Economist Intelligence Unit OVERVIEW

For the seventh year running, The Economist Intelligence Unit, commissioned by Kroll, surveyed senior executives from around the world across a wide variety of sectors and functions. This year's 901 respondents report that fraud remains a widespread problem regardless of the industry or region in which their businesses operate. It is also as protean, and hence unpredictable, as ever. The results of our 2013 report reveal a number of key insights.

1. The incidence and costs of fraud rose markedly in the past year, in turn driving up companies' sense of vulnerability.

According to this year's survey, the level of fraud increased by every measure in the past 12 months, reversing recent trends. Overall, 70% of companies reported suffering from at least one type of fraud in the past year, up from 61% in the previous poll. Individual businesses also faced a more diverse range of threats: on average, those hit in the past year suffered 2.3 different types of fraud each, compared with 1.9 in 2012. Finally, the economic cost of these crimes mounted, increasing from an average of 0.9% of revenue to 1.4%, with one in 10 businesses reporting a cost of more than 4% of revenue.

The damage occurred in a wide variety of ways. Every kind of fraud covered in the survey saw an increase in incidence, with vendor, supplier or procurement fraud and management conflict of interest seeing the biggest growth.

The survey offers little hope for relief on the immediate horizon. Of those surveyed, 81% believe that their firm's exposure to fraud has increased overall in the past 12 months, up from 63% in the previous survey. Respondents attribute this increase to the complexity of information technology (IT) infrastructure, high staff turnover and entry to new, riskier markets.

Just as striking, the share of respondents perceiving a high threat from individual types of fraud has more than doubled in every case. As previous reports have discussed, recent experience with fraud tends to raise feelings of vulnerability, but the sharp growth in the latter this year far outpaces even that of fraud incidence. This suggests that companies are becoming increasingly sensitized to the threats they face and their (sometimes) inadequate protection.

Perhaps the most worrying finding in this year's survey is that, for six of the 11 types of fraud covered by the survey—corruption, money laundering, regulatory breach, misappropriation of company funds, IP theft and market collusion—the percentage of executives admitting that their firms are highly vulnerable to fraud was higher than the proportion of companies that have been hit in the past year. This indicates that fraud has fertile soil in which to grow.

2. Information-related fraud is common and evolving, but many companies are not prepared for when things go wrong.

Information theft remains the second most common fraud, affecting more than one in five companies over the past year, and three-quarters of respondents describe their businesses as at least moderately vulnerable. Looking ahead, complex IT structures are the most commonly cited reason for an increase in overall fraud exposure (named by 37% of respondents), suggesting that there will be no quick diminution of the threat.

Information theft, like most types of fraud, is typically an inside job: of those hit in the past year in which the attacker is known, 39% say it was the result of employee malfeasance, roughly unchanged from the 37% in last year's survey. Nevertheless, greater exposure to fraud from IT complexity is being exploited increasingly by outsiders. In this year's survey, 35% of information theft victims who know the source of the attack report that it was an external hacker, up from 18% in 2012. In addition, 17% of this group suffered as a result of a hacker attack on a vendor or supplier, compared with 5% in the previous survey.

Despite growing concern about information theft and the evolving nature of the threat, preparedness is far from universal. Of those surveyed, 68% say that they currently invest in some sort of IT security, which raises the question of how exposed the other one-third might be.

Chart 1. Percentage of companies affected by listed types of fraud

	2013	2012
Theft of physical assets	28%	24%
Information theft	22%	21%
Management conflict of interest	20%	14%
Vendor, supplier or procurement fraud	19%	12%
Internal financial fraud	16%	12%
Regulatory or compliance breach	16%	11%
Corruption and bribery	14%	11%
IP theft	11%	8%
Market collusion	8%	3%
Misappropriation of company funds*	8%	—
Money laundering	3%	1%

*Not covered in 2012 survey

Chart 2. Percentage of companies describing themselves as highly vulnerable to the following types of fraud

	2013	2012
Information theft	21%	7%
Corruption and bribery	20%	10%
Theft of physical assets	18%	6%
IP theft	18%	7%
Vendor, supplier or procurement fraud	18%	5%
Regulatory or compliance breach	18%	5%
Management conflict of interest	17%	4%
Market collusion	14%	5%
Misappropriation of company funds*	13%	—
Money laundering	11%	4%

* Not covered in 2012 survey

Chart 3. Percentage of respondents whose companies:

Plan to invest in IT security software in next year to reduce exposure to information security incidents	68%
Regularly conduct security assessments of their data and IT infrastructure	66%
Plan to invest in training IT employees in next year to reduce exposure to information security incidents	60%
Plan to invest in training their employees across all business functions in next year to reduce exposure to information security incidents	57%
Have an information security incident response plan that has been updated in the past year	53%
Have tested information security incident response plan in the past six months	48%

Chart 4. Percentage dissuaded from investing in:	
Latin America	31%
Central and Eastern Europe	27%
Africa	25%
At least one Asia-Pacific market	19%
Western Europe	18%
North America	16%
Southeast Asia	11%
China	10%
India	8%

Looking more closely at these investments, although 66% of respondents say that their firms regularly assess the security of their data and IT infrastructure, only around one-half have a current information security incident response plan [chart 3]. For professional services, the equivalent figures are particularly low, at 51% and 33% respectively, despite sensitive client data being central to many of their activities. Given the breadth of the problem, giving more attention to this area is something worth considering.

3. Fraud remains an inside job, but so does its discovery.

As reported in our earlier surveys, fraud is typically carried out by employees within the company. For the firms that had suffered fraud and the perpetrator was known, 32% had experienced at least one crime where a leading figure was in senior or middle management, 42% in which the incident involved a junior employee, and 23% where it was an agent or intermediary. Similarly, as noted above, employee malfeasance remains the most common driver of information theft. Overall, 72% of those surveyed say that their company has been hit by a fraud involving at least one insider in a leading role, slightly up from 67% last year.

However, this year's survey also shows that most types of fraud are discovered internally. Management's discovery of the crime was the most common reason for it coming to light, playing a role 52% of the time when a fraud was exposed, followed closely by internal audits (51%). Only in 10% of such cases did an external audit play a role.

Although senior employee alertness and audits are essential to combating fraud, these mechanisms can be weaker when senior employees themselves are the culprits. For example, according to the survey results, internal audits are slightly less likely to be involved in the uncovering of crime when senior or middle management is involved. Whistle-blowers are therefore an important means to expose wrongdoing. Of those hit by fraud, 32% report that whistle-blowers were responsible for its discovery at their company. More striking, such a tip-off played a role in 41% of the cases in which senior or middle management was involved in the fraud.

Surprisingly few companies, however, are cultivating whistle-blower programs. Only 52% of those surveyed report that they have already invested in staff training about fraud and the creation of whistle-blower hotlines, and just 43% say they intend to increase their investment in this area in the coming year. This may be short-sighted. With most fraud conducted by insiders, helping employees to recognize and report red flags will have clear benefits for companies.

4. Global business practices often increase fraud exposure.

Globalization has changed the way business operates. Companies have for some years now been in search of bigger international markets, while at the same time striving to become leaner. The latter typically involves becoming more focused on areas where they have a strategic advantage and finding ways for others to do the rest through outsourcing or partnerships.

Less appreciated is that these shifts, however profitable, lead to a higher risk of fraud in a variety of ways. For example, 30% of respondents report that entering new, riskier markets has increased their exposure to fraud in the past year. In the same period, greater levels of outsourcing and offshoring raised fraud risk for 28% of those surveyed, and increased collaboration in the form of joint ventures and partnerships for 20%. Overall, 54% of respondents report increased exposure owing to at least one of these factors.

The dangers of new business norms are feeding into other fraud figures. Of the companies that were hit in the past year and where the perpetrator was known, 30% suffered at the hands of vendors or suppliers and 11% at those of their joint venture partners. Similarly, procurement fraud was the fourth most common type of those covered in the survey this year (19%) and saw the biggest increase compared with last year.

Given the high level of risk, a surprisingly small proportion of companies are taking action. Only 43% intend to invest in greater due diligence for partners or vendors over the next 12 months. One of the reasons may be that, in the search to reduce costs—a permanent feature of global competition—fraud prevention can get left to the side: 20% of respondents report that a lack of resources or an insufficient budget to support compliance infrastructure is increasing their exposure to fraud. Companies need to be prepared for the dangers of fraudsters operating in the same global marketplace as they do.

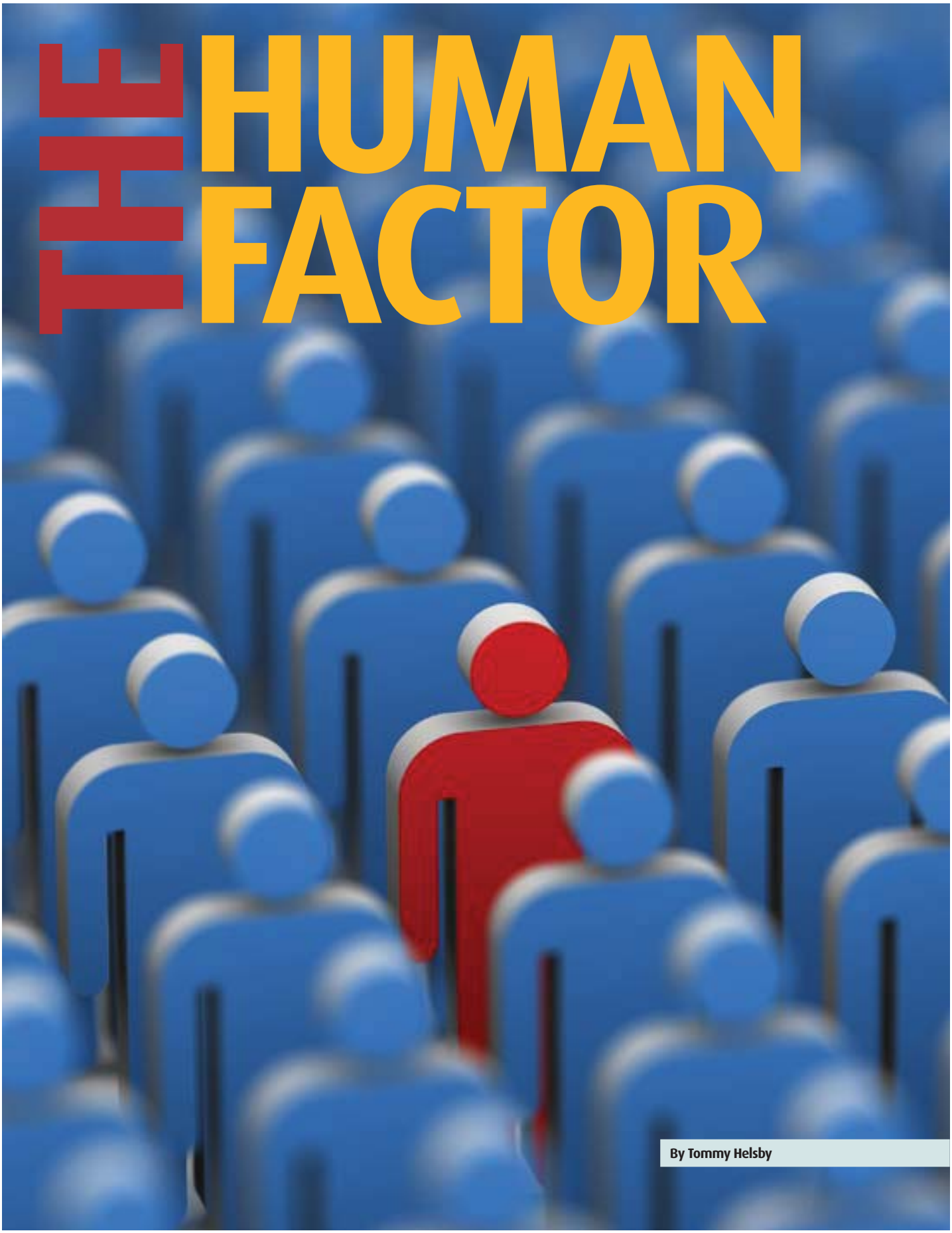
5. Those with local knowledge see fraud risks everywhere.

Certain regions have a reputation for high levels of fraud. It comes as no surprise, therefore, that 13% of all respondents were dissuaded in the past year from operating in Africa, and 11% in Latin America, from their experience or perception of fraud.

More striking is the degree to which fraud is keeping companies from making local investments, even in regions where the problem is thought to be relatively well controlled, particularly North America.

Even in a globalized world, companies typically invest closer to home. These figures therefore suggest that both the existence or appearance of fraud is a substantial drag on possible new investment and that outsiders coming in need to be aware of risks even in regions with a reputation for low levels of fraud.

THE HUMAN FACTOR



By Tommy Helsby

Economies are growing again. Stock markets are booming. Big deals are closing. And the fraud statistics are back on the rise. It's as if the financial crisis never happened.

Well, not quite. Regulatory pressure shows no sign of disappearing – in a separate survey of general counsels we have just completed, it was clearly the prime issue on people's agenda, and is driving a significant growth in compliance activity. This is probably driving increased fraud awareness – and fraud detection, given that we also see a rise in companies reporting that they have been victims of fraud. Undiscovered and unreported fraud, however minor, is an infection with the potential to grow into a life-threatening corporate disease – just read the stories of Enron, Satyam, Madoff, Parmalat and other major scandals, each of which started with small frauds that grew to consume the business.

It is noteworthy that awareness of the vulnerability to insider crime has shown particular growth.

Regulatory breach, conflict of interest and market collusion are all classic inside jobs, and the Global Fraud Survey results show a tripling of the number of companies being aware that they are "highly vulnerable," an awareness that is driving and being driven by the growth of the compliance function.

This has been a theme in many previous Kroll Fraud Reports and it is encouraging that the message is being received more broadly.

Increased regulation is not the only change. Much of the financial recovery is being led by government spending; not only quantitative easing but massive investment in infrastructure projects – one estimate suggests an average of $4 trillion per year over the next 15 years. Even when it is not government funded, infrastructure investment involves heavy interaction with government, for licensing, planning and coordination. It is also disproportionately focused on emerging markets, which have the greatest need of development; and typically, it involves joint ventures and local partners. When you look at this from a fraud-risk perspective, it's a high stakes trifecta: government contracts, emerging market exposure and third party agents, each one of which is identified by our survey participants as an area of concern.

So, one of our themes in this year's Fraud Report is infrastructure. Our experience in this area shows the global nature of the sector – Japanese companies investing in South America, Chinese and European companies competing in Africa and so on. But this should not distract from the equally damaging local problems: I can think of many examples of fraud cases involving a company operating in a single country suffering real damage from a crooked procurement or contracts manager. The impact is often not just financial, but costs management time, morale and reputation.

Our second big theme this year centers around one of the other major changes since our first Fraud Report in 2007: the rise of cyber fraud.

Computer-related crime is certainly not new – we have been active in this area for over 25 years. But the scale of the threat is new, and as an ever greater proportion of business activity becomes digital, the potential for economic and commercial damage grows with it. Every day brings a report of a new incident, with victims including companies in every sector and size, together with government agencies, charities, universities, hospitals and NGOs.

Clearly, awareness of the problem has grown rapidly, especially in the media. But there is still too much focus on the threat from 5,000 miles away rather than the man in the next office.

It is perhaps more comforting to think of the enemy as a faceless hacker in a distant land; but our experience shows that to be the exception rather than the rule.

The greatest vulnerability is a careless, vengeful or malicious employee, who has already got past most of your defenses by virtue of being an employee (or often, an IT contractor). Equally, your best defense may be another employee, who spots the aberrant behavior and has been encouraged to alert management on a timely basis. The human dimension to cyber fraud is often overlooked.

Indeed, the human dimension to fraud in general is central to Kroll's work. Cyber investigation tools, forensic analysis of books and records and open-source data research are all critical tools in our arsenal, and our use of them is second to none. But the most valuable tool is the experience of human nature gained through years of investigation, and cultural understanding of what to expect and what to look for in different regions around the globe. This connects with one further change: the inexorable spread of globalization.

The fraud case involving a single location is now a rarity: the client is in one country, the fraud in a second, the perpetrator in a third and the money…well, that's often the challenge.

But without a good understanding of how things work in each place, that's a challenge that may not be fully met.

Tommy Helsby is Chairman of Kroll, based in London. Since joining Kroll in 1981, Tommy has helped found and develop the firm's core due diligence business, and managed many of the corporate contest projects for which Kroll became well known in the 1980s. Tommy plays a strategic role both for the firm and for many of its major clients in complex transactions and disputes. He has a particular interest in emerging markets, especially Russia and India.