How well do you know the organizations that you're doing business with?

Due Diligence in Vetting and Monitoring Suppliers

A LexisNexis® White Paper

Introduction

In January 2014, Walmart was forced to issue a major recall of meat sold at some of its China stores after tests showed the meat contained DNA from foxes. The Chinese government got involved, the person in charge at the factory that supplied the meat to Walmart was detained, Walmart was forced to reimburse customers and the company was the subject of embarrassing news stories worldwide.

In the aftermath of the incident, the comments from Walmart China's president and chief executive officer, Greg Foran, were very instructive: "We are deeply sorry for this whole affair. It is a deep lesson that we need to continue to increase investment in supplier management."[1]

Two months prior, during the 2013 winter holiday shopping season, another prominent Fortune 500® company suffered a massive data breach as a result of a third-party security hack. In December 2013, Target disclosed that it had been the victim of a major credit card security breach. Experts believe the thieves gained access to roughly 40 million credit and debit card numbers and the personal information (including names, email addresses, phone numbers and home addresses) of as many as 70 million customers. The subsequent investigation found that the hackers may have used a third-party Target contractor — a Pittsburgh-based heating and refrigeration business — as the back door to get in.

Every large corporation is faced with the same challenge: you need to do business with third-party suppliers to deliver products and services to customers, but you're also vulnerable to a wide variety of problems — ranging from operational disruptions to legal exposure — if those suppliers let you down.

Commenting on the Walmart meat recall in China, Richard Matthews, head of product liability at global law firm Eversheds, said that while "the unusual circumstances of this 'fox meat' scandal in China" are unlikely to be replicated elsewhere, the story "illustrates the importance of supplier due diligence and the vulnerability of multinational businesses of damage to their reputation, even in markets where the regulatory frameworks and consumer expectations may be less well-developed."[2]

The purpose of this white paper is to draw attention to the importance of thoroughly vetting third-party suppliers. The risks of doing business with suppliers that fail to perform appropriately include potential supply chain disruption, reputational damage and even government investigations that may arise when regulatory compliance issues are involved.

Risks of Doing Business with Third Parties

Most companies have relationships with a wide range of third-party organizations that help them get things done. These third-party business relationships include suppliers, distributors, consultants, accountants and lawyers. And while these third parties are essential to every major company if they are to grow and succeed in the marketplace, they bring with them all sorts of new risks that need to be mitigated and managed.

The Walmart and Target examples are glaring ones, but there are dozens of others that have been in the news over the past several years. Here are just a few:

- In 2012, the SEC charged a top pharmaceutical company for using third-party intermediaries to make improper payments to foreign officials;

- In 2013, a major aerospace contractor was forced to conduct a review of potentially deficient parts that were provided by a titanium supplier—the same supplier that was investigated and subsequently fined by the U.S. Attorney's office in 2007 for falsely certifying the titanium they sold at that time;

- In 2012, a number of technology companies were dragged into embarrassing news stories when a third-party contractor was found to be violating labor and working conditions rules in its factories with illegal amounts of overtime, crowded working conditions, under-age workers, and, in some cases, serious industrial accidents; and

- In 2011, a major U.K.-based insurance company was fined for inadequate anti-bribery and corruption systems controls related to payments made by the company to overseas third parties.

Supply Chain Risk

In recent years, supply chains have become more complex and larger as the drive for efficiency has led to increased outsourcing, sub-contracting and the search for lower cost providers. It's likely that your company is in danger of having to stop or delay operations if you're prevented from obtaining the tools, supplies or necessary services at your various places of business.

For example, in November 2012, a fire erupted at an apparel factory in Bangladesh, tragically killing 112 workers, many of whom were unable to escape due to locked doors and windows. Journalists on the scene who were literally sifting through ashes and charred clothing labels identified a number of prominent customers being supplied by that factory.

Supply management officials at those companies were surprised to learn that the Bangladesh factory was even manufacturing clothing for distribution in their stores, let alone stuck with the consequences of having their supply chain disrupted.

Financial Risk

Chances are that your business agreements with third parties include some contractual terms that even your most loyal suppliers will seek to ignore or step around from time to time. Likewise, suppliers who appear to be on solid financial ground may actually be on thin ice when it comes to their capitalization.

The 2013 bankruptcy of KSL Media illustrated the risks when an advertiser entrusts significant funds to a third party that ultimately proves to be financially unstable. Many companies pre-paid for KSL services and the would-be supplier went out of business prior to delivery. Undercapitalized or fiscally imprudent third-party business partners can pose significant financial risk to the corporation.

Security Risk

Perhaps the most disconcerting illustration of security risks posed by third parties in today's economy is in the area of intellectual property. Counterfeiting, piracy, trade secret theft and trademark infringement are all serious considerations for any company, but IP theft is a particular vulnerability when it comes to working with third-party business partners.

A 2013 report by The Conference Board found that roughly half of the executives surveyed perceived extensive risk of IP infringement in emerging markets when engaging suppliers (43 percent) and when engaging agents/business partners (48 percent)[3]. Other examples of security risks include competitive threats, such as conflicts of interest, and information technology problems, such as systems failures or even cyber crime. These operational risks to an enterprise from third parties that fail to perform appropriately are serious and can have measurable financial consequences.

Emerging Regulatory and Compliance Mandates

In addition to these areas of operational risk associated with doing business with third parties, there are a number of new regulatory mandates that constitute an entirely separate area of compliance risks to any company that engages third-party suppliers.

These critical regulatory guidelines are serious business; failure to comply with them can mean more than just a sluggish quarterly performance or a series of embarrassing news stories, they can involve government investigations and perhaps even prosecutions for breaking the law. This includes anti-

bribery legislation, labor laws, federal government regulations, and federal, state and local tax laws.

The best illustration of this flurry of new regulatory mandates is in the financial services business. Here are just a few examples of new regulatory mandates that pose compliance risk in doing business with third parties if you're in the financial industry:

New guidance on risk management

In October 2013, the U.S. Department of Treasury's Office of the Comptroller of the Currency—commonly referred to as the OCC—provided new guidance to national banks for assessing and managing risks associated with third-party relationships. In its bulletin, the OCC makes it clear that it "expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws."

SEC's new "covered person" provisions

In July 2013, the Securities and Exchange Commission finalized amendments to Rule 506, which require private investment funds to conduct due diligence to confirm no "covered person" has engaged in a "disqualifying event," also known as the "Bad Actor" provisions. This new rule was broadened specifically to include third parties and various categories of business partners.

CFPB expectations for supplier due diligence

The newly created Consumer Financial Protection Bureau (CFPB) released a bulletin in April 2012 clarifying that financial institutions may be held responsible for the actions of the companies with which they contract. The agency now expects for companies to have an effective process for managing the risks of service provider relationships, including conducting thorough due diligence to verify that service providers understand and comply with the law.

Of course, there is also a wide range of recent compliance requirements that affect virtually all large corporations with interests in multiple jurisdictions around the world. Legislation against bribery and corruption — such as the U.K. Bribery Act and the U.S. Foreign Corrupt Practices Act — have put a scare into all corporate executives whose companies do business in global markets where bribery of government officials used to be known as the normal course of business. And some states have taken aggressive steps to mandate more visibility into supply chains, such as the California Transparency in Supply Chains Act that went into effect in 2012.

This law requires that retailers and manufacturers doing business in California (with more than $100 million in annual sales) must disclose their efforts to eradicate slavery and human trafficking from their direct supply chains for goods offered for sale. Other states are looking at adapting similar regulations now.

These emerging regulatory mandates that apply to your third-party business relationships pose a major compliance risk to corporations. Worse yet, those suppliers that are further removed from the company's immediate major suppliers may pose the biggest supply chain risk. A survey by the Business Continuity Institute found that almost 40 percent of reported supply chain disruptions originated with Tier 2 and Tier 3 suppliers.[4] The lesson is that supply chain problems can come from virtually any supplier in the world at any time.

Importance of News and Public Records Updates

These operational and compliance risks are formidable, but the reality is that every major corporation must be able to enter into new business relationships with third parties to survive. So what is a corporate executive to do to mitigate those risks?

The answer is that you must commit to aggressive due diligence in the vetting of your third-party suppliers, and then invest in ongoing monitoring of those suppliers. One crucial element of this due diligence is to take advantage of emerging business information tools now available to businesses that can help you screen and then closely monitor those key suppliers.

Unfortunately, many corporate executives have been lulled into the false notion that they can rely on traditional sources of information used to monitor supply chain risks — such as financial scores,

background reports and, in the past decade or so, occasional Google™ searches — to conduct this due diligence. While these methods still have value, they are no longer sufficient on their own because they are unable to uncover potential supplier business issues in real time, nor perhaps before they have blown into problems more visible to the public.

For the initial vetting of third parties, it's important to review reports about the potential new supplier in both news media accounts and in various public records databases. For example, real-time supplier information can be used to identify potential areas of concern with an individual supplier before you sign on the dotted line and become formal partners.

If an ounce of prevention is worth a pound of cure, then surely the ability to sniff out some worrisome information about a potential third-party supplier — such as legal problems, financial problems or compliance issues — is far preferable to discovering these things after a problem has already flared up and caused a business problem.

After a new relationship has been put in place, however, the fact is that a one-time vetting of a supplier is just not enough. It's important to invest in ongoing monitoring of third parties with whom your company is doing business.

While financial scores and open Web searches can be helpful in making quick decisions about suppliers and their financial health, this can hardly be considered due diligence because it is relying on limited data that is, at best, a lagging indicator of what is truly going on with your third-party suppliers. By the time a company has stopped paying their bills and their financial score has changed, it's often too late for you to take action to minimize the impact on your company — whether that impact is reputational, operational or legal.

Business information services that monitor news articles and public records mentioning your third-party suppliers are powerful tools for helping corporations to more thoroughly vet a supplier before entering into a relationship with them. Once those contracts are signed with new suppliers, these same services can be valuable ways to conduct ongoing due diligence by monitoring the activities of those suppliers as much as possible. This is an important strategy for conducting aggressive due diligence and protecting your company from problems arising from doing business with third-party suppliers that fail to perform appropriately.

LexisNexis® Supply Management Solutions

Powered by the unsurpassed LexisNexis database of real-time news and public records content, LexisNexis® Supply Management Solutions can be used by corporate executives to conduct due diligence, comply with regulatory requirements and create an "early warning system" for potential supplier risks through ongoing monitoring.

For more information

LexisNexis Benelux, Amsterdam

T +31 (0)20 485 34 56
E servicedesk@lexisnexis.nl
W www.lexisnexis.nl

1. www.foxnews.com/world/2014/01/02/walmart-recalls-donkey-product-in-china-after-other-animal-dna-found-in-it/
2. http://press.eversheds.com/Latest-views/Eversheds-comment-Wal-Mart-fox-meat-scare-echoes-2013-horsemeat-scandal-e91.aspx
3. http://www.executiveboard.com/blogs/supply-chain-risk-too-important-to-ignore/
4. http://www.bcifiles.com/Mumbai/LyndonBMumbai.pdf

LexisNexis®