provide insights into instances of noncompliance with contractual terms, and (3) lead to potential cost savings through more-automated monitoring of third-party relationships and more-data-driven operational insights. Supply chain assurance can even be a competitive differentiator in an environment characterized by unprecedented consumer awareness, as more and more consumers are basing purchasing decisions on ethical considerations and as they increasingly want to know the origins of goods and services.

Finding solutions for the supply chain risk management capabilities that companies need today does not have to involve new decision science. The tools are available and have proved effective in meeting similar large-scale monitoring challenges. The tools simply have to be adapted to fit a different, and increasingly imperative, business objective.

Endnotes

1 PwC Fifth Annual Risk in Review study, Risk in Review: Going the distance, April 2016, https://www.pwc.com/us/en/risk-assurance/risk-in-review-study/risk-in-review-2016.pdf.

2 Ibid.

3 Martha Mendoza, "US lets in Thai fish caught by slaves despite law," Associated Press, April 22, 2015, http://www.ap.org/explore/seafood-from-slaves/us-lets-in-thai-fish-caught-by-slaves-despite-law.html.

4 Hope King, "Is your cell phone powered by child labor?" CNN, January 18, 2016, http://money.cnn.com/2016/01/18/technology/smartphone-child-labor-cobalt/.

5 Eric Fidel, "Supply chain alert: The risk of human trafficking," Law.com, February 12, 2016, http://www.law.com/sites/articles/2016/02/12/supply-chain-alert-the-risk-of-human-traffickin g/?slreturn=20160424160837.

6 Tom Andel, "Keep Iran Out of Your Supply Chain," *Material Handling & Logistics,* July 26, 2012, http://mhlnews.com/blog/keep-iran-out-your-supply-chain/.

7 J. Michael Martinez de Andino, "Counterfeits in the Supply Chain: A Big Problem and It's Getting Worse, *IndustryWeek,* February 3, 2014, http://www.industryweek.com/inventory-management/counterfeits-supply-chain-big-problem-and-its-getting-worse?page=2.

8 "Human trafficking and forced labor: Ethical supply chain challenges for multi-national companies," PwC, 2016, http://www.pwc.com/us/en/forensic-services/publications/human-trafficking.html.

9 Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

10 Benjamin Coulter, "The Yates Memo: Its Impact on the Prosecution of Corporations and Individual Defendants," *InsideCounsel,* March 11,2016, http://www.insidecounsel.com/2016/03/11/the-yates-memo-its-impact-on-the-prosecution-of-co?&slreturn=1464274739, and Kirkland & Ellis LLP, "$42 Million Blackwater Settlement Demonstrates ITAR Enforcement on the Rise," Kirkland Alert, September 2010, http://www.kirkland.com/siteFiles/Publications/Alert_092310.pdf.

11 Benjamin Coulter, "The Yates Memo."

12 Kirkland & Ellis LLP, "$42 million Blackwater settlement."

13 Global Supply Chain Institute, University of Tennessee, "Managing Risk in the Global Supply Chain," summer 2014, http://globalsupplychaininstitute.utk.edu/publications/documents/Risk.pdf.

14 "Vendor Controls Assurance (SOC 2+): A cost effective approach to building customer trust," PwC, 2015, https://www.pwc.com/us/en/risk-assurance-services/publications/assets/pwc-vendor-control-assurance.pdf.

15 "Name, set, match: Enhancing watch list screening through analytics," PwC, April 2016, https://www.pwc.com/us/en/risk-assurance/publications/watch-list-screening.pdf.

16 Ibukun Taiwo, "90% of the Internet Is Hidden from Your Browser; and It's Called the Deep Web," *TechCabal*, November 18, 2015, http://techcabal.com/2015/11/18/90-of-the-internet-is-hidden-from-your-browser-and-its-called-the-deep-web/.

www.pwc.com

To have a deeper conversation about building supply chain risk resiliency by knowing your vendor network, please contact:

John Sabatini
Principal
+1 (646) 471 0335
john.a.sabatini@pwc.com

Jeff Hunter
Principal
+1 (914) 374 5422
jeff.hunter@pwc.com

Norm Litterini
Manager
+1 (703) 220 2418
norman.p.litterini@pwc.com

Harrison Smith
Manager
+1 (347) 216 5521
harrison.e.smith@pwc.com