The Risk Monitoring Imperative

A practical guide for increasing visibility to potential risks

LexisNexis®

Why Monitoring Matters:

Among ABC survey respondents, 55% reported uncovering third-party legal, ethical or compliance issues after due diligence was complete.[1]

1. http://www.kroll.com/en-us/abc-report
2. https://erm.ncsu.edu/az/erm/i/chan/library/2017-Top-Risks-Executive_Perspectives-Protiviti-NC-State-ERM.pdf
3. http://www.kroll.com/en-us/abc-report
4. http://www.kroll.com/en-us/abc-report
5. http://www.kroll.com/en-us/abc-report

The Risk Monitoring Imperative

Organizations today face an evolving array of risks—and corporate boards and executive leaders are feeling the pressure. According to a global survey of board members and C-suite executives, "The impact of the U.K. Brexit vote, increased volatility in commodity markets, polarization surrounding the recent U.S. presidential election, terrorist events, asset bubbles in China, continued discussion about fair wages and income equality, and ongoing instability in the Middle East" has resulted in elevated concerns about business risk in 2017.[2]

Moreover, companies increasingly rely on third parties to conduct business—from complex, globally-distributed supply chains to extensive networks of clients, partners, or agents working on their behalf. How vast are these networks?

- 40% of companies oversee 1,000 third parties annually[3]
- 29% manage more than 5,000 third-party relationships[4]

And those numbers don't include customers. As a result, companies need a risk mitigation strategy that goes beyond traditional due diligence for on-boarding suppliers and third parties. The 2017 Anti-Bribery & Corruption Benchmarking Report, issued jointly by Kroll® and Ethisphere®, found that "More than half (55 percent) of respondents report that they identified legal, ethical, or compliance issues with a third party after due diligence had been conducted."[5] Ongoing monitoring can help you build a more complete picture of risk exposure—and proactively mitigate risk.

40% OF COMPANIES OVERSEE 1,000 THIRD PARTIES ANNUALLY

29% MANAGE MORE THAN 5,000 THIRD-PARTY RELATIONSHIPS

What types of risk do organizations face?

Business risks generally fall into four categories: reputational, regulatory, financial and strategic. Let's take a closer look at the types of risk that require ongoing monitoring.

REPUTATIONAL RISK

Protecting corporate and brand reputations has long been a risk consideration, but the Harvard Business School "Working Knowledge" blog notes, "In this age of 24-hour information, the traditional news cycle is long dead and buried. Assume the information will get out sooner or later—and most likely sooner."[6] Lynn Schulman, national crisis director for Magnet Communications in New York City, admits, "You have to think that everything your company does will reach the outside world."[7]

Corporate leaders are sensitive to the shift: In the 2017 Anti-Bribery & Corruption Benchmarking report, for example, reputational concerns moved from least likely to most likely reason for a third party to fail vetting standards in just one year.[8] They are right to be concerned because it's not just regulators that are watching. Consumers pay attention too, and when they lose trust—whether due to a data breach, product recall, regulatory or social compliance failures, consumers speak with their wallets.

REGULATORY RISK

Mitigating regulatory risk is a top concern, especially given the evolving regulatory environment and the leap in enforcement actions. The TRACE International 2016 Global Enforcement Report (GER) found a significant year-over-year increase in the number of U.S. and non-U.S. enforcement actions related to bribery of foreign officials. In the U.S., for example, the number of enforcement actions was double that of the previous year. In non-U.S. jurisdictions, TRACE International notes, "European countries remain at the forefront of this trend, together accounting for 42% of all open investigations, compared to the 46% being conducted by the U.S. The United Kingdom remains the leader within Europe with 29 open investigations, followed by Germany with 17."[9]

6. http://hbswk.hbs.edu/archive/2402.html
7. http://brandchannel.com/2017/02/09/harris-corporation-reputation-poll-020917/
8. http://www.kroll.com/en-us/abc-report
9. http://traceinternational.org/GER

WHAT IS SOCIAL COMPLIANCE?

Social compliance refers to pressure on companies—from non-governmental organizations, consumer groups and consumers—to adhere to ethical business practices and require the same adherence from suppliers and third parties. Laws like the UK's Modern Slavery Act or California's Transparency in Supply Chains Act serve to increase the pressure.

When children are discovered laboring in a cobalt mine in the Congo, unsafe conditions in a clothing factory in Bangladesh lead to preventable deaths or forced labor takes place on a scallop dredger off the coast of Scotland, major media outlets are covering it. The increased visibility that always-on media affords—combined with greater awareness about forced labor, workplace safety, eco-sustainability and more—means that companies must now address traceability along their supply chains to meet both regulators' and the public's expectations.

"THE UNITED STATES HAS BEEN CONCLUDING ENFORCEMENT ACTIONS AT AN UNPRECEDENTED RATE, OTHER JURISDICTIONS HAVE BEEN STEPPING UP THEIR PROSECUTION RATES AS WELL, AND NEW ANTI-CORRUPTION LAWS CONTINUE TO BE PASSED WORLDWIDE."

In addition, the GER revealed that Engineering/Construction, Extractives and Manufacturing/Service industries are more vulnerable to non-U.S. actions related to domestic enforcement. Foreign enforcement, on the other hand, targets Extractives the most, with Engineering/Construction and Transportation/Communications close behind. Alexandra Wrage, president of TRACE International, says, "The United States has been concluding enforcement actions at an unprecedented rate, other jurisdictions have been stepping up their prosecution rates as well, and new anti-corruption laws continue to be passed worldwide."[10] Wrage continues, "Although there may be short-term fluctuations in these trends, we believe this represents the continued development of a global consensus that transnational bribery will not be tolerated."[11]

Banks and other financial services providers also have anti-money laundering compliance requirements to consider—and these issues often overlap with social compliance because the proceeds from forced labor and human trafficking may be involved. A report from the Royal United Services Institute for Defence and Security Studies notes that banks can monitor for negative media related to "... the existence of a branch network, the extent of their geographic footprint or based on previous defined financial crime priorities" to help spot signs of human trafficking.[12]

ACTIONS RELATED TO FOREIGN OFFICIAL BRIBERY

10. https://www.traceinternational.org/blog/875/Notable_increase_in_bribery_enforcement_worldwide_according_to_TRACE_s_2016_Global_Enforcement_Report

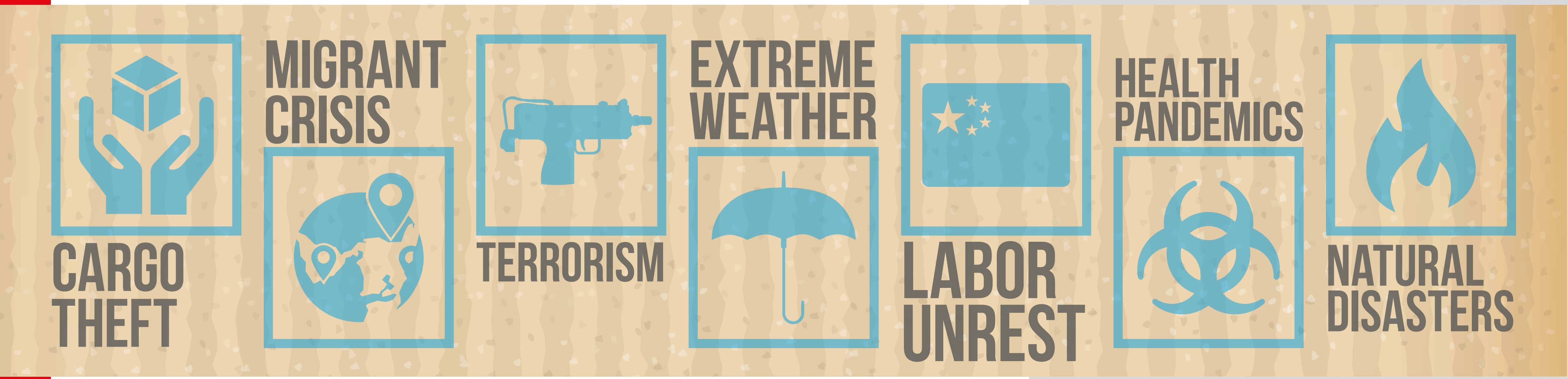
11. https://www.traceinternational.org/blog/875/Notable_increase_in_bribery_enforcement_worldwide_according_to_TRACE_s_2016_Global_Enforcement_Report

12. https://rusi.org/publication/whitehall-reports/disrupting-human-trafficking-role-financial-institutions

FINANCIAL RISK

While financial risk scores are a typical consideration in third-party onboarding, companies cannot afford to let down their guard. Financial risks manifest in numerous other ways. Supply chain disruption bears a heavy cost. Research from the British Standards Institute (BSI), for example, found that such disruptions led to an estimated $56 billion in added costs in 2015.[13]

$56 BILLION MORE SUPPLY CHAIN COSTS DUE TO:

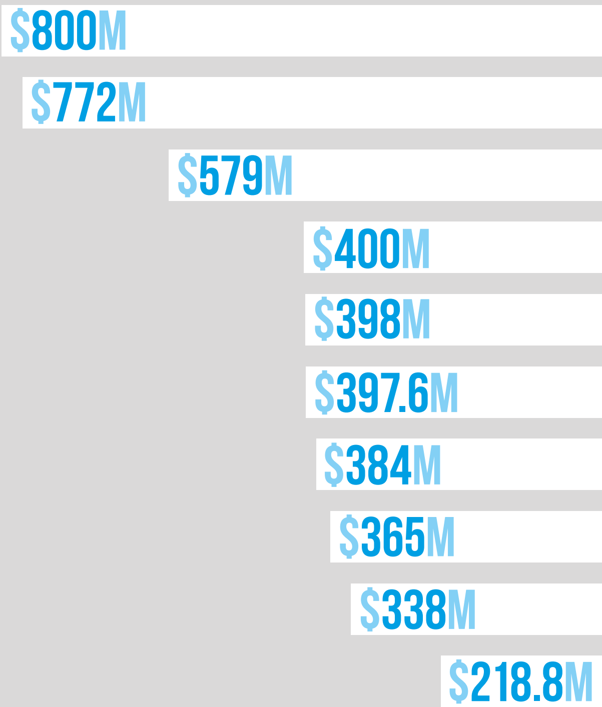


In addition, the negative impact reputational damage can be significant. Yahoo's delayed disclosure of two cybersecurity breaches not only harmed the brand in the eyes of consumers, but it also put the brakes on a multibillion-dollar acquisition deal with Verizon and led to a 7 percent drop in Yahoo's share price.[14]

Likewise, regulatory compliance failures can result in fines, settlements and remediation measures that take a financial toll and limit future business opportunities. Companies need ongoing monitoring of supply chains and third parties for compliance with anti-money laundering (AML) and anti-bribery and corruption (ABC) compliance, including checking against sanctions, watch lists and PEPs. As of 2016, for example, the top 10 U.S. Foreign Corrupt Practices Act (FCPA) cases incurred financial penalties of $4.65 billion.[15]

13. https://sourcingjournalonline.com/here-are-the-biggest-threats-to-the-global-supply-chain-in-2016-td/
14. http://www.inc.com/salvador-rodriguez/biggest-pr-fails-2016.html
15. http://www.fcpablog.com/blog/2016/2/19/heres-our-new-top-ten-list-with-vimpelcom-landing-sixth.html

TOP 10 FCPA FINANCIAL PENALTIES



1. Siemens (Germany): $800 million in 2008.
2. Alstom (France): $772 million in 2014.
3. KBR / Halliburton (USA): $579 million in 2009.
4. BAE (UK): $400 million in 2010.
5. Total SA (France) $398 million in 2013.
6. VimpelCom (Holland) $397.6 million in 2016.
7. Alcoa (U.S.) $384 million in 2014.
8. Snamprogetti Netherlands B.V. / ENI S.p.A (Holland/Italy): $365 million in 2010.
9. Technip SA (France): $338 million in 2010.
10. JGC Corporation (Japan) $218.8 million in 2011.

STRATEGIC RISK

All three of the previous risk categories contribute in some way to the fourth category: Strategic risk. When a company fails to spot reputational, regulatory or financial risks among the third parties on which it relies, it can slow or even impede growth. Visibility into potential risks is also critical when organizations seek to identify new supplier sources or expand into emerging markets. And, of course, companies need to have a demonstrable, effective due diligence and risk monitoring process in place to meet the expectations of stakeholders and strategic partners.

How Risk Monitoring Helps

In addition to monitoring the media for negative news mentions of third parties, companies need to implement ongoing risk-based monitoring. Companies in highly-regulated industries, for example, may already monitor for compliance risk, but they also need to track the regulatory rulemaking environment to understand how compliance risks may change as new policies or guidance come to light.

Using a risk-based approach brings greater focus to risk monitoring by allowing organizations to assign priorities based on their unique situation.

Just as PESTLE categories can help companies analyze their own strengths, weaknesses, opportunities and threats, those categories—when applied to risk monitoring—can help companies spot relevant information sooner. A risk-based approach to monitoring, in fact, offers a strategic advantage given the sheer volume of news, industry, country, legal and regulatory data that merits ongoing consideration.

Onboarding due diligence alone is not enough to mitigate risk. Companies need to integrate risk monitoring into their process to complement conventional financial risk scoring and to better anticipate supplier and third-party risks on a continuing basis. In fact, the 2017 Anti-Bribery & Corruption Benchmarking Report found that 50 percent of organizations that discovered issues with third parties after their initial due diligence investigations did so because of ongoing monitoring.[16]

16. http://www.kroll.com/en-us/abc-report

P

POLITICAL: Tax policies, trade tariffs, political unrest, government ethics

E

ECONOMIC: Inflation rate, interest rates, foreign exchange rates, economic growth patterns

S

SOCIO-CULTURAL: Cultural trends, population changes, immigration, education levels (of consumers and workers)

T

TECHNOLOGICAL: Availability and reliability of power or internet access, vulnerability to cyber attack, automation, rate of innovation or technology adoption

L

LEGAL: Regulatory landscape for anti-money laundering and anti-bribery and corruption compliance as well as consumer laws, safety standards, labor laws

E

ENVIRONMENTAL: Climate, weather, geographical location, global changes in climate

"COMPANIES SHOULD UNDERTAKE SOME FORM OF ONGOING MONITORING OF THIRD-PARTY RELATIONSHIPS. WHERE APPROPRIATE, THIS MAY INCLUDE UPDATING DUE DILIGENCE PERIODICALLY, EXERCISING AUDIT RIGHTS, PROVIDING PERIODIC TRAINING, AND REQUESTING ANNUAL COMPLIANCE CERTIFICATIONS BY THE THIRD PARTY."

A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT[17]

17. https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf

LexisNexis®

About LexisNexis®

We help our customers mitigate business risks, meet their strategic goals and accomplish greater return on investment. Using our efficient, agile and cost-effective due diligence and monitoring solutions empowers our customers to find the information they need on people, companies and countries. Our experienced industry specialists and thought leaders are well-versed in the evolving requirements our customers need to address.

LexisNexis Business Insight Solutions delivers interconnected and flexible product modules aligned to the customer workflow including:

» PEP, watch list and negative news screening
» Enhanced due diligence and reporting
» Proactive supply-chain and third-party risk media monitoring that leverages PESTLE-based risk scoring
» Outsourced due diligence, compliance and risk advisory
» Content integration and data feeds into proprietary systems

Ask us how LexisNexis® Entity Insight can help you conduct proactive, risk-based monitoring to improve visibility into potential reputational, regulatory, financial and strategic risks.

For More Information

Due Diligence Solutions:
internationalsales.lexisnexis.com/produtcts/diligence