# A triple threat across the Americas: KPMG 2022 Fraud Outlook

## Sector Spotlight: Energy and Natural Resources

## Five things energy and natural resources executives need to know

KPMG's "A triple threat across the Americas" highlighted the overlapping fraud, non-compliance, and cyber-attack challenges that confront businesses across all sectors today. This follow-up piece reviews the dangers facing energy and natural resources (ENR) companies, and outlines five things that sector executives need to know:

### 01 Energy and natural resources business are less likely to report experiencing fraud than those in other sectors, but they may simply be missing more perpetrators.

The size of the ENR sector's fraud problem can be interpreted in different ways. An optimist would note that the 62% of industry firms which experienced a fraud in the last 12 months is comfortably below the survey average (71%). A realist would point out that higher crime frequency elsewhere does not change the problem that fraud remains the norm, not the exception, at energy and natural resources firms. The figures for the mean economic cost of fraud provide less comfort to any hopeful executives. ENR companies, on average, lost 0.45% of profits to these crimes over the last 12 months, which is very close to the overall survey figure (0.48%). This suggests that, even if less frequent, individual frauds against energy and natural resources firms are typically more costly than those elsewhere.

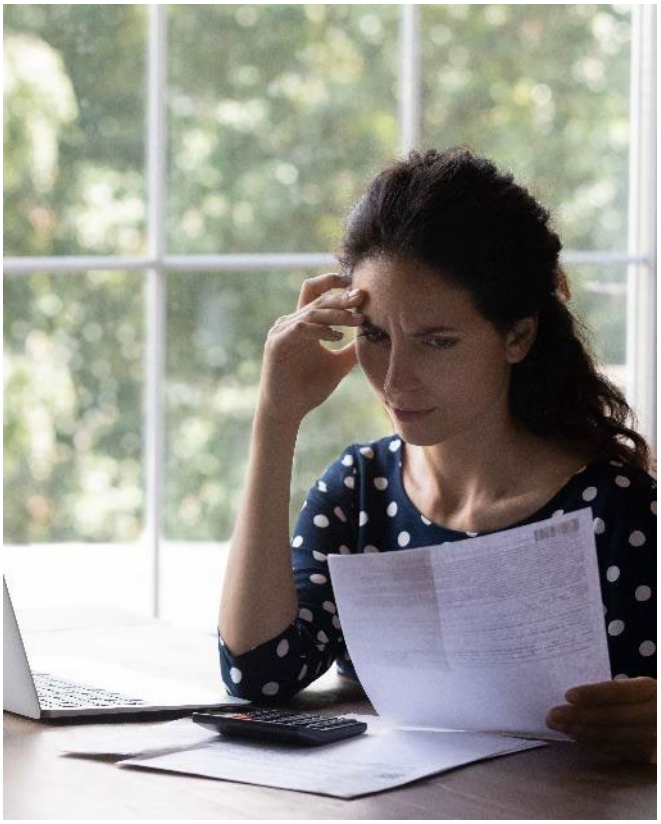
A final concern about fraud levels affecting the sector is that its companies may catch a smaller share of criminals than firms in other industries. For example, ENR businesses were least likely of those in any sector to report finding fraud through an internal audit in the preceding 12 months (26% compared to 34% overall), but most likely to say that an external audit revealed one (21% to 14%). Similarly, only 17% of ENR respondents say that data analytics revealed fraud in the last year, the lowest for any sector and well below the survey average of 27%. It is difficult to be certain, in any given case, whether illicit activity is not occurring or is merely undiscovered, but these data do make the latter possibility a substantial concern.

## 02 Complacency surrounding fraud is a danger among energy and natural resources companies.

The survey answers from this industry reveal an insufficient concern about fraud risk. For example, while 76% of ENR respondents consider their company fraud response plans somewhat or extremely effective, only 45% actually include a response element in their anti-fraud programs. The latter is the smallest figure for any sector. In other words, at least 31% say that non-existent efforts are somewhat effective.

More striking, 74% of ENR respondents believe that in the next year the risk of fraud from perpetrators inside the company, outside the company or both will go up. This is the second highest sectoral figure (after life sciences' 76%) and markedly higher than the survey average of 66%. Meanwhile, 67% report that "the anti-fraud controls we had in place pre-pandemic have not been effectively updated to reflect the new working reality." That is the highest proportion for any industry. The clear need, then, is for better defences, but only 38% of ENR respondents expect corporate investment in anti-fraud measures rise in the coming year – this time the lowest sector figure and in marked contrast to the survey average of 53%.

This combination of attitudes exacerbates risk. One of the worst scenarios for fraud is when employees recognise an absence of investment in controls. Those who can rationalise engaging in fraud – a growing number amid high inflation in many countries – will likely see an opportunity.

## 03 Specific fraud risks for the sector appear to come, literally, with the territory.

Despite lower than average overall fraud figures, ENR companies are the most affected of any by two specific kinds of crime: 18% of sector companies suffered from vendor/supplier fraud in the past year. The survey average was just 13%. Similarly, bribery came to light at 13% of businesses in the industry, against just 9% overall. These specific fraud schemes may reflect an attribute of the ENR activity. Businesses need to operate wherever it is possible to extract product, limiting their ability to choose environments with lower fraud risks. If unable to move locations good defences against fraud constitute one of the only viable options for the industry.

## 04 Environmental compliance, a high-profile and growing concern for energy and natural resources businesses, is receiving attention.

These respondents are the most likely of any sector to expect new environmental regulatory or compliance requirements will affect them in the next five years (54% compared to 47% overall). On the positive side, industry environmental compliance programs are much more likely than average to follow international best practice: 31% of sector respondents say that their companies meet this standard, compared to just 21% overall.

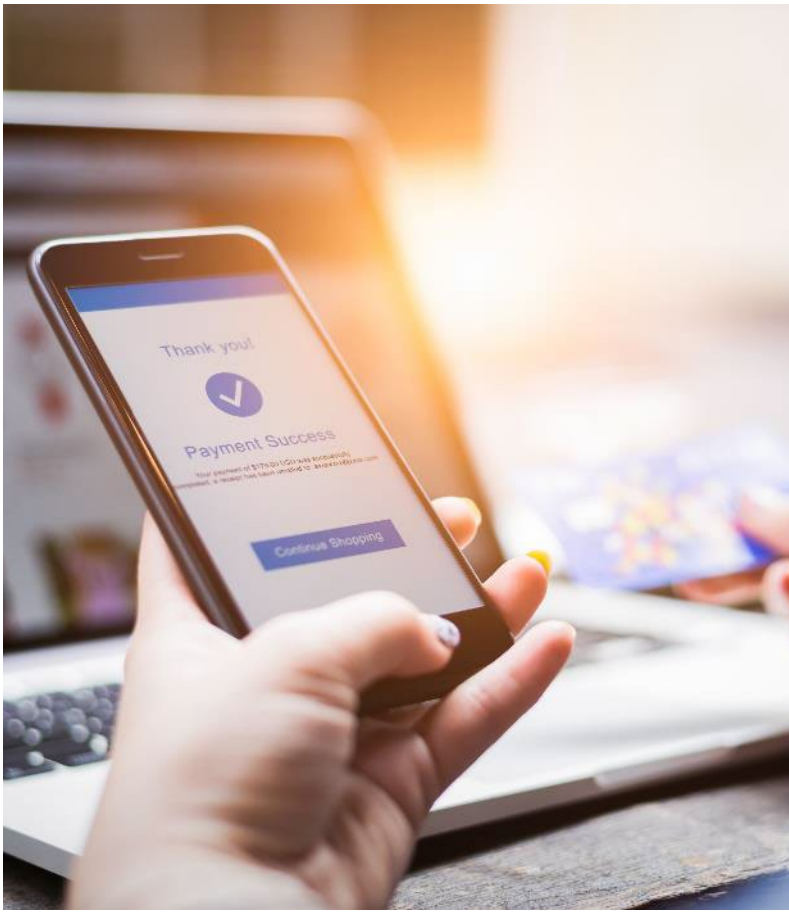
It is an open question whether this is a high enough proportion when extractive industries in particular are associated with high environmental footprints. For these companies, their metaphorical and actual license to operate is tied up with strong compliance programs: 85% of ENR experts report that reputational risks are causing leadership in their company to pay substantial or greater attention to compliance issues; 80% say the same of more rigorous enforcement; and 80% again of the demands by clients or suppliers. A majority of industry firms are playing it safe: 53% expect to increase spending on general regulatory compliance in the coming year, the highest sector figure.

## 05 Cyber-security is another field where apparent over-confidence is a danger.

ENR respondents know that cyber-risks are substantial. To cite one example, 69% would not be surprised to hear in the next year that customer private data had leaked from their company in some way. Looking ahead, 71% expect to see an increase in overall cyber-risk in the coming year and only 8% a decline.

This goes beyond the generally growing level of cyber-risk facing all businesses. Sector companies, notably energy ones, are particularly tempting targets for hackers at the moment both because of their monetary assets and because they deliver critical infrastructure to societies.

Given this worrying risk environment for the industry, other responses seem to reveal a jarring excess of self-belief. To begin with, 87% of ENR executives say that company controls to prevent data loss from employee mistakes are somewhat or very effective, making this the most confident sector response on this question. Meanwhile, 51% of those same respondents would not be surprised to hear of a leak of client data from employee equipment. More striking, 86% are somewhat or completely satisfied with how quickly their companies can identify attacks on their IT system, but only 21% of these companies can do so in a week or less, the lowest sector figure.



## Sector Spotlight: Energy and Natural Resources

The world is always changing but, occasionally, it experiences a dramatic inflection point. The COVID-19 pandemic reset all kinds of assumptions about how people live and work. Now, geopolitical events are exposing the fragilities of people's assumptions about the international environment.

The risk landscape that businesses are grappling with has been similarly reshaped. The need to maintain access to supplies has driven many companies to rely on previously unvetted partners, potentially raising new fraud risks. On compliance, the drive for net zero is expected to create further environmental regulation and new global sanctions may lead to more stringent oversight of financial and trade activity. Finally, cyber-attacks, already on the rise during the pandemic, are allowing cyber threat actors to pursue a range of aims.

The ENR sector faces urgent new threats for which it must be prepared. For example, sector companies, notably energy ones, are especially tempting targets for hackers, both for their financial assets and because they deliver critical infrastructure to societies. KPMG has seen evidence of bad actors seeking to identify individuals within these organizations who might be willing to help them gain a digital foothold.

In short, if your company has not recently conducted a full review of its fraud, compliance, and cyber security risks, it should conduct one as soon as possible. Otherwise, your defenses may not be tailored to combat today's threats, or be able to react as those risks rapidly evolve.

For some ENR companies, this may require a difficult change of course. During the pandemic, lower prices caused energy companies in particular to retrench. This, in turn, led to a greater emphasis on day-to-day business and a reduced focus on anti-fraud controls and internal audits. Our survey results repeatedly highlight the resultant poor efficacy of security control when these measures are neglected. With prices recovering, there are no excuses not to address the triple threat aggressively.

For those ready to do so, the basic framework of prevention, detection, and response remains the soundest foundation for addressing fraud, non-compliance and cyber-attack. The environment in which these defenses are deployed, however, means that they should retain the most effective elements and build upon them to defeat evolving threats.

### Prevention

In our view, certain elements will remain largely the same, such as implementation or enhancement of internal controls; risk-based integrity due diligence on employees and third-parties; security assessments of critical information systems; and simulated cyber attacks to expose exploitable vulnerabilities. Others are expected to take a new shape. For example, implementing rules on exceptions to vendor due diligence policies may be necessary amid supply-chain shortages, but companies need to balance strategic necessity with the imperative to avoid falling victim to fraud and staying on the right side of regulation.

### Detection

We believe tools such as data analytics, internal audits, and cyber intrusion detection protocols will remain fundamental, but the misbehaviors they look for may be different. Moreover, even where more employees are working at home, theirs are the eyes and ears that will see compliance failures or fraud. Measures that companies should take include updated training on fraud and compliance risks, and on the importance of reporting unusual behavior through existing incident-reporting mechanisms

### Response

Protocols must be in place to respond to fraud, instances of non-compliance and cyber breaches. Companies also need to be ready for the emerging challenges within today's risk triangle. This might include, for example, deciding ahead of time whether you are willing to pay in the event of being hit by ransomware or choosing in advance who would make that call.

**For further information on how KPMG can help you, please contact us:**


**Marc Miller**
Partner, Advisory
Americas* and US Forensic Lead
KPMG US

**Ivan Velez-Leon**
Managing Director, Advisory
Forensics
KPMG US

**Ana Lopez Espinar**
Partner, Advisory
Co-Lead, Forensic Practice South America*
KPMG Argentina

**Emerson Melo**
Partner, Advisory
Co-Lead, Forensic Practice South America*
KPMG Brazil

**Luis Preciado**
Lead Partner
Risk Advisory Solutions
KPMG Mexico


**Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities**

**kpmg.com/socialmedia**